International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Conference Issue – ICDEBI-2018
INTERNATIONAL CONFERENCE ON DIGITAL ECONOMY AND ITS IMPACT ON BUSINESS AND INDUSTRY
Organised By: V. P. Institute of Management Studies & Research, Sangli

A Brief Study on Cyber Crimes and IT Act in India

Dr. Adv. Mrs. Neeta Deshpande
Assistant Professor & HOD, Commerce Department
V. P. Institute of Management Studies & Research, Sangli,
Affiliated to Shivaji University, Kolhapur, Maharashtra, India

ABSTRACT
Digital India is a campaign launched by GOI to ensure that government services are made available to Indian citizens online. As Digital India encourages cashless payments, but still many people are not very familiar with cashless payments; they have fear in their mind of losing their money. The success of digital India project is depending upon maximum connectivity with minimum cyber security risks. Increasing Technological advancements result into increase in cyber crimes. India has cyber laws to protect the citizens from the growing cyber crimes. The present paper is based on both primary and secondary data. The objectives of the study are to understand growth of internet users in the world and in Asia, to study growing cyber crimes, to understand the opinion of practicing advocates regarding the provisions of existing cyber laws in India to tackle with the cyber crimes and to understand the shortcomings in the IT Act.

KEYWORD: *Internet, unauthorized access, cyber crime, cyber law, spam, hacking.*

INTRODUCTION
Now the computer and internet are the inseparable part our daily life. In present Era, people can access information, store information, share information through internet. The growing fastest world of internet is known as cyber world. Government of India has launched the Digital India campaign. Accordingly, India goes digitally fast, its vulnerabilities also grow at a disturbing pace. With demonetization pushed Indians to adopt E-platforms at a great pace, its vulnerability is also growing fast. After demonetization, India shifts to a cashless economy and now cyber threats are at a new high. A joint study by ASSOCHAM, an ATM Card hack hit the Indian bank in affecting, around 3.2 million debit Card. The study said the attacks on Indian website have increased nearly five times in the past four years. India's budgetary allocation towards cyber security was only about Rs. 42.2 crores(2012-13) whereas US spends $ 658 Million through Department of Home land security & $ 93 Million through US-CERT . Cyber threats will rise as India is seeing a shift towards a cashless economy. [1]

There are huge gaps in India's cyber security infrastructure. According to the survey of ASSOCHAM, India has witnessed 350% rise in cyber crimes in the three years i.e. from 2011 to 2014. According to IEEE Conference report, 72% Indian companies faced cyber attacks in 2015.[2]

ASSOCHAM also reported that attacks on Indian websites have increased five times in last four years. India's budgetary allocation towards cyber security was only 35.45 crores and which is increased to Rs 42.2. crores in the year 2011-2012. [3]

According to National Cyber Record Bureau, in 2012 27605 and in 2011, 21699 Indian websites are hacked. In 2013, total 28481 Indian websites were hacked by various hackers groups operating over the Globe. According to NCRB report, in 2011 total 1791 cases were registered, in 2012-2876 cases and in 2013-4356 cares were registered under Information Technology Act 2000. NCRB reported that 422 cyber crimes are registered under Indian Penal Code which

were increased to 601 in 2012 and increased to 1337 cyber crimes in 2013.[4]

This statistical data of NCRB about cyber crime in India, government's budgetary allocation for cyber security are shocking. Cyber Security is the key to realizing the dream of a truly digital India. This present paper is based on both primary and secondary data. Efforts have been taken to understand the current scenario of cyber crime, the existing cyber law and its major provision, opinion of advocates regarding the lacunas in the Act.

Objectives:

1. To understand the basic concept of the cyber world and cyber crime.
2. To study the growing trend of internet users in the world.
3. To study about the provisions of Information Technology Act in India.
4. To study the proportion of growing cyber crimes and person arrested in India.
5. To point out the possible loopholes in the existing cyber law in India
6. To give suggestions / preventive measures to reduce cyber crimes.

Research Methodology:

In the present study, both primary and secondary data have been used. Primary data is collected by discussions with selected respondents. For the purpose of understanding the available provisions of Information Technology Act, to understand the problems in implementing and tackling with the cyber crimes registered in India, the research has under taken a survey of twenty practicing advocates who are located in different cities and practicing in cyber cases. Convenience sampling method is used for selecting the respondents. Discussions with the advocates helped the researcher to understand the lacunas in IT Act 2000 and IT amended Act 2008. Three point scales has been used to understand the opinions of respondents and weighted average has been calculated. The secondary data has been collected though web sites, e-journals, research papers, theses etc. Information Technology Bare Act, news papers etc. To test the hypotheses, weighted average mean has been calculated to understand the opinion of respondents regarding the lacunas in IT Act.

Limitations of the Study:

The present study covers only two chapters i.e. IX and XI with selected sections / provisions which are related to cyber crimes and punishments under cyber crimes. Due to time constraint only few advocates practicing in Maharashtra are contacted to understand the shortcomings in the Act. .

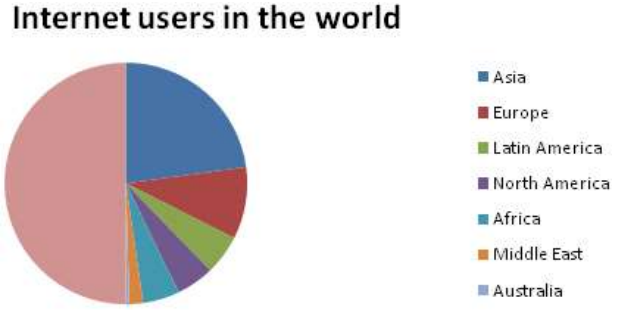
Internet Users in the World:

Today's world is the cyber world. The statistical data about internet users in the world has been published on internet world states indicate that the number of internet users in the world is increasing. Asian countries are leading in the use of internet.

Table No 1: Growth in Internet Users in the world in last three years

Sr. No.	Countries	June 30, 2014		Dec 31 , 2017	
		Int. users in Millions	% to total users June, 2014	Int. users in Millions	% to total users Dec 31, 2017
1	Asia	1386.2	45.66	2013.00	48.7 %
2	Europe	582.4	19.19	704.83	17.0%
3	Latin America	320.3	10.55	437.00	10.5%
4	North America	310.3	10.22	345.66	8.3%
5	Africa	297.9	9.81	453.32	10.9%
6	Middle East	111.8	3.68	164.04	3.9%
7	Australia	26.8	0.88	28.44	0.7%
	Total	3035.7	100.00	4156.93	100.00

Source: www.internetworldstats.com/stats.htm

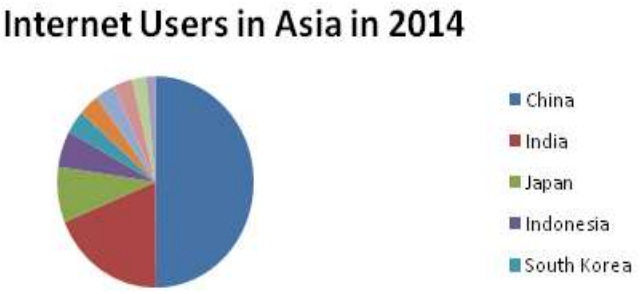


The above table depicts the internet users in the world. Asian countries are most users of internet in the world. Asia tops in the use of internet. Following Asia, Europe is the second largest continent in internet use.

Table No 2: Asian Top Internet Using Countries (In millions)

Sr. No.	Countries	June,30, 2014		Dec 31, 2017	
		Internet Users	% to total	Internet users	% to total
1	China	642.3	49.92	772.00	45.24
2	India	243.0	18.89	462.12	27.08
3	Japan	109.6	8.52	118.63	6.95
4	Indonesia	71.2	5.53	143.26	8.39
5	South Korea	45.3	3.52	NA	NA
6	Philippines	44.2	3.44	67.00	3.93
7	Vietnam	41.0	3.19	63.06	3.70
8	Bangladesh	40.8	3.17	80.48	4.72
9	Pakistan	29.1	2.26	NA	NA
10	Malaysia	20.1	1.56	NA	NA
	Total	1286.60	100.00	NA	100.00

Source: www.internetworldstar.com



The above table depicts the internet user countries and their rank in Asia. China is the top country which ranks first in internet use. In Asia region, India has rank two in internet user countries in the Asia. India is the fastest growing country.

Cyber crime:

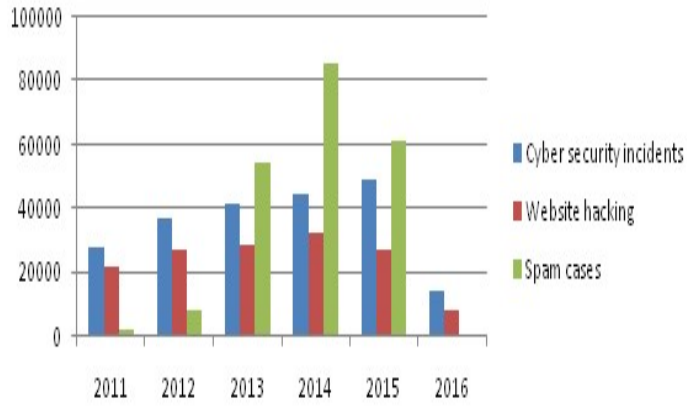
Today all internet users can access the internet anytime from anywhere. Along with the good side internet may be used for many illegal works also. The term cyber crime relates to the violation of network system. It is a criminal activity that takes numerous forms. It may consist of freeing of a virus into a network, the defacing of computer data or it may also be an unauthorized access into the information stored in computer. Cyber crime is not a static term. Cyber crime includes Email-bombing, Hacking, Spreading computer virus, Phishing, identity theft, Internet Frauds, Malicious software, domain hijacking, SMS spreading, voice phishing etc. Identifying the hackers is very difficult as they live three continents away from victim. We were aware about only traditional types of crimes like murder, rape, theft, extortion, robbery, dacoit etc. Now with the development and advancement of science and technology, new weapons such as computers and internet which are used in committing crime have emerged. With the technology increasing criminals don't have to rob banks, nor do they have to be outside in order to commit any crime because by sitting at home, they can commit any crime because they have everything on their lap. Their weapons are mouse, cursors and password.

From many literatures, it is observed that, there is a grave underreporting of cyber crimes in India. Cyber crime is committed now and then but is hardly reported. The cases of cyber crime that reached to the court of law are therefore very few. There are practical difficulties in collecting, sharing, appreciating digital evidence. The act has not succeeded in solving all the problems and satisfying the victims of cyber crime. The rapidly increasing incidence of cyber crime indicates that the nature of traditional crime is changing its shape and being facilitated by digital mediums.

Table No 3. Table showing Cyber Crimes cases registered in India

Years	Cyber security incidents	Website hacking	Spam cases
2011	28127	21700	2480
2012	36924	27605	8150
2013	41319	28481	54677
2014	44677	32323	85659
2015	49455	27025	61628
2016*	14363	8056	13851

***Figures as on March 2016**

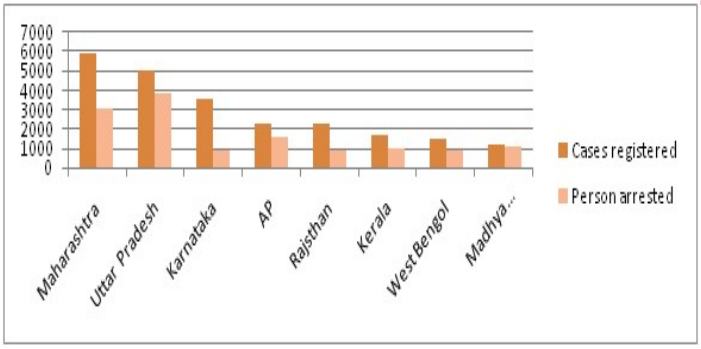


The cyber security incidents are doubled in 5 years i.e. from 2011 to 2015, cyber security incidents were 28127 which are increased to 49455 in 2015. Similarly span cases are also increasing year after year, in 2011 only 2480 spam cases were there but in 2015, the amount of cases increased to 61628.

Table 4: Cyber crimes in different States in India (2011 to 2015)

States	Cases registered	Person arrested	% of cases registered & actual arrested
Maharashtra	5935	3088	52.03
Uttar Pradesh	4990	3868	77.52
AP	2295	1577	24.69
Karnataka	3597	888	68.71
Kerala	1680	958	41.02
Madhya Pradesh	1162	1093	57.02
Rajasthan	2243	920	57.97
West Bengol	1461	847	94.06

http://ncrb.nic.in



The above table shows the total cyber cases registered in different states. Maharashtra ranks first in total cyber crimes registration in last four years. Out of total 5935 cases only 52% people were arrested and AP only 24% people were arrested under cyber crime. It may be because, most of time, the person committing the crime is located outside of the country i.e outside the legal jurisdiction of the court. Even though India has established cross-boundary reciprocal legal rules, many countries won't participate and never honor warrants of arrest.

Table 5: Table showing cyber crimes in India reported by CERT-In

Year	Cyber crimes reported
2014	44679
2015	49455
2016	50362
2017*	27482

Source: Indian Computer Emergency Response Team(CERT-In) *data of 2017 is up to Dec

The above table depicts the cyber crimes in India in last four years. As per the report of Indian Computer Emergency Response Team (CERT-In), a total of 44679 cyber crime cases have been reported in 2014. While in 2016, 50363 cases were reported. In 2017, a total of 27,482 cases of cyber crimes have been reported till Dec 2017. With the high percentage of cybercrime coming forward, the number is expected to shoot up in coming future.[5]

Information Technology Act 2000

The problem of cyber crimes is not confined to one or two countries but the whole world is facing this big problem. India is no exception to this computer generated nuisance. As a measure to prevent and control internet crimes, the parliament enacted the Information Technology Act, 2000 which came into force on Oct 17, 2000. This Act is the sole redeemer to fight cyber crime where computer is either tool or target also falls under the IPC and other legislations of India. This Act applies to the internet and internet associated technology. It offers legal protection to people involved with the use of the internet. IT Act 2000 is a special Act to tackle the problem of cyber crime. The Act was sharpened by the amendment Act of 2008. The IT Act 2000 deals with the various cyber crimes in chapters IX & XI. Chapter IX deals with penalties and adjudication and chapter XI deals with offences. The important sections are Ss. 43,65,66,67, 70, 71, 72. Following are the sections under IT Act 2000.

Section 43
deals with the unauthorized access, unauthorized downloading , virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provides for a fine up to Rs 1 crore by way of remedy.

Section 65
Deals with tampering with computer source documents:
Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for the computer, computer programme and computer system or computer network, The Act provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Section 66
Deals with hacking with computer system and data alteration:
Whoever with the intention to cause any loss, damage, or to destroy, deletes or alter any information that resides in a public or person's computer. The Act provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Section 67
A deals with transmission or publication of material that contains sexually explicit contents, acts etc in electronic form and provide for imprisonment up to a term of 10 years and also with fine up to Rs. 20 lakhs.

Section 70:
Under this section, the appropriate government may, by notification in the official gazette, declare that any computer, computer system or computer network to be protected system. Any person secures or attempting to secure access to a protected system shall be punishable with imprisonment upto 10 years ans shall also be liable for fine.

Section 72,
For breaking confidentiality of the information of computer, It provide punishment for an unauthorized access or disclosure of that information to third person punishable with an imprisonment up to 2 years or fine which may extend to 1 lakh rupees or with both.

Section 73
Deals with publishing false digital signatures false in certain particulars, Fine of 1 lakh, or imprisonment of 2 years or both,

Table 6: A few important sections regarding cyber crimes

Offences	Section under IT Act
Damage to Computer, Computer system etc	Section 43
Power to issue direction for blocking from public access of any information through any computer's resources	Section 69A
Power to authorize to collect traffic information or data to monitor through any computer's resources for cyber security	Section 69B
Un-authorized access to protected system	Section 70
Breach of confidentiality and privacy	Section 72
Publishing false digital signature certificates	Section 73
Act to apply for contravention or offence that is committed outside India	Section 75
Offences by companies	Section 85
Sending threatening messages by mail	Section 503 IPC
Sending defamatory messages by e-mail	Section 499 IPC
Bogus websites, cyber frauds	Section 420 IPC
E-mail Spoofing	Section 463 IPC
E-mail abuse	Section 500 IPC
Online sale of drugs	NDPS Act
Online sale of Arms	Arms Act

Source: www.irjet.net International research journal of engineering and technology Vol 4 Issue 6 , June 2017

Cyber law is important to touch almost all aspects of transactions and activities on and concerned the internet, the worldwide web and cyberspace. In India, IT act 2000 has helped in handling cyber crimes. It has triggered tear in the minds of cyber terrorists. Internet and cyberspace helps people to perform

innumerable transactions. In this competitive Era, to promote the trade & business, internets facilitates convenience and give access to the world of technology. Today most of the transactions and communications are made via cyber space and are carried via electronic means. This act has introduced a legal framework to authenticate, supervise, secure electronic records by way of digital signature encryption modes etc.

Thus IT Act 2000 has both positive and negative aspects as well. After finding lot of shortcomings in IT Act 2000, amendment is done in Rajya Sabha on Dec 23rd of 2008. This Act was renamed as IT (Amendment Act 2008) and referred as ITAA 2008. The amendment is made to IT Act in 2008 to provide relief to computer owners/users by extending the reach of law to almost all the online criminal activities and increasing awareness among the people. It is primarily enacted for the promotion of E-commerce to meet the needs of globalization and liberalization of the economy. The Act suffers from some lacunas as it doesn't provide adequate security against web-transaction nor does it contain adequate provisions to prevent security frauds, stock confidentiality, in the internet trading.

The survey was conducted by the researcher to study the lacunas in the cyber Act. For this purpose the opinion of total 20 advocates who are currently practicing in different cities and handling the cases of cyber crime were considered. As per their view, there are some lacunas in the Act.

Table no 7: Opinions of respondent's regarding provisions of IT Act

Opinions of Respondents	Agree 3	Neutral 2	Disagree 1	Wt avg
1. The amended IT Act is sufficient to tackle with all cyber crimes in India.	3	2	15	1.40
2. The amended IT Act defines hacking or hacker clearly	4	1	15	1.45
3. The amended Act clearly defines the jurisdiction of E-contracts.	1	2	17	1.20
4. There is provision of stamp duty on E-contracts in IT Act.	0	1	19	1.05
5. There are separate provisions regarding online defamation and claim for compensation in sec 43.	0	3	17	1.15
6. The Act covers all the sections with regard to jurisdiction of courts over the parties operating in different countries.	2	2	16	1.30
7. The amended Act deals with the issues of E-Discovery of evidence .	2	2	16	1.30
8. The IT Act deals with spam issues .	3	1	16	1.35
9. Sec 79 & the rules framed in the IT Act are clear & complete rules for Internet Café .	5	1	14	1.55
10. The IT Act deals with pornography by foreign websites .	0	2	18	1.10
11. The IT Act deals with crimes of spreading of virus and worms by websites of foreign origin .	0	1	19	1.00
12. The IT Act deals with crime of selling banned medicines & drugs	2	2	16	1.05
13. The IT Act deals with crimes like selling devices harmful for nation's security .	1	1	18	1.30
14. The Act provides for separate legal jurisdiction for cyber world .	0	0	20	1.15
15. The Act provides for authorized cyber forensic tools for investigation.	0	2	18	1.00
16. Clear guidelines have been issued to lower courts to tackle with cyber cases .	7	3	10	1.10
17. There is unification of internet laws	6	3	11	1.85
18. The required powers have been rendered to police for entering & searching private places	5	5	10	1.75
Total respondents	20	20	20	

The weighted average mean of the responses on the different issues were calculated which are below 1.5 in most of the responses. Through the weighted average mean of responses, the researcher has concluded that there are some lacunas in IT Act 2000 and ITAA 2008. While discussing with advocates, researcher come to know some ground realities and shortcomings in the IT Act. Accordingly following observations regarding the IT Act in India are recorded.

1. The IT Act is not sufficient to tackle with all types of cyber crimes in India. Even the amended Act 2008, is lacking in defining the: hacking" and "hacker" clearly. The only IT Act is not sufficient to tackle all types of cyber crimes. For publication of harmful contents or such sites, we have IPC, Communication Decency law, Data Protection Act. IPC & CPC etc deal with the many subjects therefore lacks efficient enforceability mechanism.
2. According to the respondents, IT Act doesn't clearly defined electronic contracts in the Act, Cross border contract since click wrap contracts are not legally recognized as equivalent to digitally signed contract. When we check-in for website, we commonly click on agree to terms of contract. This is a contract without stamp duty. None of the E- contract contains stamp duty. There is no provision related to stamp duty on electronic contract i.e. E-stamp duty.
3. We hear many cases of online defamation to many people. This occurs when defamation takes place with the help of computers and internet. There was no any clause under section 43 of the Act, which describes online defamation and provision for compensation for cyber defamation.
4. The Act lacks in catching the cyber criminal ho commits crimes sitting at another continent. IT Act should applicable to all the persons irrespective of their nationality (i.e. non citizens also) who commit offence under the IT Act outside India, provided the Act or conduct constituting the offence or contravention involves computer, computer system, or computer network located in India under sec 1 & Sec 75 of IT Act. This provision lacks practical value until and unless the person can be extradited to India.
5. The amended IT Act 2000 has not dealt with the issues related to E-discovery. Most of the organizations are relying upon digital evidence. Email and media are the means of communication with each other to conduct and carry on the business. As per the opinion of advocates, IT act doesn't provide for E-discovery.
6. Spam issues are increasing rapidly but IT Act has not dealt with these issues in a detailed manner. As there is no clear definition of the word spam. The practice of sending unsolicited email is getting common in India which is also amounts to breach of individual's right to privacy on the net. The legislature did not think of taking exclusive cognizance to this huge menace.
7. Selected respondents said that, the obligations under section 79 and rules framed there in for intermedatories are applicable to cyber cafes. But they replied that the rules are incomplete rules which need further rules at state government level to control and prevent the cyber crimes.
8. The crime of pornography by foreign websites is let loose in the Act. It has not covered, nor discussed, nor being penalized. This will lead to Indian cyber criminals to host their pornography related websites on foreign shores without being accounted for Indian Territory.
9. Spreading of viruses and worms is a severe cybercrime. But it's very difficult to detect cyber crimes committed by websites of foreign origin like spreading of viruses and worms from abroad.
10. The IT Act doesn't cover online selling of banned medicines and drugs which is a serious offence. A separate NDPC Act deals with this issue. It also not touched the online selling devices which are harmful for our nation's internal security is not described in the IT Act. These issues are tackled by Indian Arms act.
11. The advocates opinioned that the IT Act doesn't have clear sections regarding jurisdiction of courts over the parties staying and operating in different jurisdiction or countries.
12. There is no provision of establishing separate courts for handling cyber crimes. There is a need to form cyber crime courts for criminal trials.
13. The present Act has no provisions regarding authorized cyber forensic tools to be used in investigation. Due to this, investigation agency may face problems in getting evidences and identification, location, prevention and extraction of digital information from a computer system to get a digital evidence to produce before the court.

14. The powers to entering and searching the private places have not been given to police under the IT Act. But unfortunately, many cyber criminals operate from their houses where police cannot reach and cannot search.
15. Through the discussions it is also observed that major offences covered under the IT Act are bailable in nature. Interim reliefs, anticipatory bails etc would be common. Cyber criminals have become use to for this practice; they may not have fear in their mind until they feel fear about the consequences after commitment of offence.

General Suggestions:

1. There is an urgent need to create awareness among the people and basically users of internet about cyber space, different forms of cyber crimes, so that internet users can take some persuasions while operating the internet. To enhance the knowledge about the ITAA Act 2008 is low, there is a need to conduct seminar-workshops on this said subject.
2. Prevention is always better then cures. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes.
3. With the healthy partnership with government, there is a need of safe, secure & trustworthy environment. The Act is passed in 2000, amended in 2008 to cover all the areas. But cyber law has to be changed with changing times..
4. Currently many laws like IPC, Arms Act, Communication Decency law, Data Protection Act, CPC etc deal with the many subjects therefore lacks efficient enforceability mechanism. To avoid the confusion of many laws dealing with the same subject, there is a need of special law dealing with the subject specifically in toto. There is a need of unification of laws by taking all the internet laws to arrive at code which will deal with all the problems related to internet crimes. Unification of internet laws will be the solution.
5. E-commerce is flourishing in India in last 4-5 years. Website owners should responsible to checking the traffic and tap any irregularity on the site. They should adopt some policy for preventing cyber crimes as number of internet users are growing day by day.

Specific Suggestions:

1. Proper Provisions regarding E-contracts and E-stamp duty have to be inserted. Body corporate need to take measures required to provide a supplementary base for validating the contracts. If E-stamp duty is permitted and provided in the Act, it can yield lot of revenue to the government.
2. Special cyber courts with trained judicial officials should be established to decide and settle the cases of cyber crimes.
3. IT department should pass certain guidelines and notifications for the protection of computer system and should some more strict laws to breakdown the criminal activities relating to cyber crime.
4. There is a need of developing cyber forensics and biometric techniques. This will provide technical assistance to the investigating agency in investigation of cyber crime.

Conclusion:

The cyber crime is a new type of crime made by a class of sophisticated and learned criminals. Science and technology is growing fast and they are connecting the Globe by cutting the national frontiers but unfortunately the cyber law is still struggling to define and redefine the boundaries for the control of cyber crimes. The IT Act does not define the data protection principles. It failed to provide any provision related to third country transfer of data. Incidents of copyright theft, hacking, virus attacks etc have increased in last few years. As a result of growing internet users globally, piles of computer crimes are increasing. It seems inability of the legislature to keep cyber crime legislation ahead of the fast moving technological advancements. The IT Act is engaged in prevention and control of cyber crimes within the country's territorial jurisdiction. But unfortunately the Act is forgetting that cyber criminality is a global phenomenon which has no territorial limits at all. There is a need to enact a global cyber law uniformly applicable to all the countries in the world. To avoid the increasing crimes, there is a need to impart education and training for internet users.

References:

1. Jitender Kumar(2017)" Cyber Crime in India: An overview" an article published in Imperial Journal of Interdisciplinary Research, Vol-3, Issue-4, 2017 ISSN 2454-1362

2. Jitendra Kumar, Abid.
3. www.business standard.com daily business standard dated 4th July 2017
4. http://ncrb.nic.in
5. India.com July 22, 2017 accessed at 12.10 pm
6. www.internetworldstar.com
7. Shashirekha Malgi " Cyber Crimes under Indian IT Laws" a article published in IJSER ISSN 2229-5518
8. Tarun Arora(2008) " The concept of Cyber Crimes: An introduction". Legal News and Views, Vol.22, No. 6, June 2008. P.28
9. www.latestlaws.com
10. Shubham Koley (2015) " Present scenario of cybercrime in India and its present scenario of cyber crime in India & its prevention" IJSER, Vol.6, Issue 4, April 2015 ISSN 2229-5518
11. Jitendra kumar (2017) Cyber crime in India: An overview" article published in Imperical Journal of Interdisciplinary Research, Vol.3, Issue-4, 2017 ISSN 2454-1362
12. Prashant Mali, An article on www.varindia.com
13. Shashirekha Malgi, " Cyber Crimes under Indian IT Laws" online article published by IJSER journal ISSN 2229-5518
14. Cybercrimelawyer.wordpress.com
15. Anuraj Singh(2017) " Studies report on Cyber Laws in India & cybercrime Security" International Journal of Innovative Research in Computer & communication Engineering" Vol. 5, Issue 6, June 2017
16. Animesh Sarmah & Amlan Baruach (2017) " A brief study on cyber crime & cyber laws of India" International Research Journal of Enginerring & Technology. Vol.4, Issue 6
17. Daily Times of India dated December 13, 2016.
18. Vakul Sharma, "Information Technology: Law and Practice: Cyber Laws and Laws related to E-commerce" book published by Universal Law Publishing Co Pvt Ltd, 5th Edition.
19. Samiksha Godara(2011) "Prevention and control of cyber crimes in India: Problems, issues & strategies" a theses submitted to Maharshi Devanand University in 2011, P-442