CYBER SECURITY ISSUES IN INDIA

A Course Activity Report

21CSC308T SECURITY RISK MANAGEMENT PRINCIPLES

(2021 Regulation) III year/ V Semester

Academic Year:2024 - 2025

BY

1. I. RAKESH [RA2211030010218]
2. K. CHARITH [RA2211030010224]
3. P. MOHAN [RA2211030010234]

4.P. ABHISHEK [RA2211030010243]

5.B. YASWANTH[RA2211030010262]

6. Y. LALITH[RA2211030010265]

Under the guidance of

Dr. Vinoth Kumar C N S

Associate Professor

Department of Networking and Communications

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

DEPARTMENT OF NETWORKINGANDCOMMUNICATIONS
COLLEGE OF ENGIEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603203
NOVEMBER 2024

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

BONAFIDE

Certified that this course activity report titled "**SECURITY ISSUES IN INDIAN**" for the course "**21CSC308T Security Risk Management Principles"** is the Bonafide work of **"I. RAKESH[RA2211030010218], K. CHARITH [RA2211030010224], P. MOHAN [RA2211030010234], P. ABHISHEK [RA2211030010243], B. YASAWNTH[RA2211030010262]"** and **Y. LALITH [RA2211030010265]** who undertook the task of completing the activity within the allotted time.

Signature

Dr. Vinoth Kumar C N S
Associate Professor
Department of NWC

Signature

Dr. M Lakshmi
Head of the Department
Professor
Department of NWC

CONTENTS OF TABLE

CHAPTER-1

INTRODUCTION

‘Over the years, Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. With the Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. An increasing proportion of the world’s population is migrating to cyberspace to communicate, enjoy, learn, and conduct commerce. It has also created new vulnerabilities and opportunities for disruption.

The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. As such, cyber security threats pose one of the most serious economic and national security challenges.

Cyberspace is such a term, which is not yet completely defined and also has no geographical limitation. It is a term associated with application of the Internet worldwide. It is also called as a virtual space as physical existence of cyberspace is not detectable at all. Cyberspace is “the total interconnectedness of human beings through computers and telecommunication without regard to physical geography.”

Information through computers is transferred in the form of Ones (1) and Zeros (0), which do not inherently carry any separate information along with them for authentication. For authentication purposes, additional information needs to be carried with cyberspace transactions for identity purposes.

Providing extra information in digital communication introduces the possibility for identity theft. Because nothing prevents the transmission of false identity information, or the duplication of another’s identity information. The seriousness of this problem is highlighted when you consider that future technologies will allow extremely important identifiers, such as a retinal scan or a fingerprint, to be represented digitally. These biometrics characteristics are protected in real space because they are embedded in the physical body of the person. This is lost in cyberspace. Thus, cyberspace needs a system that allows individuals to verify their identities to others without revealing to them the digital representation of their identities.

DEFINITION

Cyber Security is “the security of information and its communicating channels as applied to computing devices such as computers and smart phones, as well as computer networks such as private and public networks, including the Internet as a whole.”

The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses.

It has proved a challenge for governments all around the world. The task is made difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators. The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialized has seen the use of cyberspace expand dramatically in its brief existence. From its initial avatar as a N/W created by academics for the use of the military, it has now become a global communications platform for socio-economic issues as well as for commercial and social purposes.

The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU), according to which,

- The number of Internet users has doubled between 2005 and 2010 and surpasses 2 billion.

- Users are connecting through a range of devices from the personal computer (PC) to the mobile phone, and using the Internet for a variety of purposes from communication to e-commerce, to data storage for several services.

The rise in the Internet population has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military-national security actors at one end and economic-civil society actors at the other.

SCOPE OF THE STUDY:

To understand the awareness among the public regarding cyber security issues in India. The study is restricted to the 50 respondents who are randomly selected with in the twin cities of Hyderabad and Secunderabad.

METHODOLOGY:

Sources of data collection:

- Primary data
- Secondary data

PRIMARY DATA:

The main source of primary data is questionnaire consisting of simple questions prepared and distributed to respondents for collection of data on awareness in public regarding web search engines.

SECONDARY DATA:

The main source of secondary data includes Books, Magazines, Newspapers, Articles and Journals and websites.

SAMPLE SIZE:

For the present study, 50 respondents were selected at random.

LIMITATIONS OF THE STUDY

- The study is conducted in Hyderabad and Secunderabad only.
- The study is restricted to the users of web search engine only.
- Time perspective is also one of the elements in limiting the scope of this study.

INDIAN CYBER SPACE

- The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government.
- Between 1986 and 1988, three N/Ws were set up:
- INDONET, connecting the IBM mainframe installations that made up India's computer infrastructure;
- NICNET (the NIC Network), being a nationwide very small aperture terminal (VSAT) N/W for public sector organizations as well as to connect the central government with the state governments and district administrations;
- The Education and Research Network (ERNET), to serve the academic and research communities.

- Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003.

Indian presence in Internet/Avenues of vulnerability in Cyber space / Indian stakes at risk in Cyber space

As per World Bank report

- By June2012, Internet users in India were approx. 12.5% of the total population (approx. 137 million).

According to the Internet and Mobile Association of India (IAMAI),

- The internet user base in India is projected to touch 243 million by June 2014, with a year-on-year growth of 28%.

This exponential growth is again expected to continue in recent future with more and more people accessing the web through mobile phones and tablets, with the government making a determined push to increase broadband(>4mbps) penetration from its present level of about 6%.

National e-Governance Plan (Ne G P)

Even though the Indian government was a late convert to computerization, there has been an increasing thrust on e-governance, seen as a cost effective way of taking public services to the masses across the country.

Critical sectors such as Defence, Energy, Finance, Space, Telecommunications, Transport, Land Records, Public Essential Services and Utilities, Law Enforcement and Security all increasingly depend on N/Ws to relay data, for communication purposes and for commercial transactions.

The National e-governance Program (Ne GP) is one of the most ambitious in the world and seeks to provide more than 1200 governmental services online. Schemes like ‘Rajiv Gandhi scheme for broadband to PRIs’ and National Optic Fiber Network (NOFN) missionare already dedicated to accelerate cyber connectivity in far reaching areas of country.

- Under The National Broadband Plan, the target for broadband is 160 million households by 2016. Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments.

- Similar level of penetration has also been seen in the social networking arena, which is the most recent entrant to the cyber platform. India currently has the fastest growing user base for Facebook and Twitter, the two top social networking sites.

CHAPTER-2

TYPES OF CYBER THREATS

As we grow more dependent on the Internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility.

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets:

1. Cyber Espionage,

2. Cyber Crime

3. Cyber Terrorism

4. Cyber Warfare

Cyber Espionage:

Cyber espionage, is "the act or practice of obtaining secret information without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware."

Simply said, Cyber espionage is "The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization."

India: Victim of Chinese Cyber Espionage

1. Cyber attack by Chinese crackers at the computers in the Prime Minister's Office (PMO) was reported in 2009.

2. In August 2015, security firm Fire Eye revealed an intense activity of hackers based in China particularly interested in entities and organization linked to the Indian Government as well as in information on Tibetan activists. The cyber espionage group sent targeted spear-phishing e-mails to its intended victims, with Microsoft Word attachments containing information on regional diplomatic issues .It said that collecting intelligence on India remains a key strategic goal for China-based APT groups, and these attacks on India and its neighboring countries reflect growing interest in its foreign affairs.

Cyber Crime/ Cyber Attacks:

Cyber-attack is "any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks with an intention to damage or destroy targeted computer network or system."

These attacks can be labeled either as Cyber-campaign, Cyber-warfare or Cyber-terrorism depending upon the context, scale and severity of attacks. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the critical infrastructure of entire nations.

The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber-crime being in billions of dollars worldwide.

While other countries are reporting enormous losses to cyber-crime, as well as threats to enterprises and critical information infrastructure (CII), there are hardly any such reports coming out of India other than those relating to cyber espionage.

- Though the report of the National Crime Records Bureau (NCRB) in 2010 reported an increase of 50% in cyber-crime over the previous year, the numbers were quite small in absolute terms.

- On 12 July 2012, a high profile cyber-attack breached the email accounts of about 12,000 people, including those of officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organization (DRDO), and the Indo-Tibetan Border Police (ITBP).

- In February 2013, The Executive Director of the Nuclear Power Corporation of India (NPCIL) stated that his company alone was forced to block up to ten targeted attacks a day.

Cyber Terrorism:

Acts of Terrorism related to cyber space and /or executed using Cyber technologies are popularly known as 'cyber terrorism'.

Definitions of cyber terrorism

"Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives, Further, to qualify as cyber terrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear, Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact."

This is one of the most comprehensive definitions of cyber terrorism. But even this has a limitation. It states that for an attack to qualify as a cyber-terrorism it should lead to violence. This is more conventional. Terrorist may direct an attack only to disrupt key services, If they create panic by attacking critical systems/infrastructure there is no need for it to lead to violence. In fact such attacks can be more dangerous.

In the last couple of decades India has carved a niche for itself in IT. Most of the Indian banking industry and financial institutions have embraced IT to its full optimization. Reports suggest that cyber-attacks are understandably directed toward economic and financial institutions. Given the increasing dependency of the Indian economic and financial institutions on IT, a cyber-attack against them might lead to an irreparable collapse of our economic structures. And the most frightening thought is the ineffectiveness of reciprocal arrangements or the absence of alternatives.

Cyber Warfare:

The Fifth domain of warfare the evolution of technology impacts the nature of conflict and war. Cyber Warfare is a very recent yet evolving phenomenon.

In the absence of a formal definition of cyber warfare, we may define it as “actions by a nation-state or its proxies to penetrate another nation’s computers or networks for the purposes of espionage, causing damage or disruption”. These hostile actions against a computer system or N/W can take two forms: cyber exploitation and cyber-attacks.

Types of Security threats:-

Cybercrimes consist of specific crimes dealing with computers and networks, such as hacking, phishing and the facilitation of traditional crime through the use of computers (child pornography, hate crimes, telemarketing/internet fraud). A brief introduction to some common cyber related violations, or cybercrimes as they are more commonly referred to are discussed below:

- **Hacking**

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian legal perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer.

- **Child Pornography**

The Internet is extensively used for sexual abuse of children. As more homes have access to internet, more children are accessing it and this enhances their vulnerability of falling victims to the aggression of paedophiles. Paedophiles (a person who is sexually attracted to children) lure the children by distributing pornographic material and then pursue them for sexual exploitation. Sometimes paedophiles contact children in chat rooms posing as teenagers or children of similar age; they win the confidence of these children, and then induce them into sexually provocative discussions. Then begins the actual exploitation of children.

- **Cyber Stalking**

This term is used to refer to the use of the internet, e-mail, or other electronic communications devices to stalk another person. Cyber stalking can be defined as the repeated acts of harassment or threatening behavior of the cyber-criminal towards the victim by using internet.

- **Denial of Service**

This is a technology driven cyber intrusion, where by the influencer floods the bandwidth or blocks the user's mails with spam mails depriving the user, access to the Internet and the services provided there from. A DoS Attack (as it is commonly known) can be perpetrated in a number of ways.

- **Dissemination of Malicious Software (Malware)**

Malware is defined as software designed to perform an unwanted illegal act via the computer network. It could be also defined as software with malicious intent. Malware can be classified based on how they get executed, how they spread, and/or what they do. Some of them are discussed below.

a) Virus

A virus is a program that can infect other programs by modifying them to include a possible evolved copy of itself. A virus can spread throughout a computer or network using the authorization of every user using it to infect their program. Every program so infected may also act as a virus and thus the infection grows. Viruses normally affect program files, but in some cases they also affect data files disrupting the use of data and destroying them completely.

b) Worms

Worms are also disseminated through computer networks, unlike viruses, computer worms are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files. For example, a mass mailing e-mail worm is a worm that sends copies of itself via e-mail. A network worm, on the other hand makes copies of itself throughout a network, thus disrupting an entire network.

c) Trojans

Trojan is another form of Malware; trojans do things other than what is expected by the user. *Trojan or trojan horse* is a program that generally impairs the security of a system. Trojans are used to create back-doors (a program that allows outside access into a secure network) on computers belonging to a secure network so that a hacker can have access to the secure network. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

d) Hoax

Hoax is an e-mail that warns the user of a certain system that is harming the computer. The message thereafter instructs the user to run a procedure (most often in the form of a download) to correct the harming system. When this program is run, it invades the system and deletes an important file.

e) Spyware

Spyware invades a computer and, as its name implies, monitors a user’s activities without consent. Spywares are usually forwarded through unsuspecting e-mails with bonafide email i.ds. Spyware continues to infect millions of computers globally.

- **Phishing**

Phishers lure users to a phony web site, usually by sending them an authentic appearing e-mail. Once at the fake site, users are tricked into divulging a variety of private information, such as passwords and account numbers.

Cyber Security Issues In India:-

The Current And Present Dangers Of Aadhaar Hacking

Cyber security is a complicated field to manage and even the most ardent players of cyber security are aware that absolute cyber security is a myth. So if anybody is claiming that his/her system, software or project is 100% cyber secure, he/she is simply ignorant of the ground realities as exist in the cyberspace.

Till sometime back, cyber warfare was considered as a fiction and not reality. But with growing incidences of cyber espionage, cyber terrorism and even cyber warfare, countries have started taking their critical infrastructures seriously. Nevertheless, the task to secure these critical infrastructures is next to impossible as the bad guys are always many steps ahead of the government and its agencies.

Aadhaar is one such highly sensitive and highly insecure project of India government that is neither prudent nor secure. It only has a false sense of security that government is projecting to divert the attention of critics of Aadhaar. But real cyber security professionals are well aware of the dangers of Aadhaar project that has put the lives and properties of Indians in great peril.

In reality, Aadhaar has created serious constitutional anomaly and irresolvable cyber security issues that would always jeopardise rule of law and personal safety and security of

Indians. No matter whatever Indian government tells you, stay away from Aadhaar. And if you have already made an Aadhaar, deseed it from all services and block your biometric as soon as possible so that it cannot be abused by government and private individuals.

Mobile Cyber Security in India is Needed Under Digital India

Mobiles are believed to play a major role in the successful implementation of the Digital India project of Indian government. From mobile commerce to mobile banking, the Indian government is betting big upon mobiles and their use for public delivery of services through electronic means. Of course, this big scale use of mobiles will also give rise to cyber law and cyber security issues that Indian government must be well prepared to deal with in future.

Mobile phones have become ubiquitous these days. They are used for multiple purposes ranging from personal use to mobile banking. Cyber criminals have also realized the importance of mobile phones for committing cyber crimes and financial frauds. This is also the reason why malware writers are also writing mobile phone specific malware to steal

confidential and sensitive information.
Mobile cyber security in India has become a cause of concern these days. Mobile phones are now proposed to be used for mobile banking and mobile governance in India. Naturally, we must ensure robust mobile cyber security in India. An electronic

authentication policy of India can help in more active and secure mobile usages in India. Mobile governance and e-authentication in India are also closely related and with the proposed electronic delivery of services in India this is also a must have requirement. For the time being we have no implementable electronic delivery of services policy of India though it may be in pipeline. Indian government is working in the direction of ensuring electronic delivery of services in India. In fact a legal framework titled electronic delivery of services bill 2011 (EDS Bill 2011) was also proposed by Indian government in the past. The same has still to become an applicable law in India. Once the EDS Bill 2011 becomes an applicable law, governments across the India would provide electronic services through various modes, including mobile phones. This requires putting a robust and reliable mobile security infrastructure in India.

However, using of mobile phones for commercial and personal transactions in India is also risky. For instance, the mobile banking in India is risky as the present banking and other technology related legal frameworks are not conducive for mobile banking in India.

Similarly, we do not have a well developed e-governance infrastructure in India. As a result India is still not ready for m-governance. We at Perry4Law Organization (P4LO) believe

that the biggest hurdles before the mobile related uses in India pertain to use of weak encryption standards and non use of mobile cyber security mechanisms in India. Absence of encryption laws in India has further made the mobile security very weak in India. The ever evolving mobile malware are further increasing the woes of mobile users' worldwide. As on date the malware are defeating cyber security products and services with ease.

It is high time for India to seriously work upon mobile cyber security aspects as soon as possible. The policy decisions in this regard must be taken urgently and must be implemented as soon as possible.

CHAPTER-3

Cyber Laws in India

The first technology based law in India was the Indian Telegraph Act of 1885. This law was framed with the advent of the telegraph and later covered yet another advance in technology, the telephone.

In the domain of technology driven law falls the Information Technology Act, 2000.While the Information Technology Act is the most significant Act addressing conduct in cyberspace in India, there are a whole lot of other Acts that would apply to govern and regulate conduct and transactions in cyberspace. Take for instance online contracts. Apart from the relevant provisions of the IT Act, the Indian Contract Act, the Sale of Goods Act, 1930 etc. would be relevant to determine the legality of such contracts.

Further the provisions of the Competition Act, 2002 or in case of unfair trade practices, the Consumer Protection Act 1986, would also be relevant. Protection of intellectual property available on the Internet is one of the greatest challenges of the day. Be it books, films, music, computer software, inventions, formulas, recipes, everything is available on the net. Protection of copyrights trademarks online would entail the invocation of the Indian Copyright Act and, the Trade Marks Act.

As far as illegal activities on the net are concerned, apart from specific provisions in the IT Act that penalizes them, a whole gamut of other Acts would govern them. For instance in case of an Internet fraud, based on the nature of the fraud perpetrated, Acts such as the Companies Act, 1956.Thus it can be inferred that while the IT Act is the quintessential Act regulating conduct on the Internet based on the facts of a case or the nature of a transaction, several other Acts may be applicable. Therefore, cyber laws includes the whole set of legislation that can be applied to determine conduct on the Internet.

Information Technology Act, 2000:-

The Information Technology Act, 2000 intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods. The Act has adopted a functional equivalents approach in which paper based requirements such as documents, records and signatures are replaced with their electronic counterparts.

The Act seeks to protect this advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and forming regulatory authorities. Many electronic crimes have been bought within the definition of traditional crimes too by means of amendment to the Indian Penal Code, 1860. The Evidence Act, 1872 and the Banker's Book Evidence Act, 1891 too have been suitably amended in order to facilitate collection of evidence in fighting electronic crimes.

National Cyber security Policy, 2013

In light of the growth of IT sector in the country, the National Cyber Security Policy of India 2013 was announced by Indian Government in 2013 yet its actual implementation is still missing. As a result fields like e-governance and e-commerce are still risky and may require cyber insurance in the near future. Its important features include:

- To build secure and resilient cyber space.
- Creating a secure cyber ecosystem, generate trust in IT transactions.
- 24 x 7 NATIONAL CRITICAL INFORMATION INFRASCTRUCTURE PROTECTION CENTER (NCIIPC)
- Indigenous technological solutions (Chinese products and reliance on foreign software)
- Testing of ICT products and certifying them. Validated products
- Creating workforce of 500,000 professionals in the field
- Fiscal Benefits for businessman who accepts standard IT practices, etc.

Ongoing efforts in India

The government has conducted several awareness and training programs on cyber crimes for law enforcement agencies including those on the use of cyber Forensics Software packages and the associated procedures with it to collect digital evidence from the scene of crime.

Special training programs have also been conducted for the judiciary to train them on the techno-legal aspects of cyber crimes and on the analysis of digital evidence presented before them. Both the CBI and many state police organizations are today geared to tackle cybercrime through specialized cyber crime cells that they have set up.

Stakeholder agencies in India

Countering cyber crimes is a coordinated effort on the part of several agencies in the Ministry of Home Affairs and in the Ministry of Communications and Information Technology. The law enforcement agencies such as the Central Bureau of Investigation, The Intelligence Bureau, state police organizations and other specialized organizations such as the National Police Academy and the Indian Computer Emergency Response Team (CERT-In) are the prominent ones who tackle cyber crimes. We will see about of few of them:

1. National Information Board (NIB)

National Information Board is an apex agency with representatives from relevant Departments and agencies that form part of the critical minimum information infrastructure in the country.

2. National Crisis Management Committee (NCMC)

The National Crisis Management Committee (NCMC) is an apex body of Government of India for dealing with major crisis incidents that have serious or national ramifications. It will also deal with national crisis arising out of focused cyber-attacks.

3. National Security Council Secretariat (NSCS)

National Security Council Secretariat (NSCS) is the apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB.

4. Department of Information Technology (DIT)

Department of Information Technology (DIT) is under the Ministry of Communications and Information Technology, Government of India. DIT strives to make India a global leading player in Information Technology and at the same time take the benefits of Information Technology to every walk of life for developing an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion & policies in electronics & IT.

5. Department of Telecommunications (DoT)

Department of Telecommunications (DoT) under the Ministry of Communications and Information Technology, Government of India, is responsible to coordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In and other government agencies. DoT will provide guidelines regarding roles and responsibilities of Private Service Providers and ensure that these Service Providers are able to track the critical optical fiber networks for uninterrupted availability and have arrangements of alternate routing in case of physical attacks on these networks.

CASES OF CYBER ATTACK

Big no. previously there are so many cyber attacks some of the famous ones includes.

1. In 2014, Sony Pictures Entertainment became the target of the biggest cyber attack in US corporate history, linked to its release of North Korea satire "The Interview", hated by Pyongyang.

2. The past year witnessed a devastating attack on Ukraine’s critical infrastructure.

Known Cases of cyber attacks and cyber warfare:

Year wise cyber attacks and cyber welfare are shown in table-1

Table-1

Year	Case
2010	Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility. The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyber warfare.
2009	Operation Aurora is a cyber attack which began in mid-2009 and continued through December 2009. The attack was first publicly disclosed by Google in January 2010, and was believed to be originated from China. The attack has been aimed at dozens of other organizations, of which Adobe Systems, Juniper Networks and Rack space have publicly confirmed that they were targeted.
2009	A series of coordinated cyber attacks against major government, news media, and financial websites in South Korea and the United States. While many thought the attack was directed by North Korea, one researcher traced the attacks to the United Kingdom.
2008	A cyber spy network, dubbed Ghost Net, using servers mainly based in China has tapped into classified documents from government and private organizations in 103 countries, including the computers of Tibetan exiles, but China denies the claim.
2007	United States government suffered an "an espionage Pearl Harbor" in which an "unknown foreign power…broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information.

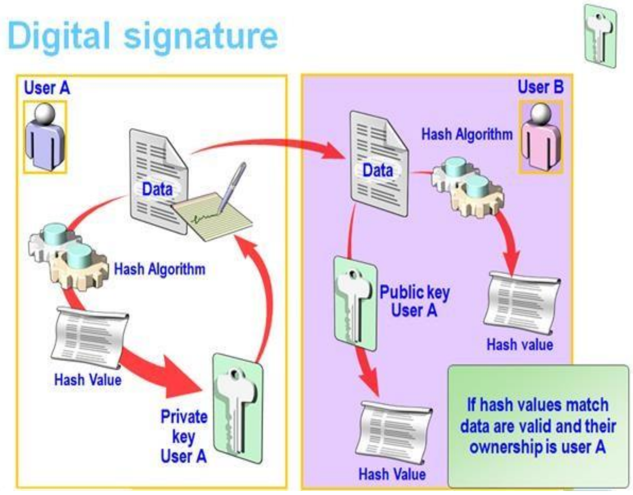
Source: www.thehansindia.com

Tools to protect against cyber threats

Other than the general use of antivirus, firewalls & gateways, strong passwords, secure Wi-Fi connection, training to netizen, etc. there are few other practice which keeps our data and network safe from cyber threats. Some of them are mentioned below:

- **Digital Signatures**

A Digital Signature is a technique by which it is possible to secure electronic information in such a way that the originator of the information, as well as the integrity of the information, can be verified. This procedure of guaranteeing the origin and the integrity of the information is also called Authentication. The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature. For a computerized message system to replace the physical transport of paper and ink documents handwritten signatures have to be replaced by Digital Signatures. A digital signature is only a technique that can be used for different authentication purposes. For an E-record, it comes functionally very close to the traditional handwritten signatures. The user himself/ herself can generate key pair by using specific crypto software. Now Microsoft IE and Netscape, allow the user to create his/ her own key pair. Any person may make an application to the Certify Authority for issue.



- **Encryption**

One of the most powerful and important methods for security in computer systems is to encrypt sensitive records and messages in transit and in storage. Cryptography has a long and colorful history. Historically, four groups of people have used and contributed to the art of Cryptography, the military, the diplomatic corps, diarists, and lovers. The military has had the most sensitive role and has shaped the field.

At present, information and data security plays a vital role in the security of the country, the security of the corporate sector and also of every individual, working for personal benefit. The message or data to be encrypted, also known as the plaintext, is transformed by a function that is parameterized by a KEY. The output of the encryption process, known as the cipher text, is then transmitted through the insecure communication channel. The art of breaking ciphers is called cryptanalysis. The art of devising ciphers (cryptography) and breaking them (cryptanalysis) is collectively known as cryptology. It is done with the help of algorithms, few of them are- The Secret-Key Algorithm, Data Encryption Standard (DES, Public Key Algorithms, RSA Algorithm, etc.

- **Security Audit**

A **security audit** is a systematic evaluation of the **security** of a company's information system by measuring how well it conforms to a set of established criteria. It is to find out the vulnerabilities that an organization is facing with its IT infrastructure. A thorough audit typically assesses the security of the system's physical configuration and environment.

- **Cyber Forensics**

Cyber Forensics is a very important ingredient in the investigation of cyber crimes. Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer systems, computer networks, computer media, and computer peripherals that allow investigators to solve a crime.

Principal concerns with computer forensics involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes. The other concern is network forensics, is a more technically challenging aspect of cyber forensics. It gathers digital evidence that is distributed across large-scale,complexnetworks.

E-discovery investigation includes areas like money laundering, corruption, financial frauds, cyber crimes, serious frauds and white collar crimes investigation, etc. Presently e-discovery services in India are in infancy stage and this is the reason why many cases of corporate frauds and cyber crimes remain unreported.

CHAPTER-4

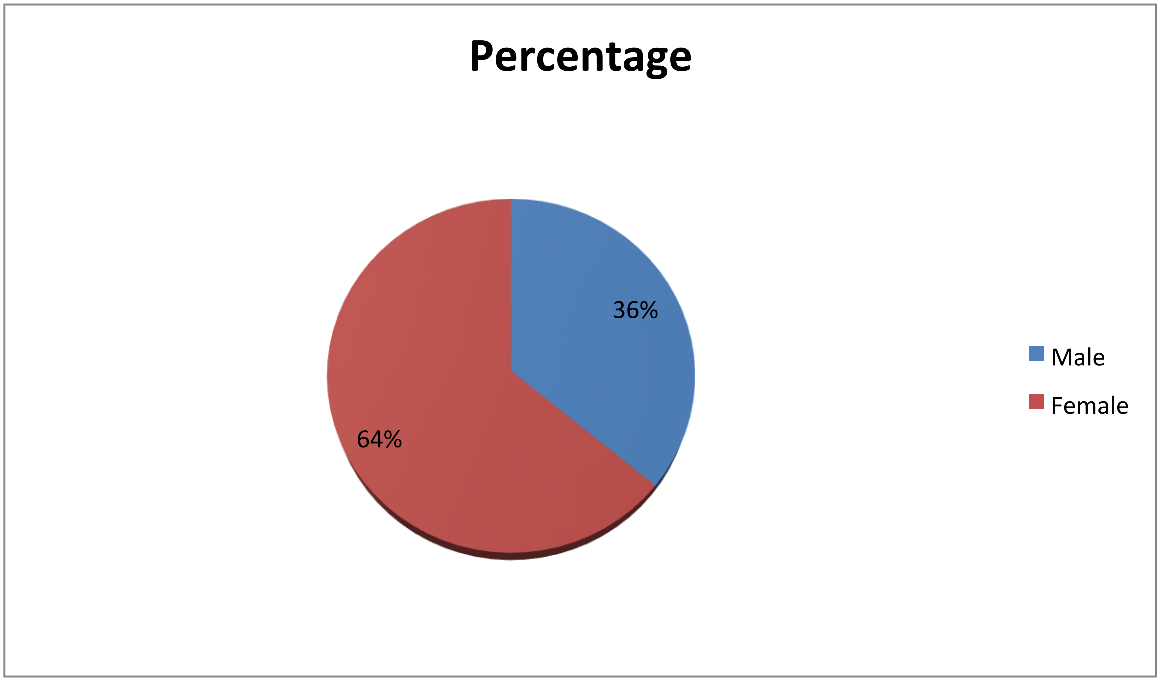
DATA ANALYSIS AND INTERPRETATION:

Questionnaires are administered to respondents selected randomly within twin cities of Hyderabad and Secunderabad. 50/50 respondents have responded. The data so collected is tabulated, analyzed, interpreted and presented in the following tables and charts:

Gender – respondents

Table – 1

Gender	Number of respondents	Percentage(%) of respondents
Male	18	36%
Female	32	64%
Total	**50**	**100%**



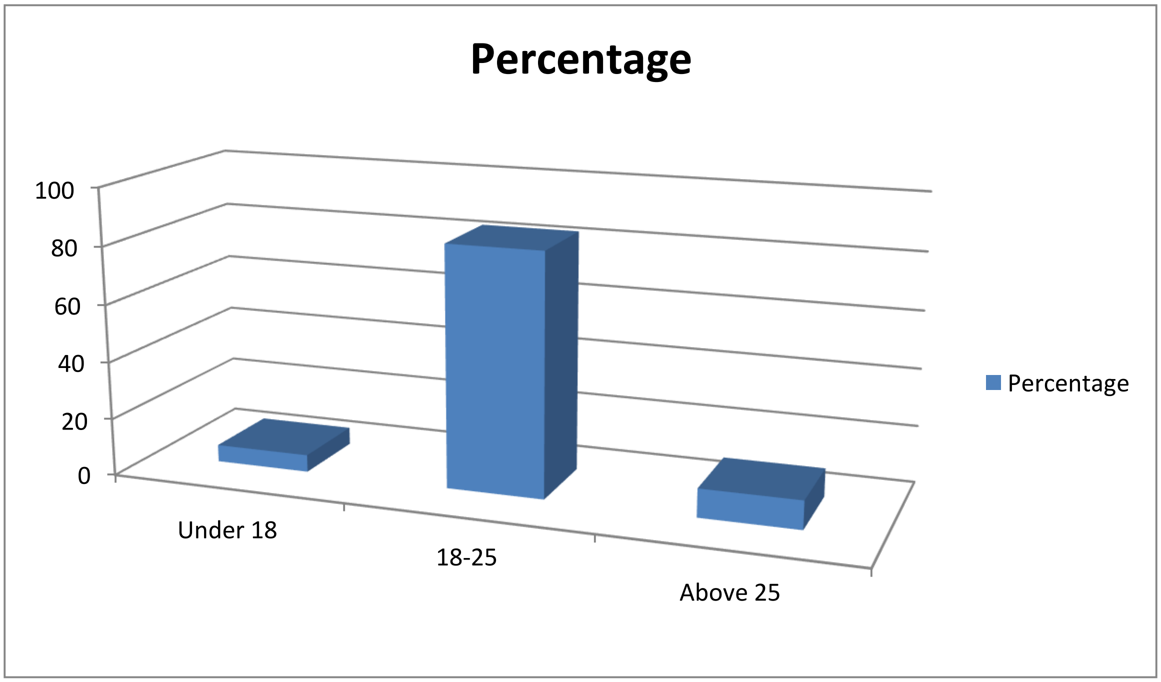
INTERPRETATION

From the above chart it is observed the 36% of respondents (18/50) are male. 64% of respondents (32/50) are female.

Age-group of respondents

Table – 2

Age group	**Number of respondents**	**Percentage(%) of respondents**
Under 18	3	6%
18 - 25	42	84%
Above 25	5	10%
Total	**50**	**100%**



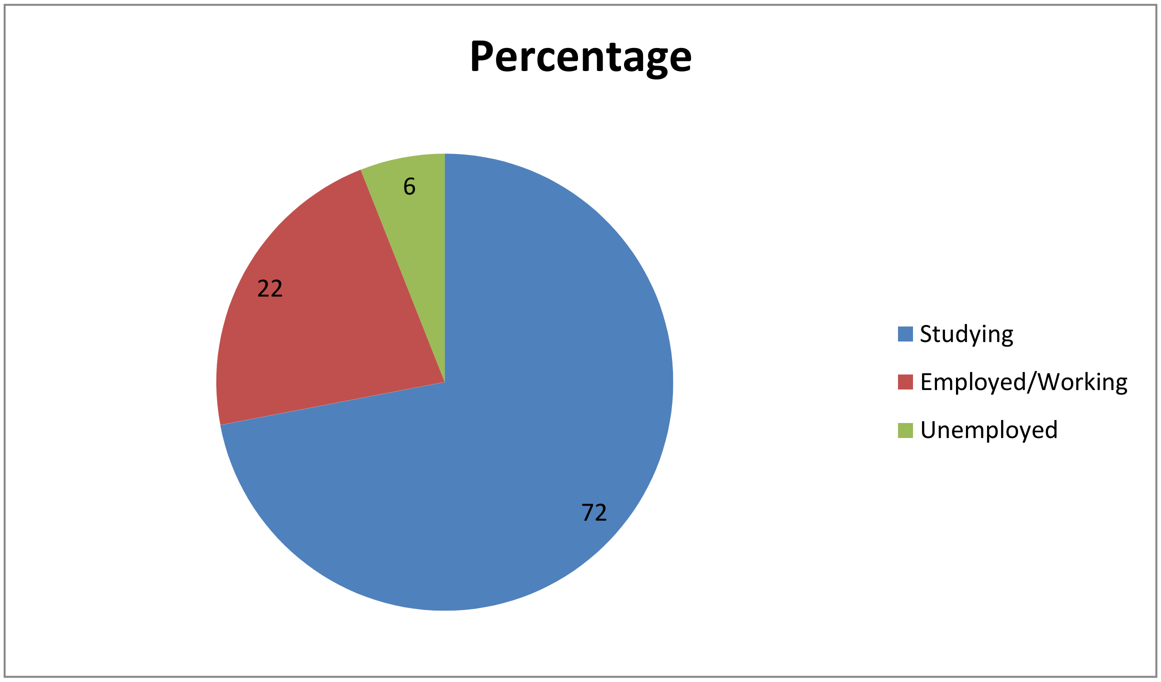
INTERPRETATION

From the above chart it is observed that the 6% of respondents (3/42) fall under the age group of below 18. 84% of respondents (42/50) fall under the age group of 18-25. 10% of respondents (5/50) fall under the age group of above 25.

STATUS

Table – 3

Occupation	**Number of respondents**	**Percentage(%) of respondents**
Studying	36	72
Employed/Working	11	22%
Unemployed	3	6%
Total	**50**	**100%**



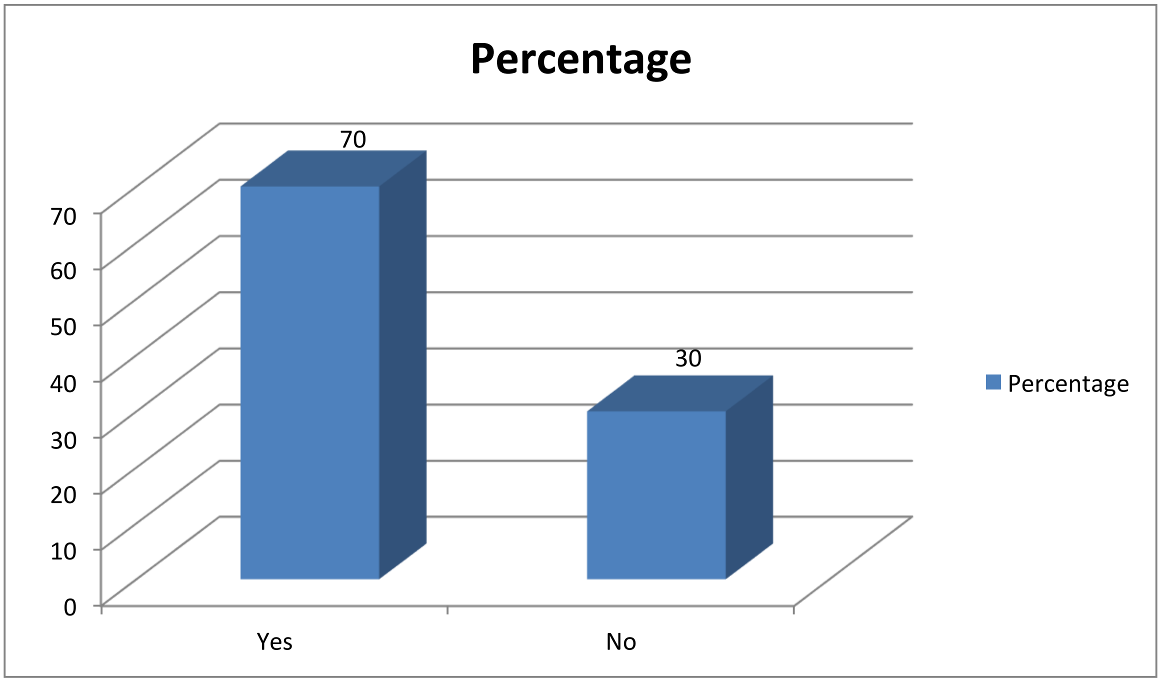
INTERPRETATION

From the above chart it is observed that the 72% of respondents (36/50) are still studying. 22% of respondents (11/50) are employed or working. 6% of respondents (3/50) are unemployed.

Awareness regarding Cyber Security Issues

Table-4

Options	**Number of respondents**	**Percentage(%) of respondents**
Yes	35	70%
No	15	30%
Total	**50**	**100%**



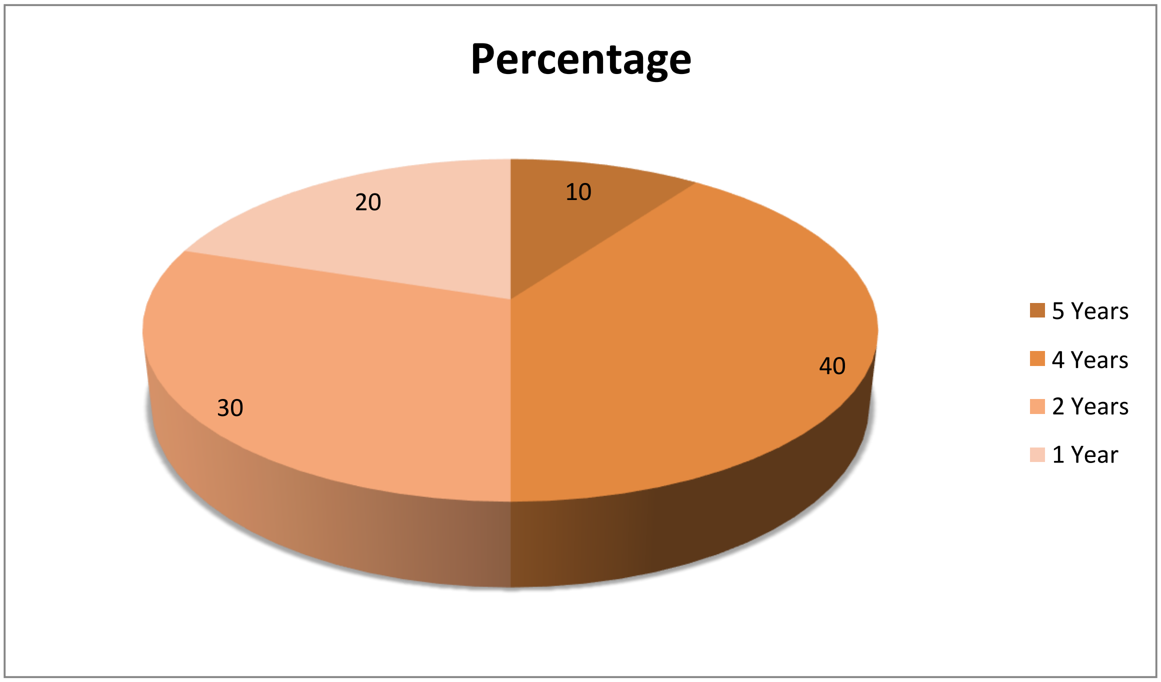
INTERPRETATION

From the above chart it is observed that the 70% of respondents (35/50), have awareness regarding Cyber Security Issues. Whereas the 30% of respondents (15/50) are not having awareness regarding Cyber Security issues.

Growth of the Internet

Table-5

Options	**Number of respondents**	**Percentage(%) of respondents**
5 Years	5	10%
4 Years	20	40%
2 Years	15	30%
1 Year	10	20%
Total	**50**	**100%**



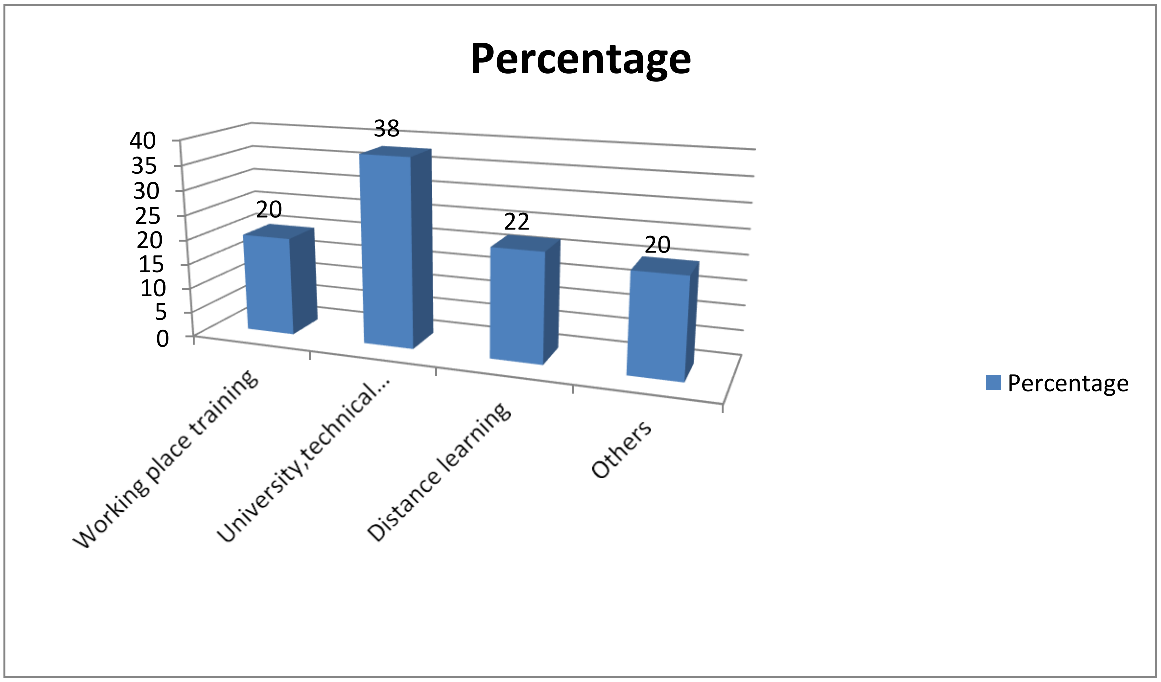
INTERPRETATION

From the above chart it is observed that the 10% of respondents (5/50) are using internet for 5Years. And 30% of respondents (15/50) are using internet for 4 Years. 40% of respondents (20/50) are using internet for 2 Years. 20% of respondents (10/50) are using internet for 1 Year.

Sources available for learning Information Security

Table-6

Option	**Number of respondents**	**Percentage (%) of respondents**
Working place training	10	20%
University, technical college etc.	19	38%
Distance learning etc.	11	22%
Others	10	20%
Total	**50**	**100%**



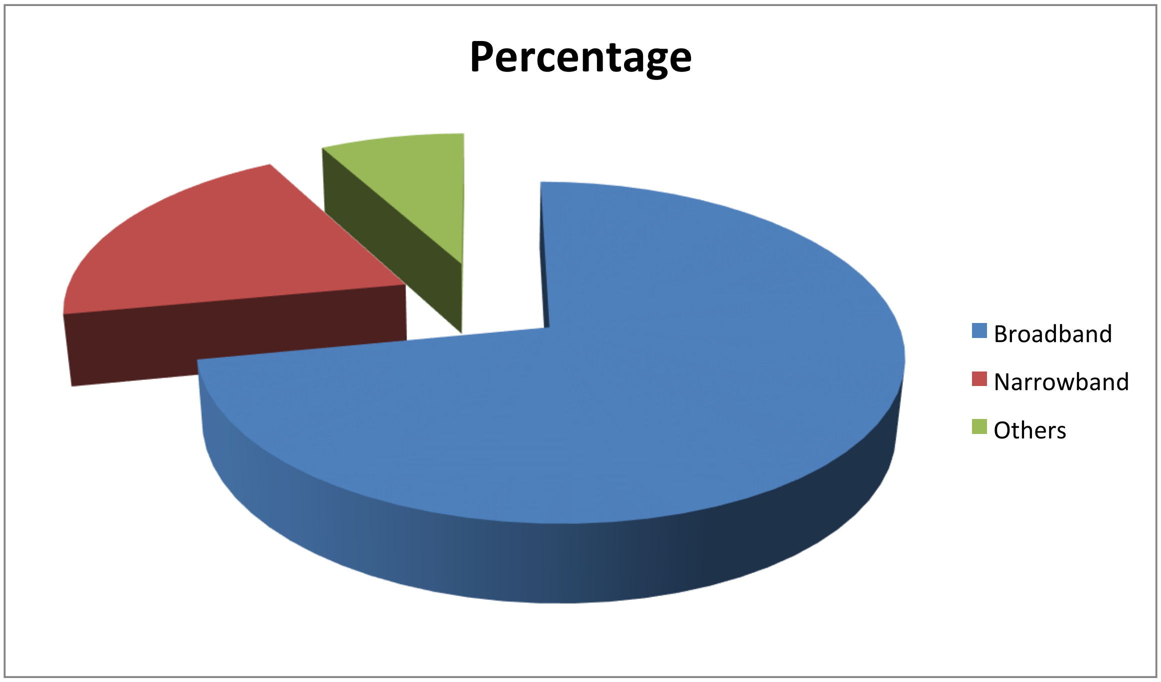
INTERPRETATION

From the above chart it is observed that 20% of respondents are learning Information Security from the source of Working place training. 38% of respondents (19/50) are learning Information Security from the source of University, technical college etc. 22% of respondents (11/50) are learning Information Security from the source of Distance learning etc. 20% of respondents (10/50) are learning Information Security from the source of others.

Kind of internet connection at home

Table-7

Options	Number of respondents	Percentage (%) of respondents
Broadband	36	72%
Narrowband	10	20%
Others	4	8%
Total	**50**	**100%**



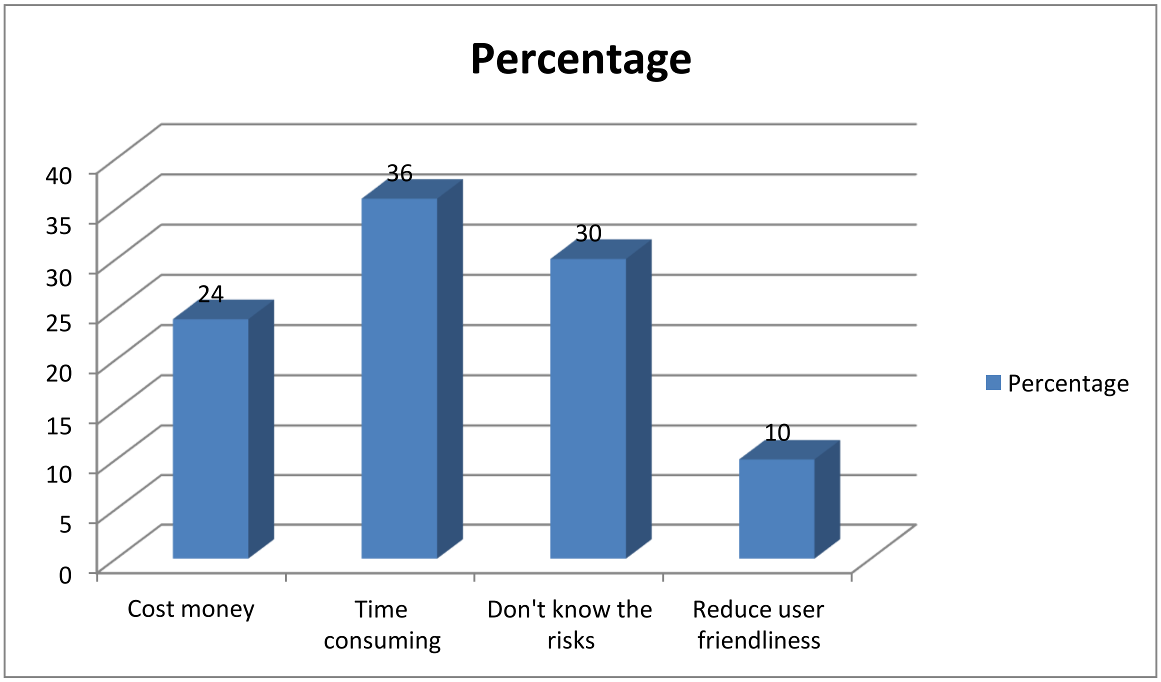
INTREPRETATION

From the above chart it is observed that the 72% of respondents (36/50) are having broadband kind of internet connection at their home. 20% of respondents (10/50) are having narrowband kind of internet connection at their home. 8% of respondents (4/50) are having other kind of internet connection at their home.

Problems/issues having with Security measures

Table-8

Options	Number of respondents	Percentage (%) of respondents
They cost money	12	24%
They are time consuming	18	36%
I don't know the risks	15	30%
They reduce user friendliness	5	10%
Total	**50**	**100%**



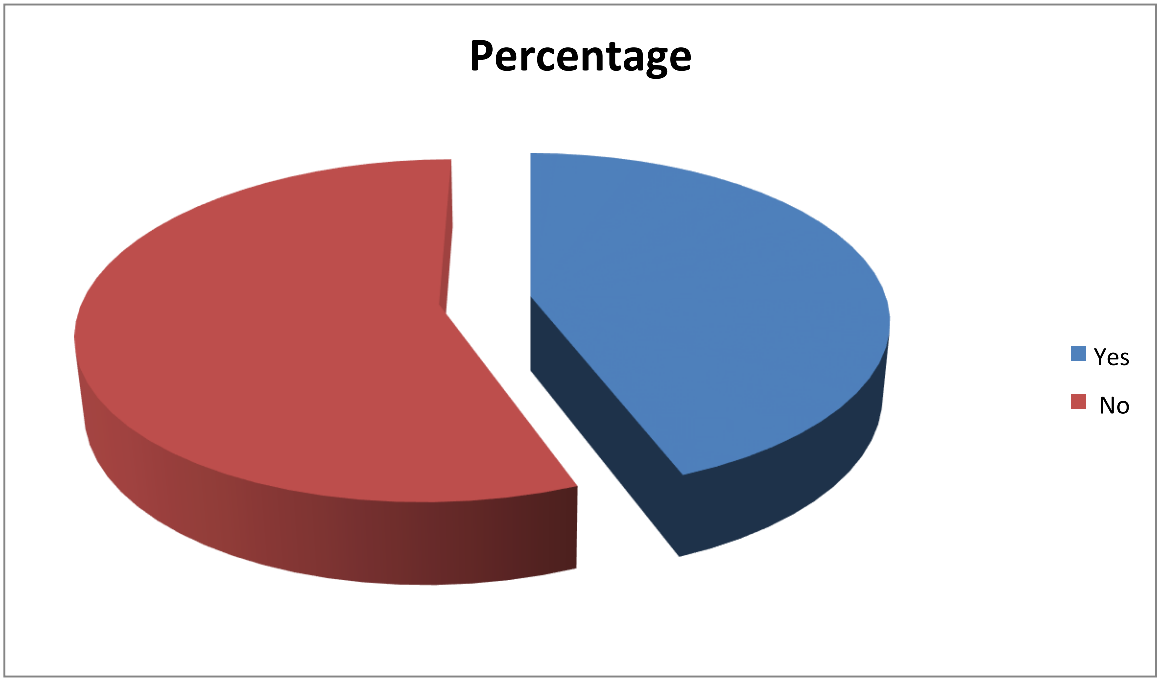
INTERPRETATION

In the above chart it is observed that the 24% of respondents (12/50) are having problem with Security measures is that they cost money. 36% of respondents (18/50) are having problem with Security measures is that they are time consuming. 30% of respondents (15/50) are having problem with Security measures is that they don't know the risks. 10% of respondents (5/50) are having problem with Security measures is that they reduce user friendliness.

Feeling worried about using the Internet

Table-9

Options	**Number of respondents**	**Percentage(%) of respondents**
Yes	22	44%
No	28	56%
Total	**50**	**100%**



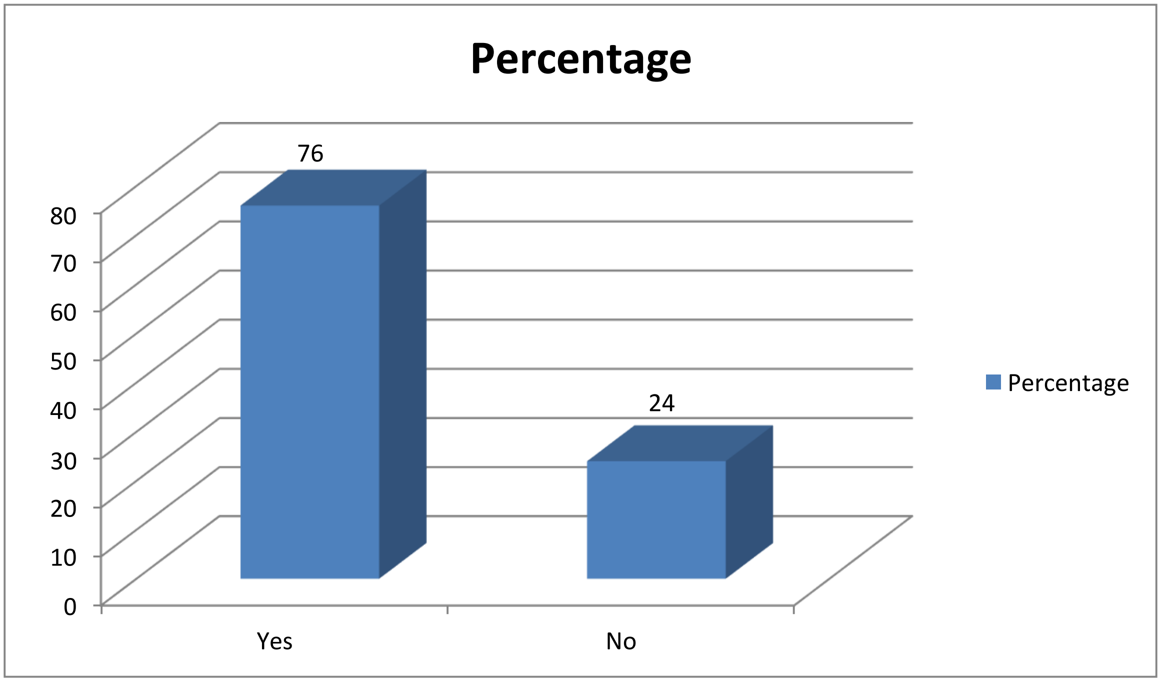
INTERPRETATION

From the above chart it is observed that the44% of respondents (22/50) are feeling worried about using the internet. 56% of respondents (28/50) are not worried about using the internet.

Awareness regarding Criminal legislation on Cyber activities

Table-10

Options	**Number of respondents**	**Percentage (%) of respondents**
Yes	38	76%
No	12	24%
Total	**50**	**100%**



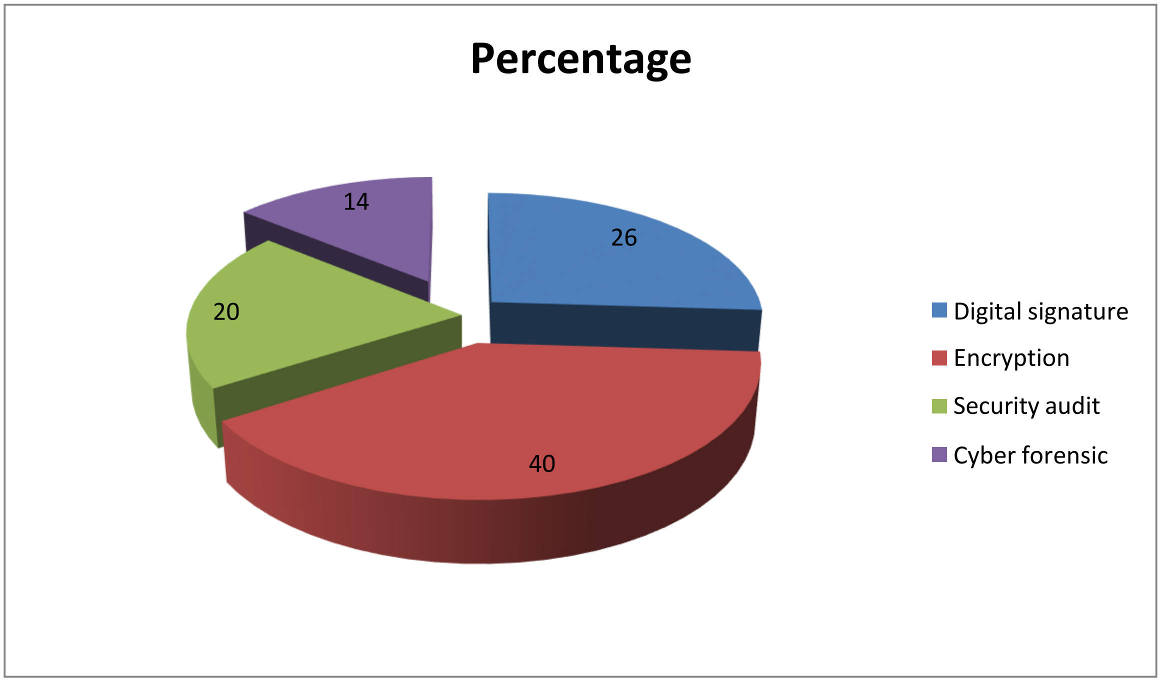
INTERPRETATION

From the above chart it is observed that the 76% of respondents (38/50) are aware of Criminal legislation on Cyber activities. 24% of respondents (12/50) are not aware of Criminal legislation on Cyber activities.

Effective tools to protect against Cyber threats

Table-11

Options	**Number of respondents**	**Percentage (%) of respondents**
Digital signature	13	26%
Encryption	20	40%
Security audit	10	20%
Cyber forensic	7	14%
Total	**50**	**100%**



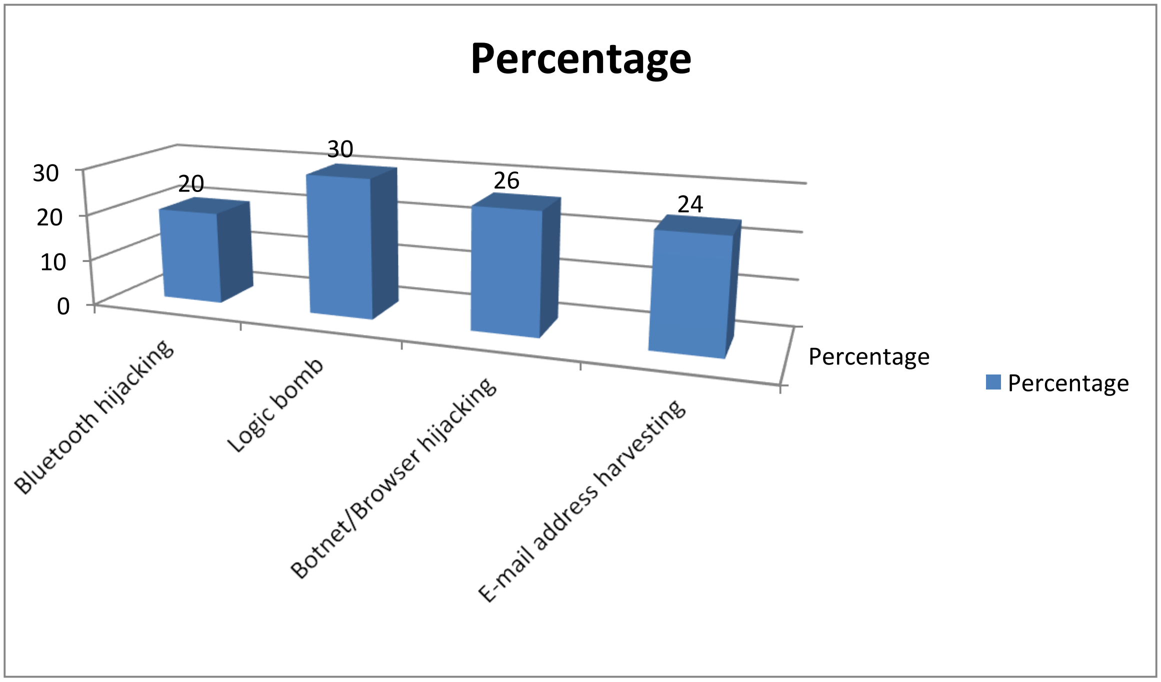
INTERPRETATION

From the above chart it is observed that the 26% of respondents (13/50) saying that Digital signature is an effective tool to protect against Cyber threats. 40% of respondents (20/50) are saying that Encryption is an effective tool to protect against Cyber threats. 20% of respondents (10/50) are saying that Security audit is an effective tool to protect against Cyber threats. 14% of respondents (7/50) are saying that Cyber forensic is an effective tool to protect against Cyber threats.

Types of Cyber attacks

Table-12

Options	**Number of respondents**	**Percentage(%) of respondents**
Bluetooth hijacking	10	20%
Logic bomb	15	30%
Botnet/Browser hijacking	13	26%
E-mail address harvesting	12	24%
Total	**50**	**100%**



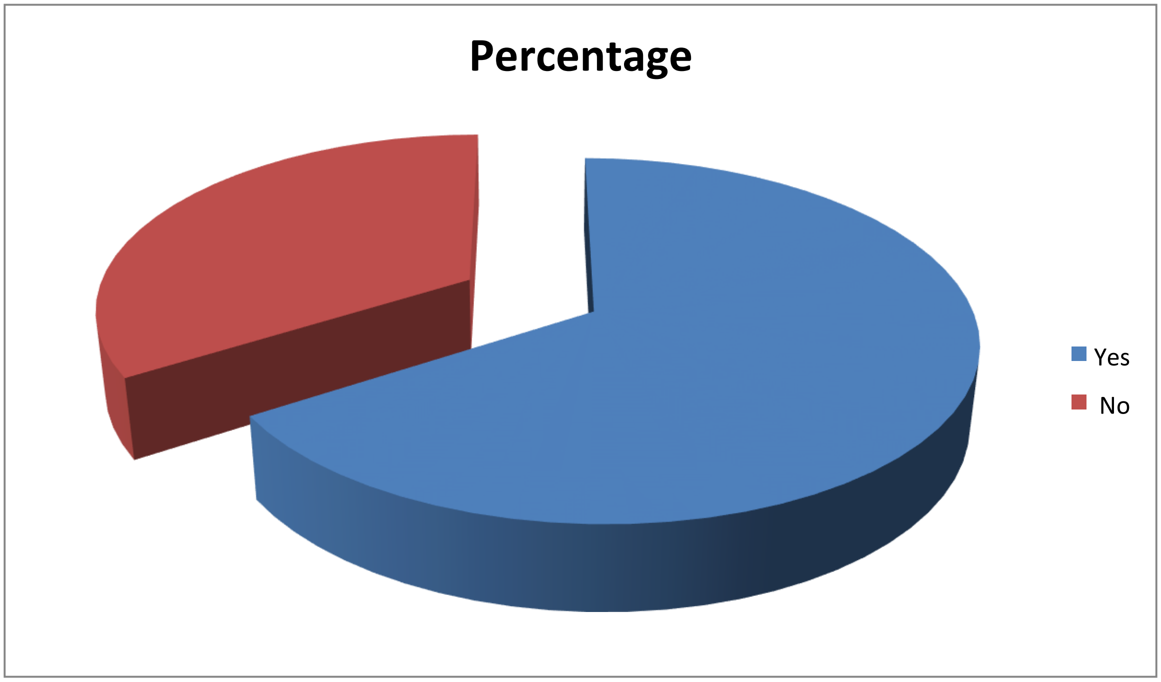
INTERPRETATION

From the above chart it is observed that the 20% of respondents (10/50) know the Bluetooth hijacking type of Cyber attack. 30% of respondents (15/50) know the Logic bomb type of Cyber attack. 26% of respondents (13/50) know the Botnet/Browser hijacking type of Cyber attack. 24% of respondents (12/50) know the E-mail address harvesting type of Cyber attack.

Awareness of current Adhaar card issue

Table-13

Options	**Number of respondents**	**Percentage (%) of respondents**
Yes	33	66%
No	17	34%
Total	**50**	**100%**



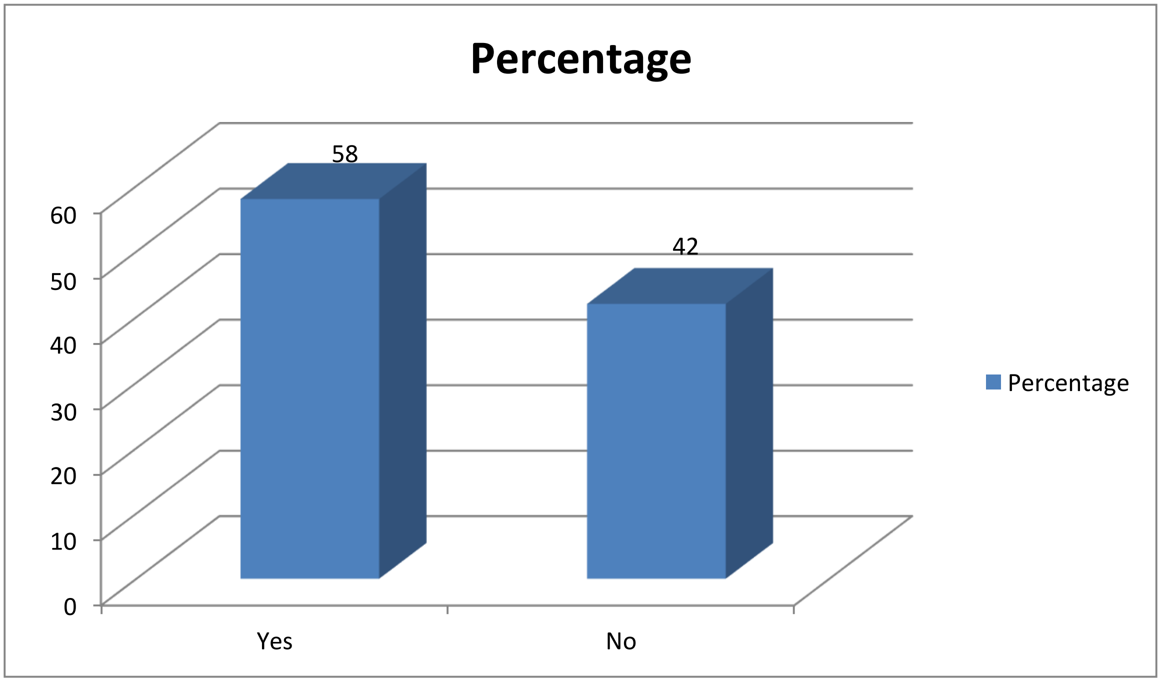
INTERPRETATION

From the above chart it is observed that the 66% of respondents (33/50) are having awareness regarding current Adhaar card issue. 34% of respondents (17/50) are having no awareness regarding current Adhaar card issue.

Mobile device passwords are encrypted and protected

Table-14

Options	**Number of respondents**	**Percentage (%) of respondents**
Yes	29	58%
No	21	42%
Total	**50**	**100%**



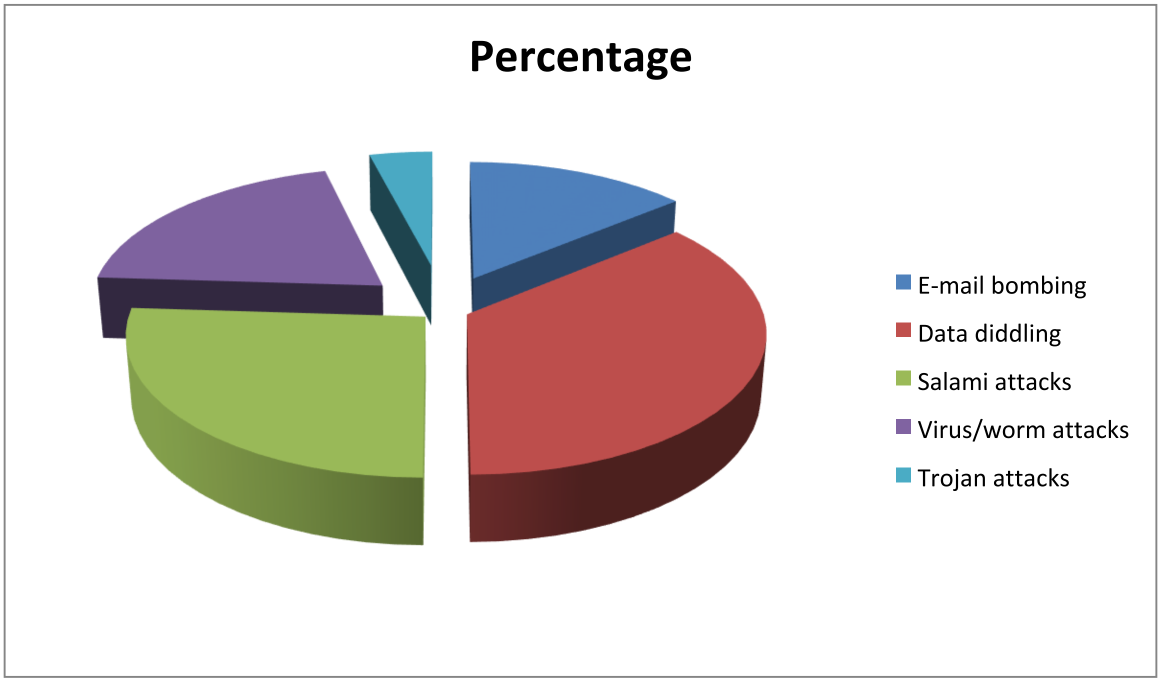
INTERPRETATION

From the above chart it is observed that the 58% of respondents (29/50) are saying that the mobile devices password are encrypted and protected. 42% of respondents (21/50) are saying that the mobile devices password are not encrypted and protected.

Most frequently encountered Cyber crimes

Table-15

Options	Number of respondents	Percentage (%) of respondents
E-mail bombing	7	14%
Data diddling	18	36%
Salami attacks	13	26%
Virus/worm attacks	10	20%
Trojan attacks	2	4%
Total	**50**	**100%**



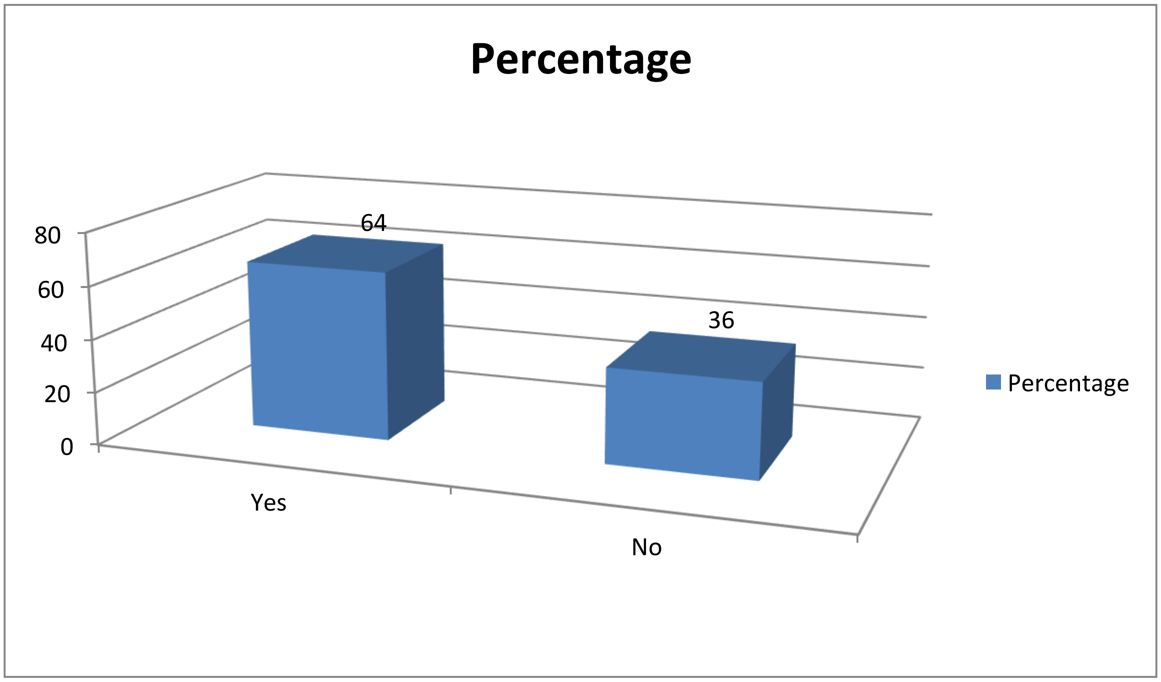
INTERPRETATION

From the above chart it is observed that the 14% of respondents (7/50) are encountered with E-mail bombing Cyber crime. 36% of respondents (18/50) are encountered with Data diddling Cyber crime. 26% of respondents (13/50) are encountered with Salami attacks Cyber crime. 20% of respondents (10/50) are encountered with Virus or worm attacks Cyber crime. 4% of respondents (2/50) are encountered with Trojan attacks Cyber crime.

Awareness of Information Technology (IT) Act, 2000

Table-16

Options	**Number of respondents**	**Percentage(%) of respondents**
Yes	32	64%
No	18	36%
Total	**50**	**100%**



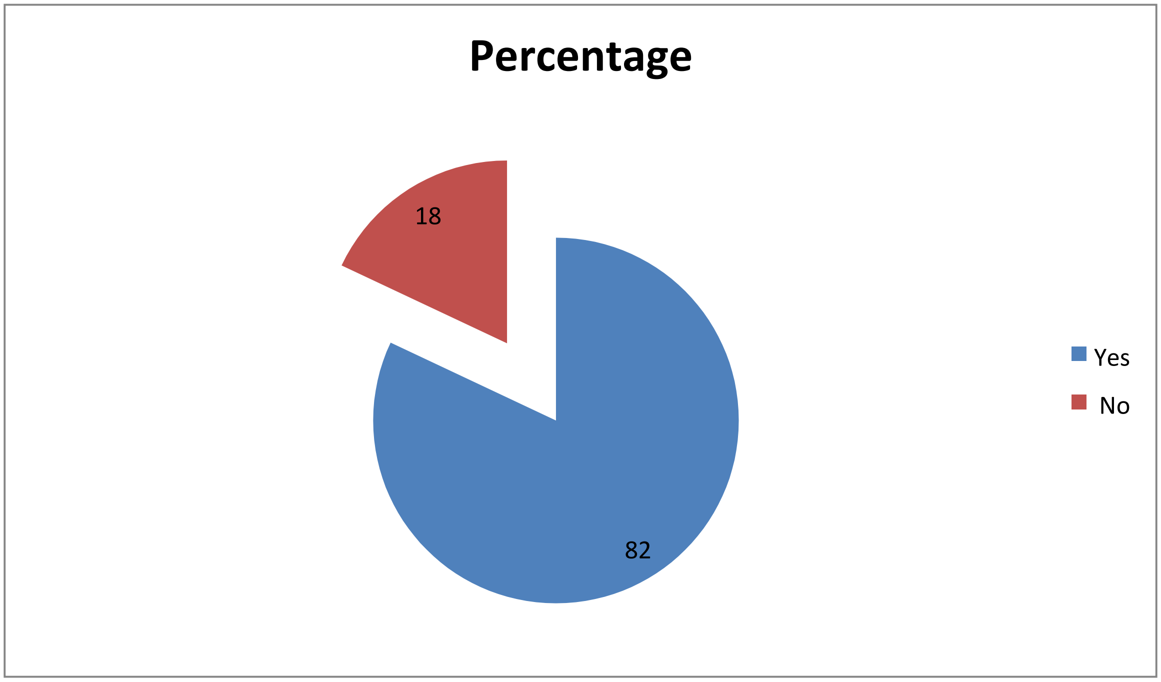
INTERPRETATION

From the above chart it is observed that the 64% of respondents (32/50) are aware of Information Technology Act, 2000. 36% of respondents (18/50) are not aware of Information Technology Act, 2000.

IT Act, 2000 is capable of preventing Cyber crimes

Table-17

Options	**Number of respondents**	**Percentage(%) of respondents**
Yes	41	82%
No	9	18%
Total	**50**	**100%**



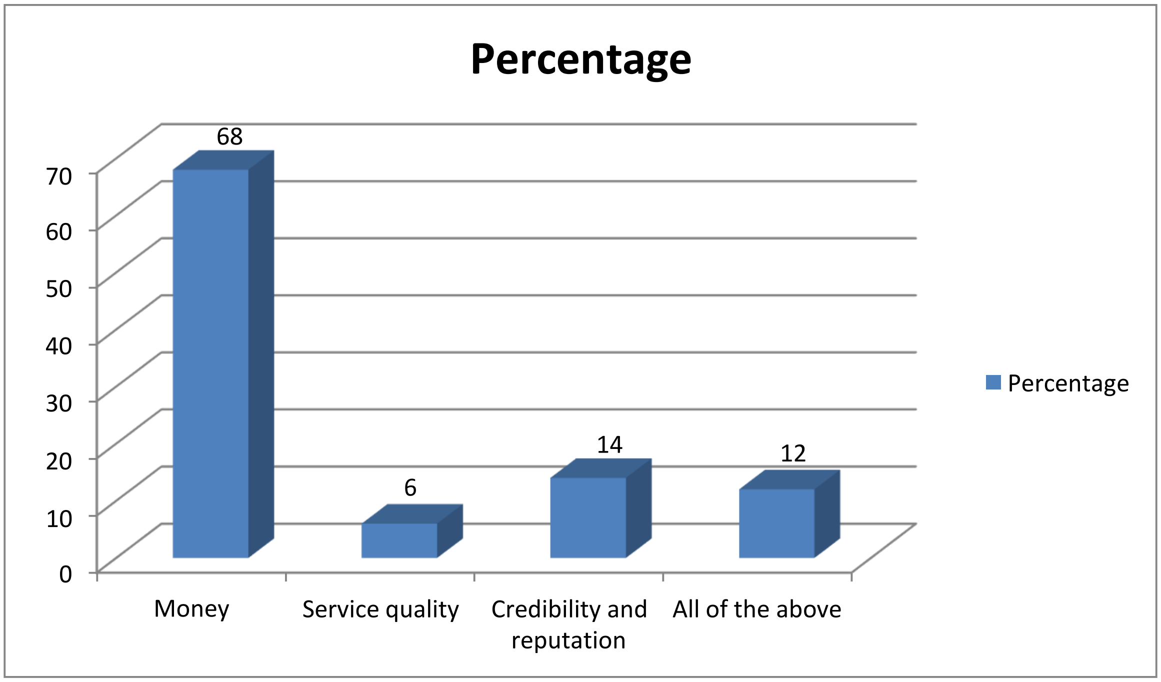
INTERPRETATION

From the above chart it is observed that 82% of respondents (41/50) think that IT Act, 2000 is capable of preventing Cyber crimes. 18% of respondents (9/50) think that IT Act, 2000 is not capable of preventing Cyber crimes.

Most common loss due to Cyber crime

Table-18

Options	Number of respondents	Percentage(%) of respondents
Money	34	68%
Service quality	3	6%
Credibility and reputation	7	14%
All of the above	6	12%
Total	**50**	**100%**



INTERPRETATION

From the above chart it is observed that the 68% of respondents (34/50) are of opinion that the most common loss due to cyber crime is money. 6% of respondents (3/50) are of opinion that the most common loss due to cyber crime is service quality. 14% of respondents (7/50) are of opinion that the most common loss due to cyber crime is credibility and reputation. 12% of respondents (6)/50) are of opinion that the most common loss due to cyber crime is all of the above stated options.

CHAPTER-5

CONCLUSION:

Community in cyberspace is based on the interaction between people. Cyberspace has an important social aspect to it that must not be overlooked. Cyberspace can be treated as a channel touching portion of real space at key points. Ideas are passed through the channel, and business is transacted through this channel. The cyberspace communities are members of the global community interacting on a different plane than in real space.

With the huge growth in the number of Internet users all over the world, the security of data and its proper management plays a vital role for future prosperity and potentiality. It is concerned with people trying to access remote service is that they are not authorized to use.

Rules for compulsory wearing of helmet for bikers by government authorities, has no benefit for them, it is for our own safety and life. Same we should understand our responsibilities for our own cyberspace and should at least take care of safety for our personal devices. These steps include installation of antivirus software and keeping it updated, installing personal firewalls and keeping rules updated. We should monitor and archive all security logs.

We should have backup of important data. Our devices should be protected by passwords and there should be restricted access to sensitive data on our devices. And above all, we should aspire for more computer literacy to understand the safety issues related to our cyberspace. At the same time we need to utilize the specialization of private sector in the field of cyber security and government should promote more PPP projects for the national cyberspace.

CHAPTER-6

Reference

1.Data Privacy and Cybersecurity Risks: India's vast internet user base and digital economy have led to heightened risks of data breaches and cyber attacks. In recent years, cybersecurity breaches exposed sensitive data for millions of users, including health and financial information. Resources like PwC's Global Digital Trust Insights survey discuss the challenges India faces and adaptive approaches, such as machine learning, that organizations can use to strengthen their defenses PwCtps://www.pwc.in/digital-trust-insights-india.html/).

2.India's Cybersecurity Framework and CERT-In: CERT-In, under the Ministry of Electronics and Information Technology, plays a crucial role in responding to cybersecurity threats in India. They provide early warnings, incident response, and guidelines on information security practices. However, there's ongoing concern about the resilience of India's crit
Drishti IASreForumIASecurity weaknesses Drishti IAS, ForumIAS.

3.Impact of Artificial Intelligence on Cybersecurity: AI presents both opportunities and threa
ForumIASd, it improves threat detection and response automation; on the other, it facilitates sophisticated cyber attacks, including phishing and malware creation. The Yojana publication examines how India can integrate AI responsibly to address these evolving challenges ForumIAS.

4. Government Initiatives and Policies: India has launched various initiatives like the National Cybersecurity Strategy and Cyber Surakshit Bharat to promote cybersecurity awareness and build defenses. However, a report by Drishti IAS notes that India needs more cohesive policies and international partnerships to tackle its cybersecurity challenges e
Drishti IAStiHindustan Timesshtiias.com/daily-updates/daily-news-editorials/india-s-cybersecurity-challenge-threats-and-strategies).

5.Emerging Cyber Threats in Digital India: The rapid digitization of sectors such as finance, healthcare, and retail makes India p
PwClnHindustan Timescent rForumIAS
that critical information infrastructure, such as banking and healthcare networks, are frequent targets, making robust cybersecurity essential for national security Drishti IAS, Hindustan Times.

6.www.google.com

7.www.wikipedia.com

8.www.insightsonindia.com/2017/10/19/insights-editorial-safe-cyberspace