deep Sir turnitin Report

by Deep Sir

Submission date: 20-Nov-2021 10:49AM (UTC+0500)

Submission ID: 1708363565

File name: Deep_IT_security_report.docx (3.26M)

Word count: 9288

Character count: 51000

PROJECT REPORT

ON

“CYBER SECURITY ISSUES IN INDIA”

SUBMITTED TO

DEPARTMENT OF COMMERCE

UNIVERSITY COLLEGE FOR WOMEN

KOTI, HYDERABAD.

IN PARTIAL FULFILLMENT FOR THE AWARD OF

BACHELOR’S DEGREE IN COMMERCE

SUBMITTED BY: JATAVATH ARUNA

B.COM (HONORS)

H.T.NO.2016-1866

PROJECT SUPERVISOR

MRS.B.MAMATHA

FACULTY MEMBER

DEPARTMENT OF COMMERCE

TITLE PAGE

NAME OF THE TOPIC	**:**	**CYBER SECURITY ISSUES IN INDIA**
NAME OF THE STUDENT	**:**	**JATAVATH ARUNA**
NAME OF THE COLLEGE	**:**	**UNIVERSITY COLLEGE FOR WOMEN**
YEAR OF THE STUDY	**:**	**2015-2018**
NAME OF THE COURSE	**:**	**B.COM (HONORS)**
HALL TICKET NUMBER	**:**	**2016-1866**
NAME OF THE GUIDE	**:**	**MRS.B.MAMATHA**

CERTIFICATE

This is to certify that **J.ARUNA is** a bonafide student of B.COM (HONORS) III year University College for Women (H.T.NO 2016-1822) and she has worked on the project title **“CYBER SECURITY ISSUES IN INDIA”** under supervision of **MRS.B.MAMATHA**, Department of Commerce, University College for Women, Koti during the year 2016-2018.

Head of the Department

Date:

Place: HYDERABAD

CERTIFICATE BY THE GUIDE

This is to certify the project work titled **"CYBER SECURITY ISSUES IN INDIA"** is bonafide work done by (H.T.NO 2016-1866) OF B.COM (HONORS) III year from University College for Women, Koti, Hyderabad under my supervision.

Signature of the Guide

(Mrs. B. Mamatha)

Date:

Place: Hyderabad

ACKNOWLEDGEMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my project. All that I have done is only due to such supervision and assistance and I would not forget to thank them.

I respect and thank Mrs. B. Mamatha, for providing me an opportunity to do the project work in "CYBER SECURITY ISSUES IN INDIA" and giving us all support and guidance which made me complete the project duly. I am extremely thankful to her for providing such a nice support and guidance, although she had busy schedule.

I would not forget to remember our Principle **Prof.Prashanta Athma**, for their encouragement and heartily thank our **Head of the Department DR. Krishna Chaitanya.**

I am thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staffs of Department of Commerce which helped us in successfully completing our project work.

JAT
AVATH ARUNA

DECLARATION

I, **JATAVATH ARUNA a** student of B.COM(HONORS) III year of University College for Women hereby declare that the project report submitted to college for the award of “Bachelor of Degree in Commerce” is a reward of bonafide work done by me under the guidance of **MRS. B. MAMATHA**, Department of Commerce, University college for Women, Koti.

Name of the Student

(Jatavath Aruna)

Place: Hyderabad

Date:

CONTENTS OF TABLE

CHAPTER-1

INTRODUCTION

In the long haul, information innovation has changed the overall economy and related people and markets in imaginative ways. With data innovation getting the centre stage, nations across the world are investigating various roads with regards to imaginative contemplations for financial new developments and exhaustive turns of events. An increasing percentage of the universe's general population is moving to the web to give, appreciate, learn, and exchange leads. It has also set out new shortcomings and opened entryways for interference.

The organization's wellbeing perils transmit from a wide variety of sources and show themselves in risky activities that target individuals, associations, public structures, and legislatures all simultaneously. Their possessions pass on basic risk to public prosperity, the security of the nation, and the adequacy of the overall associated economy generally. The start of an interference, the character of the culprit, or the motivation for it could be hard to find, and the show might happen from basically anywhere. These credits manage the usage of data innovation for troublesome exercises. Within that limit, advanced insurance perils present one of the most authentic monetary and public security challenges.

The web is such a term that isn't yet totally depicted and, additionally, has no geological prerequisite. It is a term related to the widespread utilisation of the Internet throughout the planet. It is, along these lines, called a "virtual space," as the certifiable presence of the web isn't unmistakable in any way. The web is the general interconnection of people through PCs and media transmission, with little regard for actual geology.

Data through PCs is moved as Ones (1) and Zeros (0), which don't intrinsically give any different data than Ones and Zeros for endorsement. For endorsement purposes, extra data should be passed on close to the web exchanges for character purposes.

Giving additional data in modernised correspondence presents the opportunity for distortion. Since nothing forestalls the transmission of bogus individual data or the duplication of someone else's data. The validity of this issue is highlighted when you consider that future advances will permit fundamental identifiers, like a retinal reach or a wonderful finger impression, to be tended to meticulously. These biometric attributes are acquired in genuine space since they are installed in the genuine body of the individual. This is lost on the web. Similarly, the web necessitates a design that allows people to insist on their characters to others while concealing the motorised portrayal of those characters from them.

DEFINITION

Computerized eventually, data development has changed the general economy and related individuals and markets in creative ways. With information advancement getting to the middle stage, countries across the world are exploring different avenues concerning innovative thoughts for monetary new turns of events and thorough developments. An expanding segment of the universe's overall public is moving to the web to give, appreciate, learn, and trade leads. It has additionally set out new weaknesses and opened entrances for obstruction.

The association's prosperity dangers come from a wide assortment of sources and show themselves in unsafe exercises that target people, affiliations, public constructions, and councils all the while. Their assets, for the most part, pose a serious threat to public well-being, national security, and the sufficiency of the broader economy. The beginning of a stumbling block, the personality of the guilty party, or the inspiration for it may all be elusive, and the show could come from anywhere. These credits deal with the utilisation of information development for inconvenient activities. Inside that cut off, progressive protection hazards present one of the most real money-related and public security challenges.

The web is such a term that isn't yet totally depicted and, in addition, has no geological prerequisite. It is a term related to the widespread utilisation of the Internet throughout the planet. It is, likewise, called a "virtual space," as the veritable presence of the web isn't conspicuous in any way. The web is the inside-and-out interconnectedness of individuals through PCs and media transmission, paying little mind to genuine geography.

Data through PCs is moved as Ones (1) and Zeros (0), which don't intrinsically give any different data than Ones and Zeros for endorsement. For endorsement purposes, extra data should be passed on close to the web exchanges for character purposes.

Giving additional data in modernised correspondence presents the opportunity for distortion. Since nothing forestalls the transmission of bogus individual data or the

Duplication of another person's information The legitimacy of this issue is highlighted when you consider that future advances will allow crucial identifiers, similar to a retinal reach or a ground breaking finger impression, to be tended to fastidiously. These biometric ascribes are gained in authentic space since they are introduced into the certified body of the person. This is lost on the web. Also, the web requires a plan that permits individuals to demand their characters from other people while hiding the mechanised depiction of those characters from them.

DEFINITION

Mechanized affirmation is the security of data and its giving channels as applied to taking care of gadgets like PCs and progressed cells, just as PC affiliations like private and public affiliations, recollecting the Internet overall.

The field covers the cycles as a whole and parts by which PC-based gear, data, and applications are defended from impromptu or unapproved access, change, or obliteration. PC security likewise provides protection against unforeseen and sad occasions.

Association affirmation is an astonishing issue that cuts across various districts and calls for multidimensional, complex drives and reactions.

It has been a test for states, starting with one side of the planet, then moving onto the next. The errand is made bothersome by the basic and diffuse nature of the dangers and the powerlessness to spread out a sufficient reaction with zero trace of critical wrongdoers. The speed of progress in data innovation (IT) and the overall ease with which applications can be upheld has seen the utilisation of the web extend on a very basic level in its smaller presence. From its fundamental picture as a N/W created by scholastics for the utilisation of the military, it has now changed into a general trade stage for money-related issues as well as for business and social purposes.

The developing centrality of the web to human life is exemplified by the unrefined numbers brought out by the International Telecommunications Union (ITU), as indicated by which

Somewhere in the range of 2005 and 2010, the quantity of Internet clients dramatically increased, outperforming 2 billion.

Clients have been interfacing through a scope of gadgets, from the PC to the remote, and utilising the Internet for an assortment of purposes, from correspondence to electronic business to information hoarding, for a surprisingly long time.

The improvement of the Internet has inferred that, while the natural dangers and deficiencies of the Internet have remained by and large unaltered, the likelihood of obstruction has increased in lockstep with the advancement in the number of clients. While such disrupting impacts can't cause exceptionally durable or shocking naughtiness all over the planet, they do serve as an idea to the specialists pushed to start measures to work on the security and adequacy of the web, considering everything. State-show associations are compelled in their reactions to pressures applied by politico-military-public security entertainers toward one side and cash-related typical society entertainers on the other.

.

Extent OF THE STUDY:

To comprehend the mindfulness among people in general with respect to network protection issues in India, The review is limited to the 50 respondents who were arbitrarily chosen in the twin urban communities of Hyderabad and Secunderabad.

Approach

Sources of information collection:

Essential information

Optional information

Essential DATA:

The principal wellspring of essential information is a poll comprising of straightforward inquiries arranged and dispersed to respondents for an assortment of information on mindfulness out in the open with respect to web indexes.

Optional DATA:

The primary wellspring of optional information incorporates books, magazines, newspapers, articles, journals, and sites.

Test SIZE:

For the current review, 50 respondents were chosen aimlessly.

- Impediments to the Study
- The review is directed at Hyderabad and Secunderabad, as it were.
- The review is confined to the clients of the web index, as it were.
- Time considerations are also a factor in limiting the scope of this review.

INDIAN CYBER SPACE

The National Informatics Center (NIC) was set up ahead of schedule in 1975, fully intent on giving IT answers to the public authorities.

Somewhere between 1986 and 1988, three N/Ws were set up:

The India PC Foundation, which incorporated the IBM centralised server establishments that comprised the India PC foundation;

NICNET (the NIC Network), a cross-country tiny gap terminal (VSAT) N/W for public area associations, as well as to connect the central government with state legislatures and neighbourhood organizations.

The Education and Research Network (ERNET) serves the scholastic and exploration networks.

For example, the New Internet Policy of 1998 made ready for a considerable length of time specialist organisations (ISPs) and saw the Internet client base develop from 1.4 million in 1999 to more than 15 million by 2003.

Indian presence on the Internet/Avenues of weakness in Cyber Space/Indian stakes in danger in Cyber Space

According to the World Bank report,

By June2012, Internet clients in India were approx. 12.5% of the absolute populace (approx. 137 million).

As indicated by the Internet and Mobile Association of India (IAMAI),

The web client base in India is projected to reach 243 million by June 2014, with a year-on-year development of 28%.

This dramatic development is again expected to proceed in late future with an ever increasing number of individuals getting to the web through cell phones and tablets, with the public authority not really settled push to increment broadband(>4mbps) infiltration from its current degree of around 6%.

Public e-Governance Plan (Ne G P)

Despite the fact that the Indian government was a late believer in computerization, there has been an expanding push for e-administration, considered a savvy method of taking public administration to the majority of the nation.

For example, basic areas like [3] defence, energy, finance, space, telecommunications, transport, land records, public essential services and utilities, law enforcement, and security all undeniably rely upon N/Ws to transfer information, for correspondence purposes and for business exchanges.

The National e-administration Program (Ne GP) is one of the most aspiring on the planet and looks to give in excess of 1200 legislative administrations on the web. Plans such as the Rajiv Gandhi [5] broadband-to-PRIs plot and the National Optic Fiber Network (NOFN) mission are currently devoted to accelerating digital availability in vast areas of the country.

Under The National Broadband Plan, the objective for broadband is 160 million families by 2016. In spite of the low numbers according to the populace, Indians have been dynamic clients of the Internet across different fragments.

Comparative degree of infiltration has additionally been found in the long range informal communication field, which is the latest participant to the digital stage. India presently has the quickest developing client [3] base for Facebook and Twitter, the two top informal communication locales.

CHAPTER-2

Cyber Threats of Various Types

As we become more reliant upon the Internet for our every day exercises, we likewise become more powerless against any interruptions caused in and through the internet. The speed with which this area has developed has implied that states and privately owned businesses are as yet attempting to sort out both the extension and which means of safety in the internet and allocating liability.

Digital dangers can be disaggregated, in light of the culprits and their thought processes, into four bushels:

1. Cyberespionage
2. Computer Fraud
3. 3rd. Cyberterrorism
4. 4rd. cyberwarfare

Digital Espionage:

Advanced observation is the display or practise of obtaining preferred intel (individual, tricky, prohibitive, or of a portrayed nature) without the consent of the holder of the information (individual, tricky, prohibitive, or of a portrayed nature) from individuals, competitors, rivals, get-togethers, state-run organizations, and enemies for individual, financial, political, or military advantage, utilising systems on the Internet, associations, or individual PCs utilising breaking techniques and dangerous programming, including Trojan h

I recently said, "Cyber covert work is the use of PC associations to secure unlawful induction to characterised information, consistently that held by an organisation or other affiliation."

Digital India: A Victim of Chinese Cyber Espionage?

1. The advanced assault by Chinese saltines on the PCs in the Prime Minister's Office (PMO) was addressed in 2009. In August 2015, security firm Fire Eye uncovered a preposterous movement of engineers organised in China, especially enraptured by parts and affiliations related to the Indian

government, as reflected in data on Tibetan activists. The high-level surveillance bundle sent doled out stick phishing messages to its organised misfortunes, with Microsoft Word affiliations containing data on neighbourhood strategy-driven issues. It said that get-together understanding of India remains a fundamental key objective for China-based APT social affairs, and these assaults on India and its associated nations reflect an interest in its worldwide concerns.

Computerized Crime and Cyber Attacks:

A computerised attack is any type of hostile move used by individuals or entire organisations that targets PC information structures, establishments, or PC networks with the intent of harming or obliterating a specific PC association or system.

Depending on the specific circumstance, scale, and truth of the assaults, these assaults can be referred to as "advanced missions," "computerized engaging," or "computerized mental battling. "Progressed assaults can go from introducing spyware on a PC to endeavouring to annihilate whole countries' principal frameworks.

The extending web has demonstrated a bright hunting ground for computerised crooks, with incidents because of advanced bad behaviour running into billions of dollars all throughout the planet.

While various countries are uncovering colossal mishaps due to cutting-edge terrible conduct, for example, dangers to attempts and crucial data foundations (CII), there are no such reports emerging out of India other than those related to automated perception.

In any case, the report of the National Crime Records Bureau (NCRB) in 2010 uncovered an expansion of half in cutting-edge awful conduct over the prior year, albeit the numbers were minuscule in totally terms.

On July 12, 2012, a prominent ongoing assault penetrated the email records of around 12,000 individuals, including those of experts 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) communicated that his association alone needed to impede up to ten assigned attacks a day.

Advanced Terrorism

Shows of terrorism related to the web as well as executed using cyber technology are commonly known as advanced mental fighting.

Implications of advanced mental mistreatment

Modernized mental mistreatment is the mix of unlawful threatening and the web. It is generally understood to mean unlawful assaults and threats of assaults against PCs, affiliations, and data saved in that when done to frighten or compel an association or its family in the progression of political or social destinations, Further, to qualify as automated mental battling, an assault should accomplish viciousness against people or property, or, once more, if nothing else, cause sufficient shrewdness to cause dread. Genuine assaults on fundamental foundations may be evidence of cutting-edge illegal threatening, depending on their impact.

This is potentially the most comprehensive meaning of "advanced mental mistreatment." Nonetheless, even this has a limit. It means that in order for an attack to be classified as computerised unlawful terrorizing, it must incite violence. This is more conventional. A mental aggressor may facilitate an attack just to upset key organizations. If they make an alert by attacking fundamental structures or establishments, there is no necessity for it to incite brutality. Honestly, such attacks can be more unsafe.

Over the last few decades, India has cut a forte for itself in IT. Most of the Indian monetary industry and money-related foundations have acknowledged IT to its fullest smoothing out. Reports recommend that advanced attacks are legitimately organised toward monetary and

establishments dealing with moneyGiven the growing dependence of the Indian money-related and financial establishments on IT, a computerised attack against them might provoke an unsalvageable breakdown of our monetary plans. Moreover, without a doubt, the most unnerving thought is the ineptitude of relative courses of action or the deficiency of decisions.

Computerized Warfare

The fifth space of battling the progression of advancement impacts the possibility of dispute and war. Computerized warfare is an astoundingly late yet propelling characteristic.

Without implying the conventional meaning of "computerized battling," we can [3] define it as exercises by a nation's state or its agents to infiltrate another nation's PCs or associations for the purposes of observation, mischief, or interference. These threatening exercises against a PC structure or N/W can take two forms: advanced cheating and computerised attacks.

types of security threats:

Cybercrime incorporates unequivocal bad behaviour overseeing PCs and associations, for example, hacking, phishing, and the facilitation of regular bad behaviour utilising PCs (youth sexual diversion, scorn infringement, selling/web blackmail).A short preface to some typical advanced related encroachments, or cybercrimes, as they are generally more consistently insinuated, is analysed underneath:

Hacking

Hacking, in direct terms, infers an unlawful interference in a PC system just as much as association. For instance, there is a practically identical term to hacking, for instance, breaking, yet as indicated by the Indian genuine [1] perspective, there is no qualification between the terms hacking and breaking. Each act submitted towards breaking into a PC is a form of hacking. Software engineers form or use momentary PC ventures to attack the true PC.

.

Young person Pornography

The The Web is, for the most part, utilised for the sexual maltreatment of youngsters. As more homes approach the web, more youngsters are getting on it, and this chips away at their inadequacy in falling misfortunes to the hostility of pedophiles. Pedophiles (individuals who are physically drawn to kids) bait kids in by appropriating unequivocal material and, afterward, seek them out for sexual maltreatment. Part of the time, paedophiles contact young people in visit rooms, acting like youths or any kind of future family of a relative age; they win the conviction of these youngsters, and from there on, they start really provocative conversations. Then, at that point, starts the veritable abuse of youths.

Progress Stalking

This term is utilised to recommend the utilisation of the web, email, or other electronic gadgets explicitly intended to follow someone else. Modernized after can be characterised as a high-level criminal's rehashed presentations of tormenting or compromising conduct towards the misfortune using the web.

Refusal of Service

This is a progression-driven, automated obstruction where the robust floods the trade speed or squares the clients' sends with spam, denying the client authorization to utilise the Internet and the associations there from. A DoS attack (for what it's worth, generally known) can be executed in various ways.

Scattering of Malicious Software (Malware)

Malware is depicted as programming that wants to play out an undesirable unlawful appearance through the PC affiliation. It can also be portrayed as programming with malicious intentions.Malware can be mentioned depending on how it is executed, how it spreads, and what it does. Some of them are talked about under.

A) Disease

An illness is a programme that can debase different endeavours by transforming them to intertwine with a potential further developed duplicate of itself. A taint can spread all through a PC or organization, utilising each client's endorsement to dirty their program. Each soiled programme may, in like manner, be spread as an infection, and thusly, the contamination will increase. Sickness has a tendency to sway programme records.

In any case, every so often they also sway information records, disturbing the utilisation of information and destroying them totally.

b) Worms

Worms are also spread through computer networks; unlike defilements, PC worms are poisonous endeavours that duplicate themselves, beginning with one structure and progressing to the next, rather than infiltrating legitimate reports. For example, a mass-mailing email worm is a worm that sends duplicates of itself through email. An affiliation worm then, at that point, duplicates itself all around an affiliation, upsetting the entire affiliation.

c) The Greeks

A Trojan is a type of malware that performs actions that are not normal for the customer. A Trojan, or redirection, is a programme that, generally, impairs the security of a structure. Trojans are utilised to make optional entries (a programme that permits outside access into a safe association) on PCs that have an association with a protected association so a developer can move toward the safe association. Unlike contaminations, Trojan horses don't repeat themselves, but they can be similarly ruinous. One of the most misleading sorts of Trojan horses is a programme that professes to clean your PC, but rather introduces diseases to it.

d) Hoax

A scam is an email that cautions the client of a specific framework that is hurting the PC. The message from there on educates the client to run a method (frequently as a download) to address the hurting framework. When this programme is run, it attacks the framework and erases a significant record.

e) Spyware

Spyware attacks a PC and, as its name suggests, screens a client's exercises without assent. Spyware is generally sent through clueless messages with bonafide email i.ds. Spyware keeps on contaminating a great many PCs around the world.

f) Phishing

Phishers bait clients to a fake site, generally by sending them a convincing email. Once at the phoney site, clients are fooled into revealing an assortment of private data, for example, passwords and record numbers.

Cyber Security Issues In India:-

The Current And Present Dangers Of Aadhaar Hacking

Digital protection is a confounded field to oversee, and surprisingly, the most impassioned players in network safety know that outright network safety is a fantasy. So, if someone claims that his/her framework, programming, or venture is 100% digitally secure, he/she is essentially oblivious to the ground realities of the internet.

Digital fighting was once thought to be a fantasy rather than a reality. Yet, with developing rates of digital reconnaissance, digital illegal intimidation, and even digital fighting, nations have begun to view their basic frameworks in a serious way. In any case, the assignment to get these basic foundations is close to incomprehensible as the troublemakers are consistently many strides in front of the public authority and its offices.

Aadhaar is one such profoundly delicate and exceptionally unreliable undertaking of the Indian government that is neither reasonable nor secure. It just has a misguided feeling of safety that the administration is projecting to redirect the consideration of pundits to Aadhaar. Yet, genuine network safety experts are very much aware of the risks of the Aadhaar project that have placed the lives and properties of Indians in extraordinary hazard.

In reality, Aadhaar has created genuine established inconsistency and irreversible digital security that will consistently jeopardise law and order as well as the individual wellbeing and security of Indians .Regardless of what the Indian government tells you, avoid Aadhaar. Also, if

If you have successfully created an Aadhaar, you should deseed it from all administrations and square your biometrics as soon as possible so that it cannot be misused by the government or private individuals

Portable Cyber Security in India is Needed Under Digital India

Mobile phones are accepted to play a significant part in the effective execution of the Digital India venture of the Indian government. From mobile business to mobile banking, the Indian government is betting big on mobiles and their use for public administration conveyance through electronic means. Obviously, this large-scope utilisation of mobile phones will also bring about digital law and network safety issues, which the Indian government should be totally ready to manage in the future.

Cell phones have become omnipresent nowadays. They are utilised for a considerable length of time, going from individual use to portable banking. Digital thugs have also realised the importance of cell phones in committing digital crimes and financial fraud. This is also the reason malware researchers are creating cell phone specific malware to take advantage of.

secrets and touchy data.

Portable digital protection in India has turned into a reason for concern nowadays. Cell phones are presently being proposed to be utilised for portable banking and versatile administration in India.

Normally, we should guarantee powerful and versatile network protection in India. An electronic

The validation strategy of India can help with more dynamic and secure portable utilisation in India. Portable administration and e-verification are also inextricably linked in India, and with the proposed electronic conveyance of administrations in India, this is likewise an absolute requirement. Until further notice, we have no implementable electronic conveyance of administration strategy in India, but it could be in the pipeline. The Indian government is working toward guaranteeing electronic conveyance of administrative functions in India. Truth be told, a lawful structure named the Electronic Conveyance of Administrations Bill 2011 (EDS Bill 2011) was likewise proposed by the Indian government previously. The equivalent has yet to be turned into an appropriate law in India. When the EDS Bill 2011 becomes material, states across India will offer electronic types of assistance through different modes, including cell phones. This requires placing a hearty and dependable portable security foundation in India.

However, using cell phones for business and personal communications in India is also risky.For example, portable banking in India is hazardous as the current banking and other innovation-related lawful systems are not helpful for versatile banking in India. Additionally, we don't have an all-around created e-administration framework in India. Accordingly, India is as yet not prepared for m-administration. We at Perry4Law Organization (P4LO) believe that the most significant barriers to versatile related uses in India are the use of weak encryption principles and the non-use of portable network security systems in India. The absence of encryption laws in India has also made portable security in India extremely weak. Malware that is constantly evolving and versatile is adding to the burdens of portable clients all over the world. As of now, malware is easily overcoming digital security items and administrations.

It is about time for India to truly work upon versatile network protection angles quickly. The strategy choices in such a manner should be taken critically and should be executed at the earliest opportunity.

CHAPTER-3

Digital Laws in India

The rule progress based law in an incredibly extensive time frame was the Indian Telegraph Act of 1885. This law was fanned out with the procedure of the message and later covered another movement being created, the telephone.

In the space of progress driven law, the Information Technology Act, 2000, turns out to be conceivably the main element. While the Information Technology Act is the fundamental Act keeping an eye out for the web in India, there are countless various Acts that would apply to control and direct exchanges and trades on the web. Take, for instance, web based blueprints. Other than the material outlines of the IT Act, the Indian Contract Act, the Sale of Goods Act, 1930, etc, would be relevant to picking the valines of such blueprints.

Besides, the plans of the Competition Act, 2002, or, by virtue of insane trade rehearses, the Consumer Protection Act, 1986, would be significant. The proportion of got improvement available on the Internet is no doubt wonderful of the day. Be it books, films, music, PC programming, redesigns, conditions, plans, everything is open on the net. Affirmation of copyright brand names online would fuse the conjuring of the Indian Copyright Act and the Trade Marks Act.

To the degree criminal technique on the web, alongside unequivocal plans in the IT Act that censure them, incalculable different Acts would oversee them. For example, by virtue of Internet investigation, contemplating the twisting executed, acts like the Companies Act, 1956, will much of the time be reasonable. Hence, it will still up in the air that while the IT Act is the quintessential Act controlling conduct on the Internet, subject to the current real components of a case or the shot at a trade, no not exactly a few Acts may be appropriate. Hence, electronic laws harden the whole course of action of endorsements that can be applied to pick straightforwardly on the Internet.

The Data Technology Act of 2000

The Information Technology Act of 2000 strategies legitimize electronic business and e-association and work with its advancement as a choice to paper-based standard systems.The Act has embraced an important corresponding methodology where paper-based necessities like reports, records, and stamps are supplanted by their electronic accomplices.

The Act endeavors to ensure this advancement being developed by portraying encroachment, recommending disciplines, putting down methods for appraisal, and laying out definitive wellinformed authorities. Different electronic awful practices have been submitted to the significance of standard encroachment too through changes to the Indian Penal Code, 1860. The Evidence Act of 1872 and the Bankers' Book Evidence Act of 1891 have also been fittingly corrected to work with a gathering of affirmation in battling electronic encroachment.

Public Cyber Security Policy, 2013

To further develop the country's IT areas, the Indian Government gave the National Cyber Security Policy of India 2013 of every 2013, except its actual execution is still lacking.Subsequently, endeavors like e-association and web business are at this point perilous and may require progressed security sooner rather than later.Its basic parts include:

- to make a strong and exceptional web.
- Building a strong progressed regular structure cultivates trust in IT exchanges.
- The 24 x 7 NATIONAL CRITICAL INFORMATION INFRASCTRUCTURE PROTECTION CENTER (NCIIPC)
- Nearby innovative plans (Chinese things and dependence on new programming)
- testing of ICT things and avowing them. Embraced things
- Making a labor force of 500,000 instructed specialists
- monetary related benefits for finance chiefs who perceive standard IT enters, and so on

Tireless undertakings in India

The public experts have driven a few thought and organizing programs on robotized infringement for law underwriting workplaces, investigating those for the use of motorized real sciences programming social affairs and the related methods to gather verification from the space of awful conduct.

Noteworthy planning programs have moreover been centered around the legitimate relationship to show them on the creatively genuine bits of state of the art infringement similarly as the evaluation of mechanized verification presented before them.Both the CBI and many state police affiliations are today equipped to oversee cybercrime through express modernized horrible direct cells that they have set up.

In India, there are colleague workplaces.

Countering progressed encroachment is a coordinated exertion as for two or three working environments in the Ministry of Home Affairs and in the Ministry of Communications and Information Technology. The law-execution work environments like the Central Bureau of Investigation, the Intelligence Bureau, state police affiliations, and other express affiliations like the National Police Academy and the Indian Computer Emergency Response Team (CERT-In) are the unmistakable ones that tackle electronic awful practices. We'll see the measure of them there are:

Countering progressed encroachment is a coordinated exertion as for two or three working environments in the Ministry of Home Affairs and in the Ministry of Communications and Information Technology. The law-execution work environments like the Central Bureau of Investigation, the Intelligence Bureau, state police affiliations, and other express affiliations like the National Police Academy and the Indian Computer Emergency Response Team (CERT-In) are the unmistakable ones that tackle electronic awful practices. We'll see the measure of them there are:

1.The National Information Board (NIB)

The Public Information Board is a zenith relationship with delegates from gigantic divisions and working environments that plan part of the foremost data framework in the country.

2. The National Crisis Management Committee (NCMC).

The National Crisis Management Committee (NCMC) is a faultlessness of the public power of India for supervising major emergency scenes that have veritable or public repercussions. It will similarly administer public emergencies happening because of allotted progressed attacks.

3. Public prosperity Council Secretariat (NSCS)

The National Security Council Secretariat (NSCS) is the summit of a coalition investigating the political, monetary, energy, and fundamental security stresses of India and goes likely as the secretariat to the NIB.

4. Data Technology Division (DIT)

The Division of Information Technology (DIT) is under the Ministry of Communications and Information Technology, Government of India. DIT attempts to make India a general driving player in information movement, meanwhile taking the possible increments of information progression to separating social conditions by drawing in a pulled in and expansive society. It is faulted for the undertaking of managing all issues identified with headings and procedure in stuff and IT.

5. Broadcast interchanges Division (DoT)

The Division of Telecommunications (DoT), under the Ministry of Communications and Information Technology, Government of India, is fit to sort everything out with all ISPs and expert centers concerning network security scenes and response rehearses as seen by CERT-In and other government affiliations. Spot will give rules for private master networks' occupations and obligations, similarly as confirmation that these master affiliations can stick to the crucial optical fiber networks for unsurprising availability and have methodologies for substitute coordinating in the event of genuine attacks on these affiliations.

Examples of cyber-attacks

huge no. There are so many digital assaults that some of the well-known ones are included.

1. In 2014, Sony Pictures Entertainment became the target of the greatest digital assault in US corporate history, connected to its arrival of the North Korea parody "The Interview," loathed by Pyongyang.
2. The past year saw an overwhelming assault on Ukraine's basic framework.

Known cases of digital assaults and digital fighting:

Insightful digital assaults and digital government assistance are displayed in table 1.

Table-1

Year	Case
2010	Iran was assaulted by the Stunt worm, thought to explicitly focus on its Natanz atomic improvement office. The worm is supposed to be the most developed piece of malware at any point in time and essentially builds the profile of cyber warfare.
2009	Digital warfare Operation Aurora is a digital assault that started in mid-2009 and proceeded through December 2009. The assault was first openly unveiled by Google in January 2010, and was widely accepted to have begun in China. The assault has been focused on many different associations, of which Adobe Systems, Juniper Networks, and Rackspace have freely affirmed that they were
2009	Targeted .a series of written digital assaults on major government, news media, and financial sites in South Korea and the United States While many thought the assault was coordinated by North Korea, one analyst followed the assaults to the United Kingdom.
2008	A digital covert operative organization, named Ghost Net, utilizing servers predominantly situated in China, has taken advantage of ordered records from government and private associations in 103 nations, including the PCs of Tibetan exiles, yet China denies the case.
2007	The US government experienced an undercover Pearl Harbor in which an obscure, unfamiliar power broke into the super advanced offices in general, the tactical organizations as a whole, and downloaded terabytes of data.

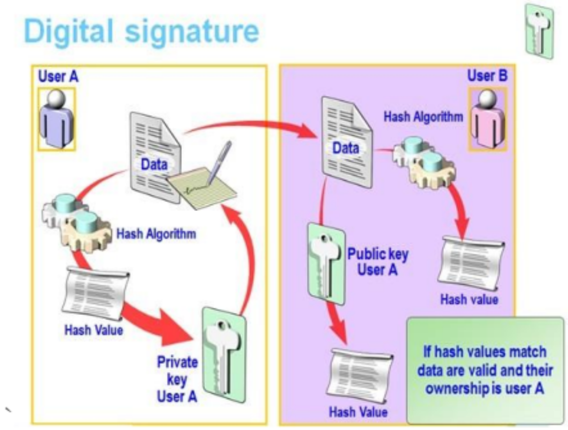
Source: www.thehansindia.com

Instruments for protecting against digital threats

Other Aside from the overall utilization of antivirus, firewalls and entries, solid passwords, secure Wi-Fi affiliation, planning to be a netizen, etc., there are not many different practices that shield our data and association from computerized dangers. Some of them are referred to underneath: :

Progressed Signatures

A high level imprint is a strategy by which it is reasonable to get electronic data determined to recognize the originator of the data, just as the steadfastness of the data. This methodology of ensuring the beginning and unwavering quality of the data is, also, called "check." The legitimacy of different genuine, cash related, and different reports is obliged by the presence or nonappearance of an upheld, truly formed engraving. For a modernized message design to supplant the certified vehicle of paper and ink documents, truly made engravings ought to be uprooted by cutting edge marks. A general engraving is just a procedure that can be utilized for various endorsement purposes. For an E-record, it comes exceptionally near the standard formed with hand marks. The client himself/herself can convey an essential pair by utilizing express crypto programming. At this point, Microsoft IE and Netscape permit clients to make their own key sets. Any individual might make an application to the attesting master for issue.



- **Encryption**

Perhaps the most phenomenal and fundamental security methodology in PC structures is to encode delicate records and messages exceeding everyone's expectations that. Cryptography has a long and striking history. All around, four social gatherings of people have used and dealt with the distinctive strength of cryptography: the military, the political corps, diarists, and dears. The military has had the most delicate effect and has delineated the field.

As of now, data and information security will have a principle impact in the security of the country, the security of the corporate locale, and, furthermore, of each individual working for individual advantage. The message or information to be blended, regardless, called the plaintext, is changed by a cut off that is portrayed by a key. The yield of the encryption correspondence, known as the code message, is then sent through the problematic correspondence channel. The particular strength of breaking figures is called cryptanalysis. The assessment of figures (cryptography) and breaking them (cryptanalysis) is all over known as cryptology. It is finished with their assistance.

To some degree very few of the tremendous number of evaluations [1] are the Secret-Key Algorithm, Data Encryption Standard (DES), Public Key Algorithms, the RSA Algorithm, and so forth

Security Audit

A security review is a cognizant assessment of the security of an association's data framework by evaluating how well it adapts to a bunch of set standards. It is to find the weaknesses in an association's IT framework that it is working. A careful review typically evaluates the security of the framework's certified plan and climate.

Computerized Forensics

Computerized Forensics is a fundamental instrument in the assessment of advanced infringement. Computerized legitimate sciences refers to the exposure, assessment, and amusement of verification isolated from any part of PC systems, PC associations, PC media, and PC peripherals that permits experts to address bad behaviour.

Chief worries with PC [17] crime scene investigation include: imaging stockpiling media, recuperating erased documents, looking through slack and free space, and safeguarding the gathered data for prosecution purposes. The other issue is network criminology, which is an especially difficult aspect of digital legal sciences. It assembles computerised proof that is appropriated across enormous scales of complexity.

The e-disclosure

The e-disclosure examination incorporates regions like illegal tax avoidance, debasement, monetary fakes, digital wrongdoings, genuine cheats, and so on. As of now, e-

Many cases of corporate forgeries and digital violations go unreported.

CHAPTER-4

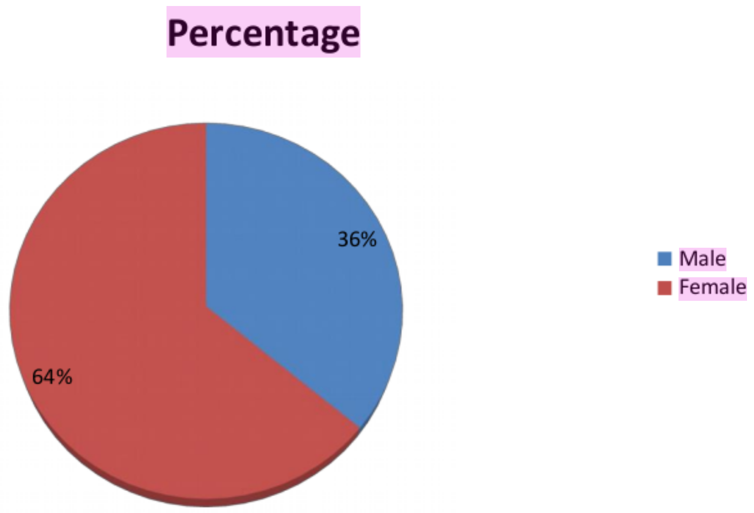
Questionnaires are Information Analysis and Interpretation:

Surveys are restricted to respondents chosen arbitrarily inside the twin urban communities of Hyderabad and Secunderabad. 50/50 respondents have reacted. The information so gathered is organized, dissected, deciphered, and introduced in the accompanying tables and diagrams:

Gender – respondents

Table – 1

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



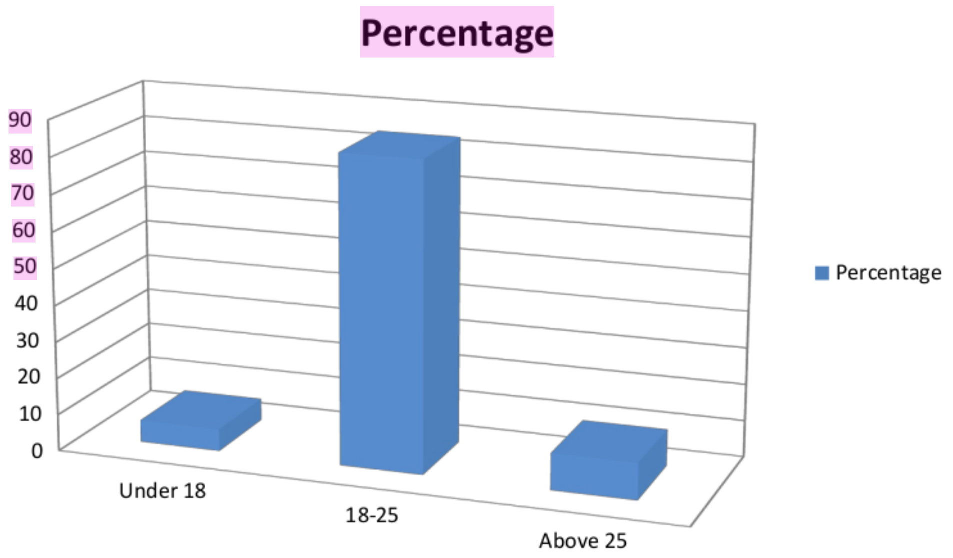
Understanding

From the above layout, plainly 36% of respondents (18/50) are guys. 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%**



Translation

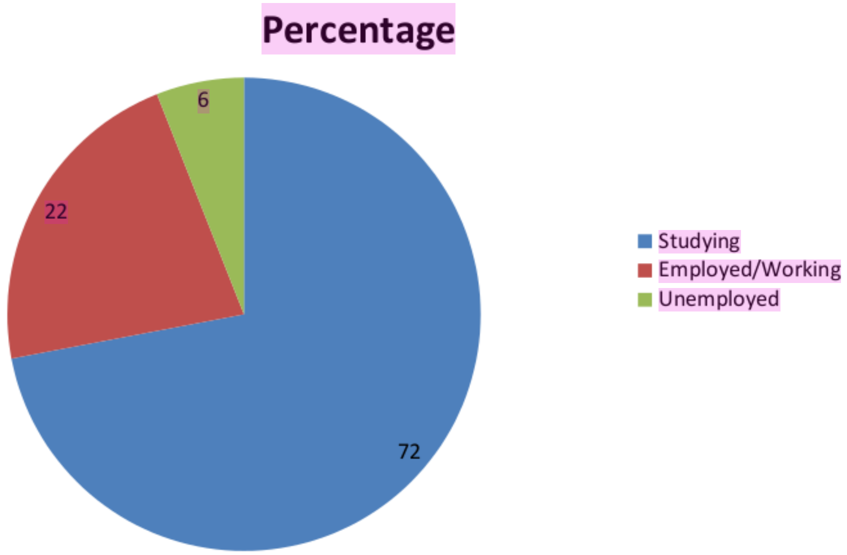
From the above chart, it is seen that 6% of respondents (3/42) fall under the age gathering of under 18. 84% of respondents (42/50) fall under the age gathering of 1825. 10% of respondents (5/50) fall under the age gathering of more than 25.

STATUS

Table – 3

Occupation	**Number of respondents**	**Percentage(%) of respondents**
Studying	36	72
Employed/Working	11	22%

Unemployed	3	6%
Total	**50**	**100%**



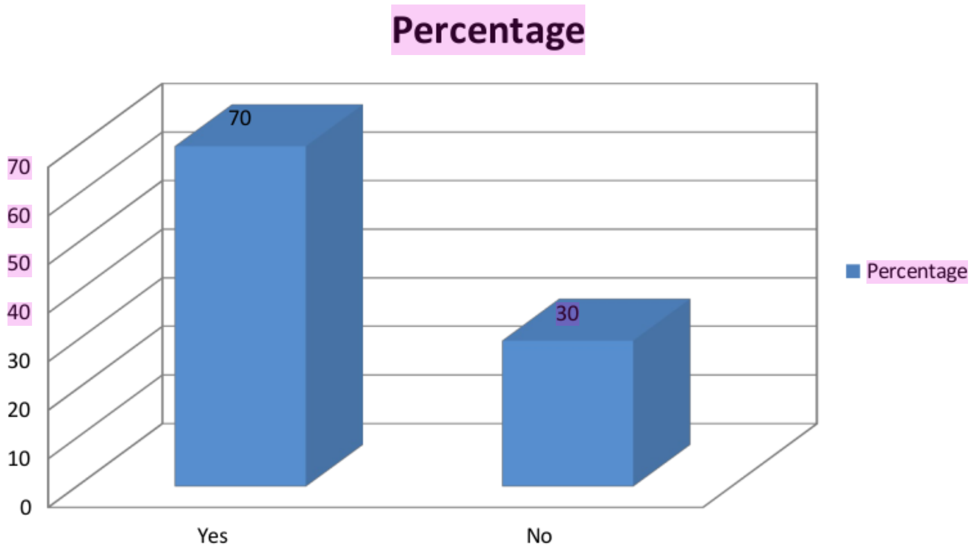
Understanding

From the above layout, it is seen that 72% of respondents (36/50) are now taking a gander at 22% of respondents (11/50) are utilized or working. 6% of respondents (3/50) are jobless.

Awareness regarding Cyber Security Issues

Table-4

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



Translation

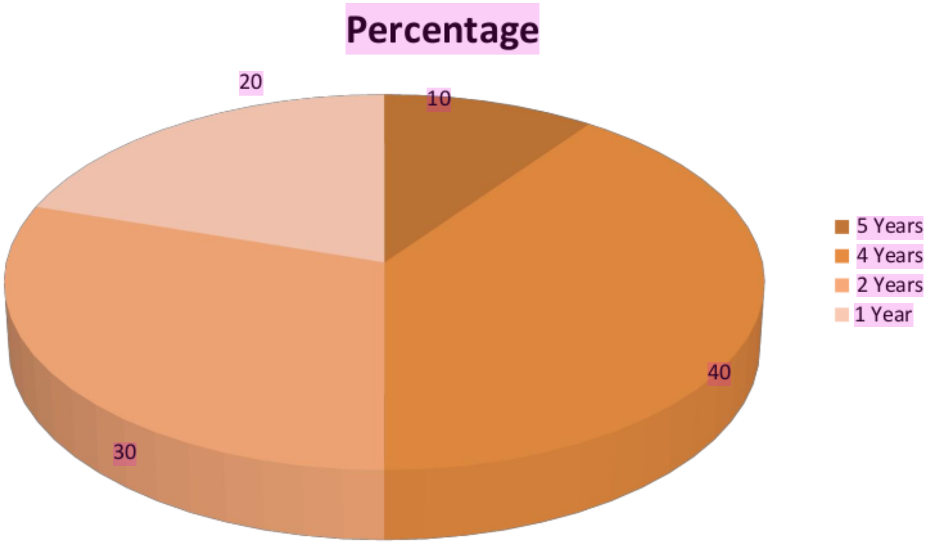
From the above chart, it is seen that 70% of respondents (35/50) have a high level of concern with respect to network safety issues. Despite the fact that 30% of respondents (15/50) are not aware of digital protection issues,

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%**



Translation

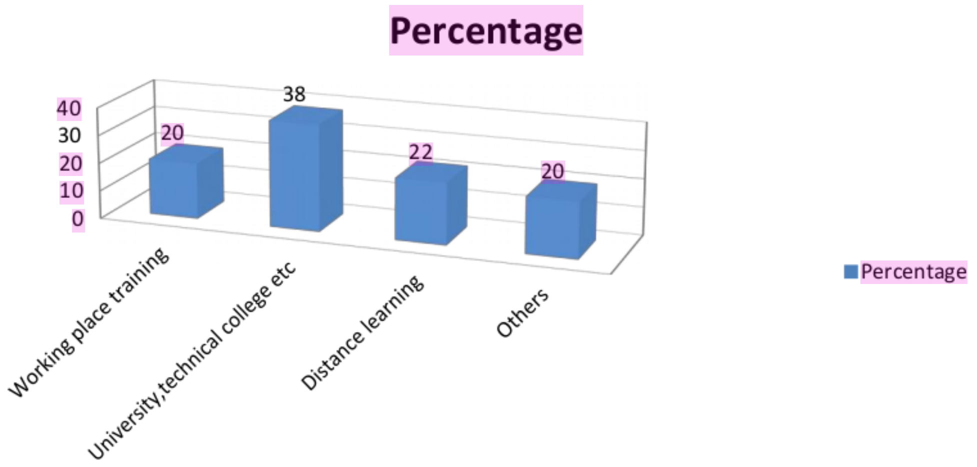
From the above outline, it is seen that 10% of respondents (5/50) have been using the web for quite a long time. Likewise, 30% of respondents (15/50) have been using the web for quite a while. 40% of respondents (20/50) have been using the web for quite a while. 20% of respondents (10/50) have been using the web 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%**



Understanding

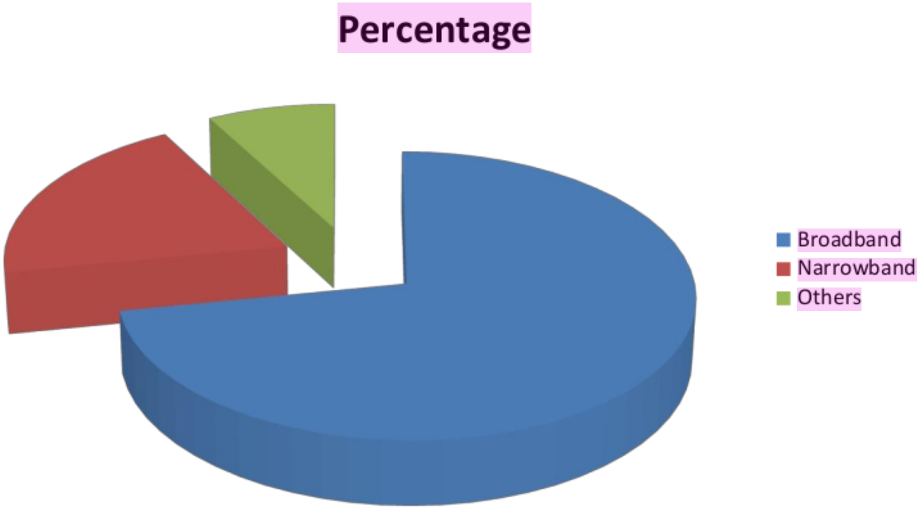
From the above chart, it is seen that 20% of respondents are taking information security from the wellspring of working spots while preparing. 38% of respondents (19/50) are taking in security from the wellspring of universities, explicit schools, and so on 22% of respondents (11/50) are taking in security from the wellspring of distance learning, and so on 20% of respondents (10/50) are taking in security from the wellspring 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

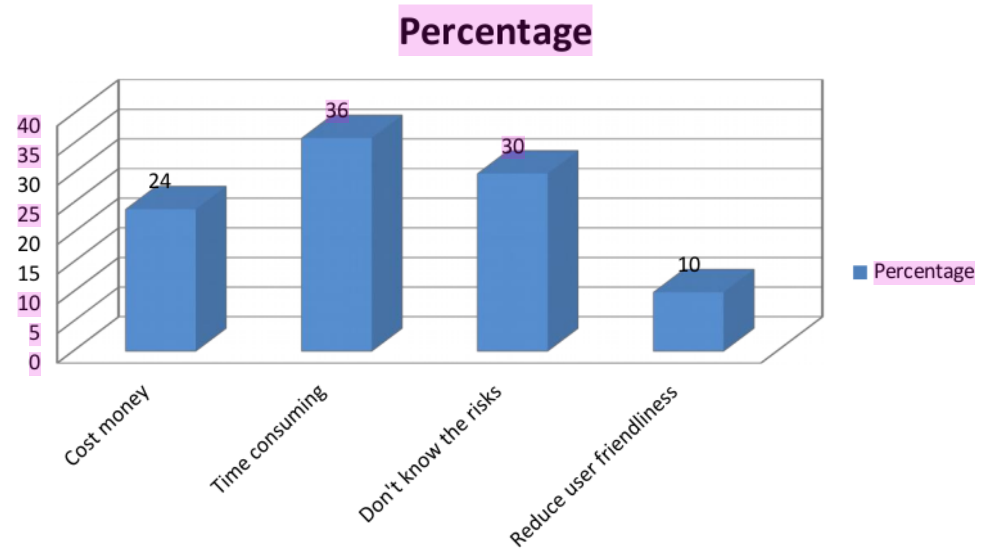
According to the above diagram, 72% of respondents (36/50) have some type of broadband connection at home.At home, 20% of respondents (10/50) have some sort of narrowband web affiliation. Different sorts of web affiliation are utilised at home by 8% of respondents (4/50).

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%**



Understanding

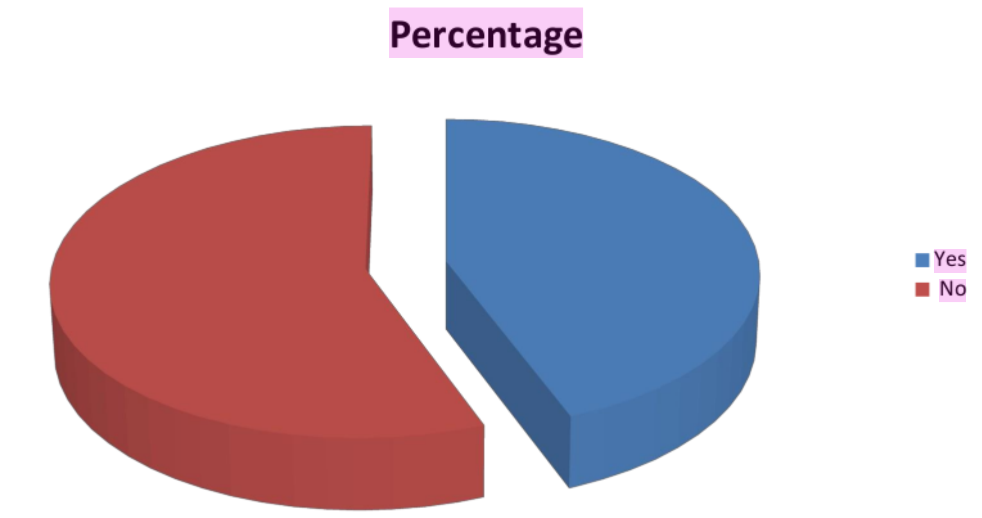
In the above outline, it is seen that 24% of respondents (12/50) are having a problem with wellbeing endeavours since they cost cash. 36% of respondents (18/50) disapprove of safety efforts in that they are grim. 30% of respondents (15/50) are having issues with safety efforts in that they don't have a clue about the dangers. 10% of respondents (5/50) disapprove of safety efforts in that they decrease ease of use.

Feeling worried about using the Internet

Table-9

Options	**Number of respondents**	**Percentage(%) of respondents**
Yes	22	44%

No	28	56%
Total	**50**	**100%**



Understanding

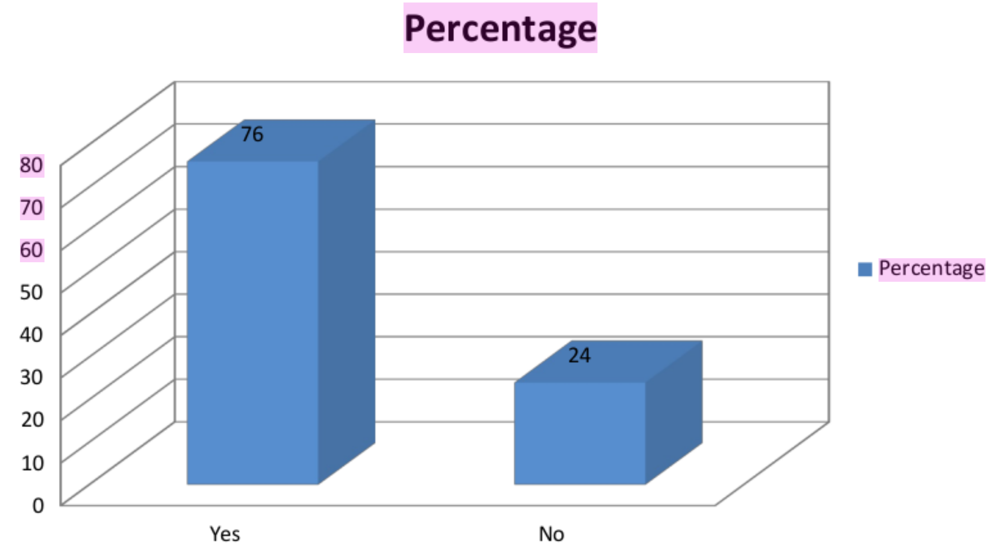
From the above outline, it is seen that 44% of respondents (22/50) have a focused point of view toward using the web. 56% of respondents (28/50) are not worried about using the web.

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%**



Understanding

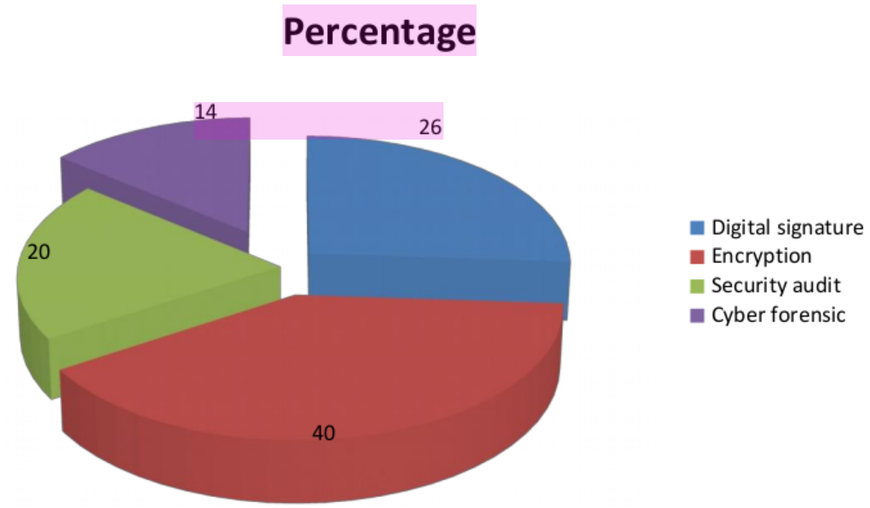
From the above outline, it is seen that 76% of respondents (38/50) have some familiarity with criminal establishments' digital activities. 24% (12/50) of respondents are unconscious of criminal sanctioning for digital activities.

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%**



Translation

From the above diagram, it is seen that 26% of respondents (13/50) say that computerised marks are an incredible gadget to get against digital risks. 40% of respondents (20/50) believe encryption is a viable tool for protecting against digital threats.20% of respondents (10/50) accept that security reviews are a practical device for securing against digital threats. According to 14% of respondents (7/50), cybercriminal science is a convincing tool for protecting against digital threats.

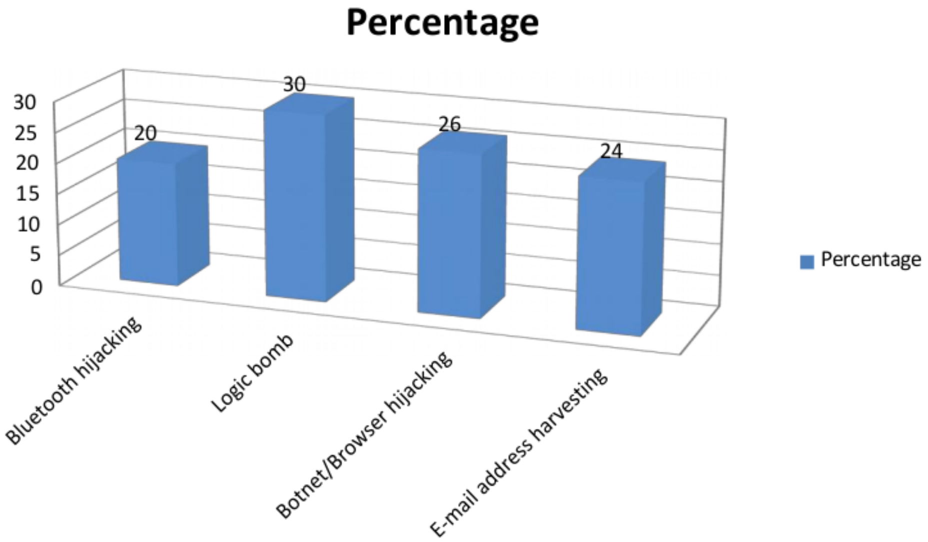
.

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%**



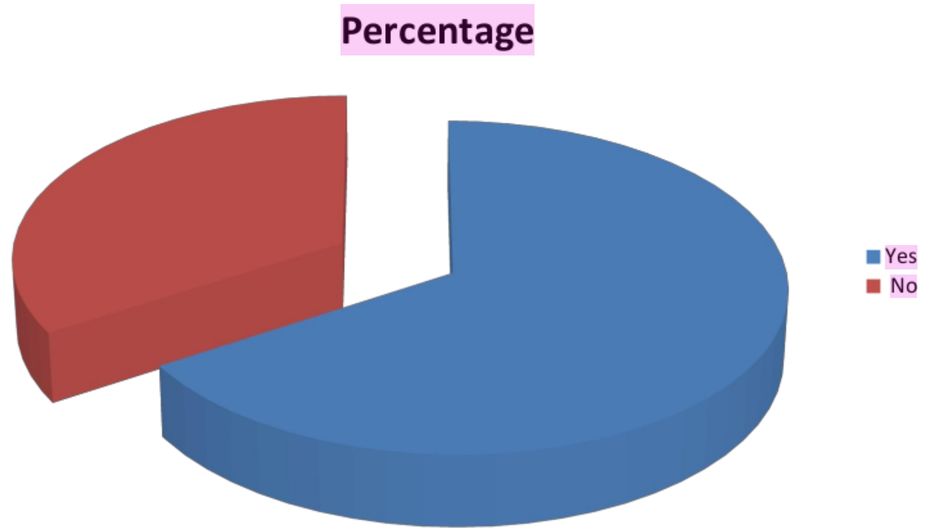
Translation

According to the above outline, 20% of respondents (10/50) are aware of the Bluetooth seizing type of cyber attack.30% of respondents (15/50) realise the Logic Bomb is a kind of cyber assault. 26% of respondents (13/50) know about the Botnet/Browser seizing sort of cyber assault. 24% of respondents (12/50) are aware that their e-mail address is being used in a 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%**



Translation

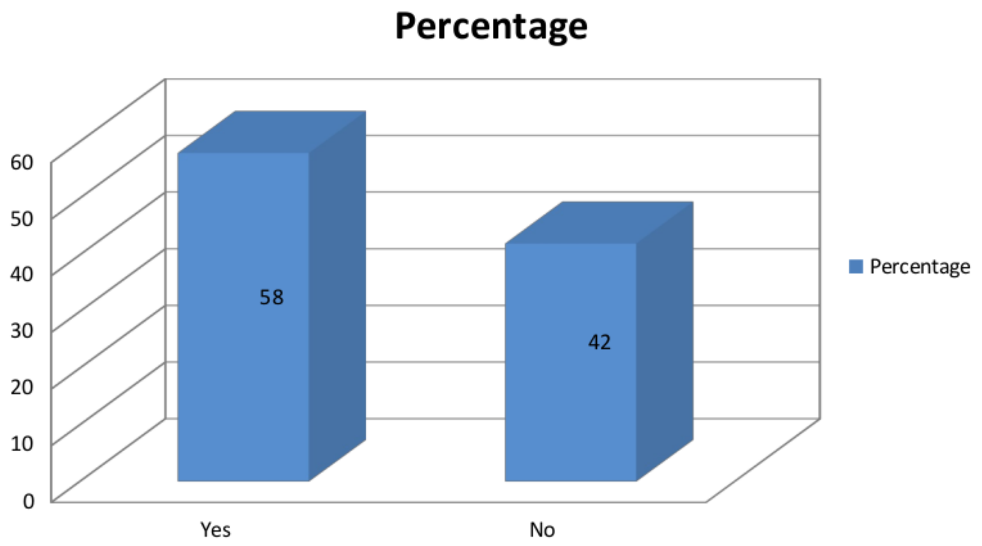
From the above diagram, it is seen that 66% of respondents (33/50) are having mindfulness with respect to the current Adhaar card issue. 34% of respondents (17/50) have no mindfulness in regards to the current Adhaar card issue.

.

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%**



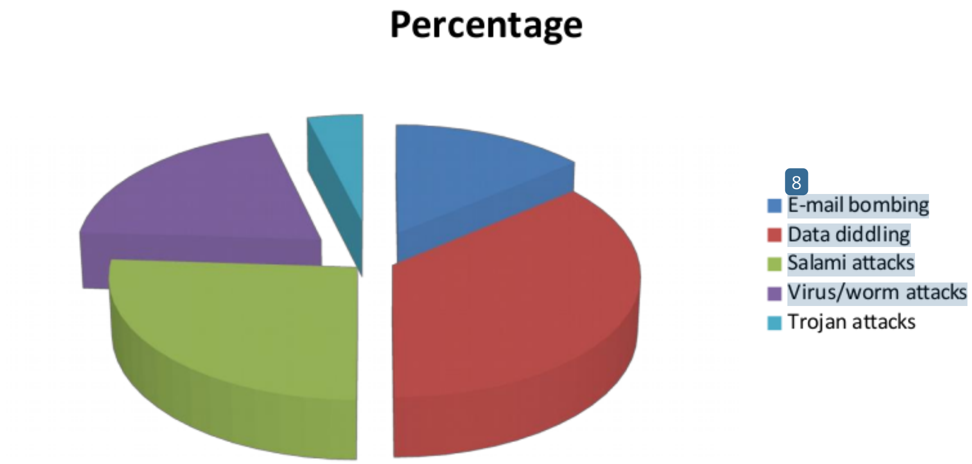
Translation

From the above diagram, it is seen that 58% of respondents (29/50) are saying that the cell phones' secret words are encoded and secured. 42% of respondents (21/50) say that the cell phone secret keys are not scrambled and ensured.

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%**



Understanding

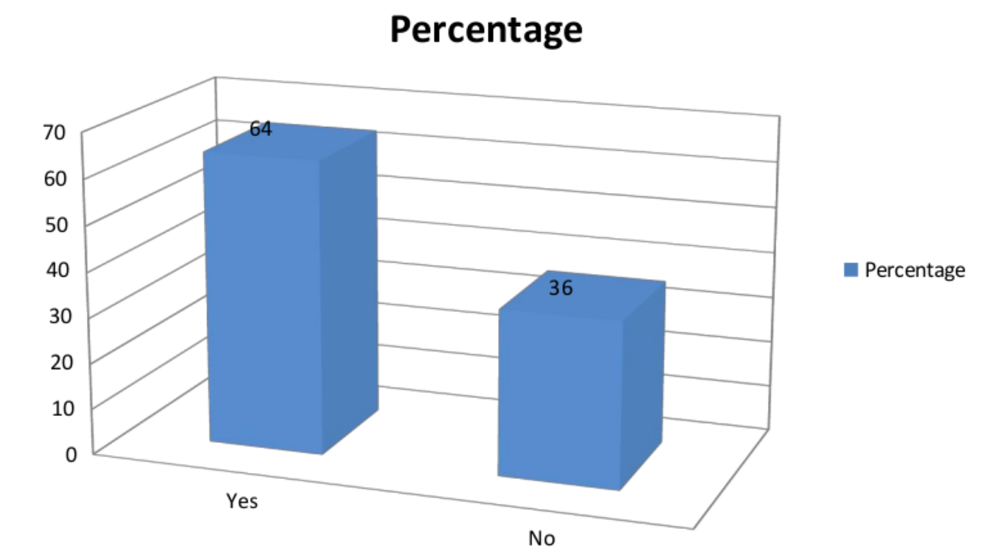
Email besieging Data diddling Salami assaults Virus/worm assaults Trojan assaults

From the above diagram, it is seen that 14% of respondents (7/50) are experienced with e-mail bombardment for cyber wrongdoing. 36% of respondents (18/50) are experienced with data diddling and cyber wrongdoing. 26% of respondents (13/50) are experienced with salami assaults and cyber wrongdoing. 20% of respondents (10/50) are experienced with Virus or worm assaults Cyber wrongdoing. 4% of respondents (2/50) are experienced with Trojan assaults Cyber wrongdoing

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%**



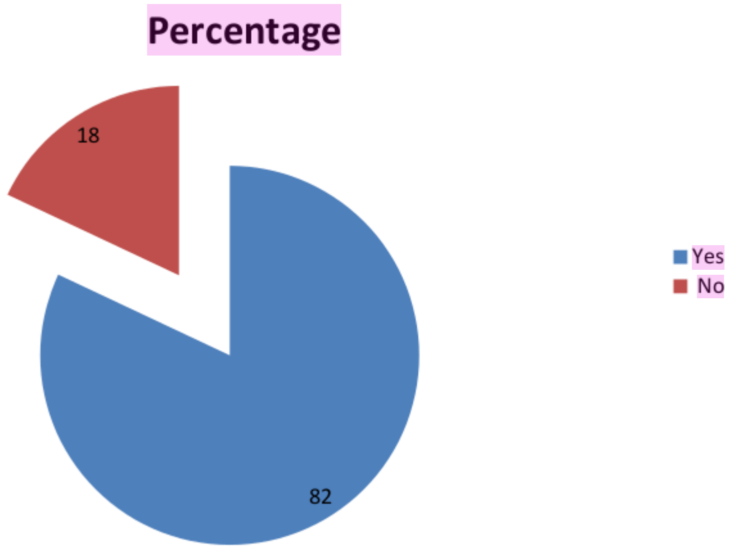
Translation

From the above outline, it is seen that 64% of the respondents (32/50) know about the Information Technology Act, 2000. 36% of respondents (18/50) don't know about the 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%**



Translation

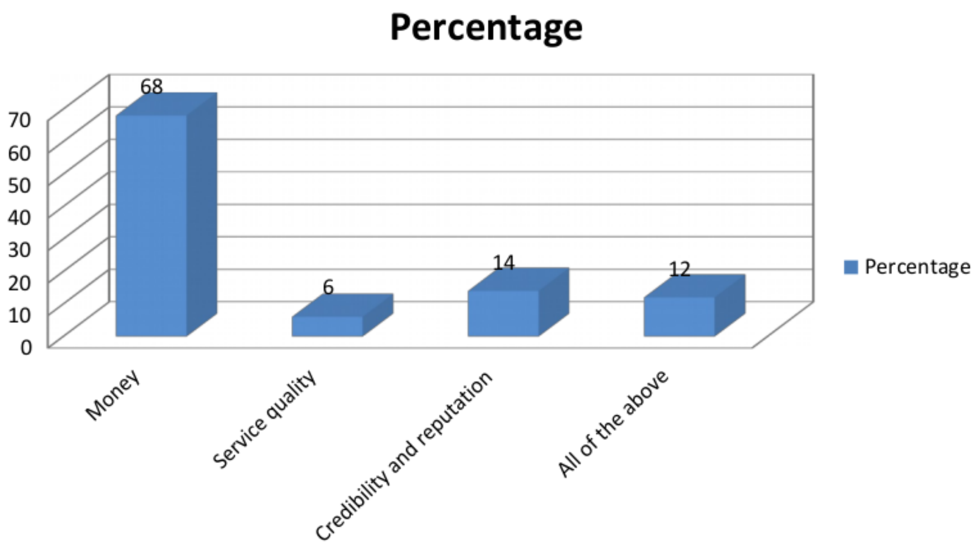
From the above graph it is seen that 82% of respondents (41/50) feel that IT Act, 2000 is equipped for forestalling Cyber violations. 18% of respondents (9/50) feel that IT Act, 2000 isn't equipped for forestalling Cyber wrongdoings

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%**



Translation

From the above graph, it is seen that 68% of respondents (34/50) are of the opinion that the most widely recognised misfortune due to digital wrongdoing is cash. 6% of respondents (3/50) agree with the assessment that the most well-known misfortune due to digital wrongdoing is administration quality. 14% of respondents (7/50) agreed with the assessment that the most well-known misfortune due to digital wrongdoing is believability and notoriety. 12% of respondents (6/50) are of the assessment that the most widely recognised misfortune due to digital wrongdoing is all of the above expressed choices.

CHAPTER-5

CONCLUSION:

Local areas on the internet depend on communication between individuals. The internet has a significant social angle to it that should not be ignored. The internet can be treated as a channel contacting a piece of genuine space on central issues. Thoughts are passed through the channel, and business is executed through this channel. The internet networks are individuals from the worldwide local area associating on an unexpected plane in comparison to genuine space.

With the gigantic development in the quantity of Internet clients everywhere, the security of information and its legitimate administration assumes a crucial part for future flourishing and possibility. It is worried about individuals attempting to get to remote help is that they are not approved to utilize.

Rules for the obligatory wearing of head protectors for bikers by government specialists have no advantage for them; it is for our own security and life. At the same time, we ought to comprehend our responsibilities regarding the internet and ought to at minimum deal with security for our own gadgets. These means incorporate the establishment of antivirus programming and keeping it refreshed, introducing individual firewalls and keeping rules refreshed. We should screen and document all security logs.

We ought to have reinforcement of significant information. Our gadgets ought to be secured by passwords, and there ought to be limited admittance to the delicate information on our gadgets. More importantly, we should aspire for increased PC proficiency in order to comprehend the health issues associated with the internet. Simultaneously, we want to use the specialisation of private areas in the field of network safety, and the government ought to advance more PPP projects for the public internet.

CHAPTER-6

QUESTIONNAIRE ON CYBER SECURITY ISSUES IN INDIA

NAME ____

GENDER	a) Male	b) Female	
AGE RANGE	a) Under 18	b) 18 to 25	c) Above 25
STATUS	a) Studying	b) Employed/Working	c) Un-employed

1) Do you are familiar Cyber Security issues?

a) Yes b) No

2) For how long have you been utilizing the web

a) 5 years b) 2 years c) 3 years d) 1 year

a) How/where did you find out with regards to data security? If it's not too much trouble, select all proper Work place training

b) University, technical college etc

c) Distance learning etc.

d) Other

3) What sort of web association do you have at home?

<Narrow band>

a) Phone line (dialup) b) ISON line (not always on) c) ISDN line (always on)

<Broadband>

a) Cable TV line b) Optical line (FTTH line) c) Fixed wireless access (FWA) d) DSL line (ADSL, VDSL, HDSL, SDSL etc)

4) What issues/issues do you have with safety efforts?

a) They cost money b) I don’t know how to go about taking them c) I don’t know the risks d) They are time consuming e) They reduce user friendliness

5) Do you at any point have a stressed outlook on utilizing the web?

a) Not really b) I know security threats exist, but Iam not concerned as I take preventive measures c) I take measures against security threats; however Iam concerned as they are insufficient

6) If you couldn't utilise the web, how much could your degree of fulfilment with life decline?

*Your current level of satisfaction with life set at 100 for these questions.

a) My level of satisfaction would increase (101 points)

b) No change (100) points

c) 10% decrease

d) 20% decrease

e) others

7) Are cell phones scrambled and secret key secured? ?

a) URL, title of laws 2) Acts 3) Articles

8) Which of these Cyber Crimes that are most often experienced by you? ?

a) Yes b) No

9) Are you mindful of Information Technology (IT) Act, 200?

a) E-mail bombing b) Data diddling c) Salami attacks d) Virus/worm attacks e) Trojan attacks f) Trojan attacks

10) Do you think the IT Act 2000 is equipped for forestalling Cyber Crimes?

a) Yes b) No

11) Do you think the IT Act 2000 is capable of preventing Cyber Crimes?

a) Yes b) No

12) Which apparatuses are powerful to ensure against Cyber dangers? What do you feel?

a) Digital signature b) Encryption c) Security audit d) Cyber forensic

13) What sort of digital assaults do you know

a) Bluetooth hijacking 2) Botnet/browser hijacking 3) E-mail address harvesting

4) Logic bomb

15) Is it true that you are mindful of current Adhaar Card issue?

a) Yes b) No

BIBLIOGRAPHY

www.google.com

www.wikipedia.com

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

www.visionias.in

deep Sir turnitin Report

ORIGINALITY REPORT

31%	23%	1%	13%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	appscgroup1mains.blogspot.com Internet Source	7%
2	Submitted to Softwarica College Of IT & E-Commerce Student Paper	7%
3	visionias.in Internet Source	4%
4	vinodtechtutorials.wordpress.com Internet Source	2%
5	durgaprasadcharakanam.blogspot.com Internet Source	2%
6	www.scribd.com Internet Source	2%
7	Submitted to The NorthCap University, Gurugram Student Paper	1%
8	shodhganga.inflibnet.ac.in Internet Source	1%
9	www.insightsonindia.com	

	Internet Source	1 %
10	blog.ipleaders.in Internet Source	<1 %
11	Submitted to RICS School of Built Environment, Amity University Student Paper	<1 %
12	upscdiary.com Internet Source	<1 %
13	dspace.uiu.ac.bd:8080 Internet Source	<1 %
14	Submitted to Sheffield Hallam University Student Paper	<1 %
15	infogalactic.com Internet Source	<1 %
16	Submitted to Lal Bahadur Shastri National Academy of Administration of Management Student Paper	<1 %
17	Submitted to ASA Institute Student Paper	<1 %
18	es.scribd.com Internet Source	<1 %
19	ictps.blogspot.com Internet Source	<1 %

20	Submitted to University of Arizona Student Paper	<1 %
21	uir.unisa.ac.za Internet Source	<1 %
22	Submitted to College of Banking and Financial Studies Student Paper	<1 %
23	Submitted to Regent Independent School and Sixth Form College Student Paper	<1 %
24	Submitted to Carnegie Mellon University Student Paper	<1 %
25	Submitted to University of Huddersfield Student Paper	<1 %
26	Submitted to Lynden High School Student Paper	<1 %
27	cybersecuritylegalissues.blogspot.com Internet Source	<1 %
28	www.slideshare.net Internet Source	<1 %
29	iasgatewayy.com Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		