CHAPTER 1
INTRODUCTION

Humans are complex social organisms and communication is the key to their survival. Humans have communicated for as long as they have existed, using a variety of physical and symbolic devices to create and convey meaning. The historical remnants proved that human communication is an age-old phenomenon and its method has evolved with the advancement of civilizations. Many factors had influenced the means of communication like social, cultural, economic, political, religious and technological aspects. The evolution of the means of communication had undergone a major boost in the past one hundred years when technological inventions had changed the communication landscape. The most remarked invention in the communication field is the advancement of information technology. The latest and the most spectacular progress in the field of information technology is the Internet during the twentieth century. The concept of internet received worldwide attention only after the United States Department of Defense used it as a communication network during the nuclear conflict. The internet integrated millions of computers around the world and facilitated communication through emails and the World Wide Web, by sending and receiving digital data.

Along with the advancement of technology, there emerged a new arena for crimes with new dimensions and sophisticated methods. As a socio-demographic group, women constitute a significant portion of the vulnerable groups of victims. Though cybercrime victimization takes place on a virtual world, the impact of the victimization can be deeper and it often transforms to the real world. Women have to face various forms of crime in cyberspace such as uploading offensive photos,
morphing, cyberstalking, defamation, online frauds, etc. The women victims of cybercrime have to circumnavigate various social, psychological and financial impacts as the aftermath of their victimization.

1.1 EMERGENCE OF CYBERCRIME

Before the invention of computers, the telephone system was in its peak and was used popularly by many users. Perhaps one among the first kind of cybercrimes was trying to break into the system to use it free of cost for making long distance calls. The growth of Information Technology, ever since the invention of computer, has been exponential. The last few decades witnessed vast developments in the arena of information sharing. Earlier computers were huge and very expensive and companies could not afford individual computer to perform their jobs. Therefore, they started to hire computers from outside. This made the computer and its users vulnerable to hacking.

From the 1970s, compact computers with affordable prices came into the market for individual use. These compact computers lacked any security measures and were so vulnerable that others could enter into it very easily. In 1969, the Advanced Research Projects Agency Network (ARPANET), a small network for military communication was established in US. In 1998, a student named Morris of Cornell University planned to test the effect of ‘worm’ on a large network and he succeeded. Perhaps, this could be the beginning of the present form of cybercrimes. In 1990s, with the advancement of the internet, cybercrimes become more common. With the rise of Microsoft Windows, a user-friendly operating system, more people started using computers. Taking advantage of the weakness of system security, hackers intruded into the government and university websites with malicious intentions. Further, the servers of Yahoo and AOL (America Online) sites have been
targeted by the hackers by constantly bombarding with hundreds of e-mail messages to down the server. Moreover, ‘Spams’ and ‘Denial-of-service’ have created a huge loss to companies and other organizations. Significantly, earlier attacks were carried out just for entertainment and personal popularity and not for financial gain. As technology advanced, flaws were also discovered and later, defense mechanisms were put in place to get rid of the weakness in the system. Hackers made use of the time gap between the discovery of flaws and the invention of defense mechanisms. This cycle was repeated for later inventions as well.

The advent of the Internet and communication devices with multiple features like Camera, Radio, General Packet Radio Service (GPRS) and Wi-Fi networks has made communication easier and faster. It also facilitates access to information from anywhere in the world at any time that has changed every aspect of human lives. Due to the technical advancements, many people started using the technology, ultimately resulting in huge increase of Internet users. These advancements in information technology, while of immense benefit for the population, has also created avenues for various criminal activities (Agarwal & Kaushik, 2014; Wall, 2008; Thapa & Kumar, 2011) and a seemingly endless source of victims (Reyns, 2010). There is no doubt that information technology is a wonderful and constructive tool for people in various fields. The World Wide Web (WWW) allows users to circulate content in the form of text, images, video and audio. Though technology is a boon to the people who like to communicate or network with others, cyber crooks abuse the technology to exploit many innocent people as well as computer illiterates for various reasons such as financial gain to lead a luxurious life, to quench their revenge, to defame, to ridicule and humiliate for their self-enjoyment etc. Cell-phone-based text messaging, internet-based instant messaging, telephone networks, email, chat rooms, Usenet
groups and Social Networking Sites are some of the popular and common communication tools exploited to commit cybercrimes. It is estimated that more than one million people become victims of cybercrimes across the world everyday (European Commission, 2012). Anybody who uses the Internet is at risk of becoming a victim of cybercrimes. However, there are reports stating that a large percentage of cybercrime cases have women as victims and men as perpetrators (Adam, 2001; Reno, 1999; Jaishankar, 2006; Fall, 2012). Cyber harassment is a uniquely gendered phenomenon (Citron, 2009). The majority of targeted individuals are women (Sheridan & Grant, 2007; Thapa and Kumar, 2011) and the female victims were abused with threatening and demeaning terms (Barak, 2005). In cyberspace, women were less safe and vulnerable as the perpetrators of these crimes were unaccountable for the offences they commit (Griffen, 2015). Women, irrespective of age group, were in danger with the advent of the internet (Halder and Jaishankar, 2009), as the traditional crimes have also taken a new form using latest information technology, due to the fact that committing the crime is easier and detecting it gets harder. In recent times, the rate of cybercrimes against women is at an alarming stage (Misra & Phillips, 2010) and it may pose a major threat to the security of a person as a whole (Jeet, 2012). Errant persons become more emboldened in their offensive behaviour since it is presumed that they will not face any consequences (Balakrishnan, 2009). In recent years, there have been numerous reports of women receiving unsolicited emails which often contain obscene and obnoxious language. An astonishing one in 12 women will be stalked in their lifetime (Moore, 2009). The vulnerability and safety of women is one of the biggest concerns of any criminal and penal law, but unfortunately, women are still defenseless in cyberspace (Halder and Jaishankar, 2008).
1.2 THE CONCEPT OF CYBERCRIME

Cyberspace refers to internet, popularly known as World Wide Web where information is circulated in a form of text, picture, audio and video. It also includes telecommunication services. To put it simply, the cyberspace refers to the broad network across the world. Cyberspace is a virtual world with no boundaries where people from different geographical location can communicate with others.

Some of the online services available in cyberspace includes social networking, instant messaging, texting through chat room, emailing, etc. These services are being operated by the individuals using a unique username and password. The identity of each user is authenticated by the username and password. These online services are popular and frequently availed by internet users as it is an easy and inexpensive means of communication. Further, texting through mobile phones popularly called SMS/MMS is another method of communication. Prior to the invention of Social Networking Sites, people shared their opinion on various topics of interest using blogs. Blogs are websites where people post their views on a particular topic and comments are posted by other users. With the recent invention of Social Networking Sites, especially Facebook, many internet users joined the service as it is a popular way of socialization with others. Social networking requires profile creation at the time of registering for the service. In addition to texting, the user uploads photos, shares information with like-minded people and finds old friends as well as new friends. Many prefer to use social networking as it is a better way to connect with people as they cannot spare time in physical space.

Information technology is of immense benefit to the society in many ways; but the negative side of it is that the cyberspace has been misused by cyber criminals
to send harassing, defamatory and obscene messages either to the victim or people known to the victim through chat rooms, blogs and social networking sites.

Cybercrimes are crimes committed in cyberspace against individual(s) or society, with or without an intention, directly or indirectly harming the individual(s) using various components of the cyberspace. Except few crimes which can be done only with Internet, most of the crimes were an extension of the traditional crimes committed in the physical space. Casey (2001) defines cybercrimes as “any crime that invokes computers and networks, including crimes that do not rely heavily on computers”. Thomas and Loader (2000) define cybercrimes as “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronics networks”.

1.3 TYPES OF CYBERCRIMES

The various types of cybercrimes that are being perpetrated against individuals have briefly been presented in this part of the chapter.

- **Cyber harassment / Stalking / Bullying**: Harassment is threatening or intimidating the victim either to control or to create fear. Cyber harassment is similar to face-to-face or letter harassments. Here the harasser makes use of the online services to harass the victim. Email is the frequent mode of communication used by the offender. The offender may either threaten the victim or contact people known to the victim. Cyber stalking is similar to cyber harassment. In cyber stalking, the harasser frequently harasses the victim by watching every move of the victim online. Sometimes, the harasser financially drains the victim’s bank account by purchasing goods in the name of the victim. Cyber bullying is another term used for cyber harassment and cyber stalking. Cyber bullying refers to a criminal
behaviour especially committed by young people and students. Unlike cyber stalking and cyber harassment where the offender can be an adult, in cyber bullying the offender is an adolescent.

- **Morphing**: Unauthorized alteration of someone’s picture with the intention to spoil the reputation of the victim. This is done through editing the pictures of the victims with pornographic content.

- **Cyber defamation**: Lowering someone in the view of others so as to defame or reduce their popularity is defamation. This is done through social networking sites by posting obscene message or pictures about the victim people known to the victim.

- **Hacking**: Unauthorized access into another computer system or network with the intention to commit malicious activity.

- **Identity theft**: Identity of the individual online users is authenticated using username and password. Offenders use the identity of others to enter into others’ account for various reasons like stealing information, financial gain or simply to hide oneself from criminal proceedings.

- **Spam/Phishing**: Phishing mails and spam mails refer to unsolicited mails from unknown people which are sent with the intention to gather important credentials from the victim. In phishing mails, a trap in a form of web links is setup by the offender to direct the victims to some fake websites similar to the genuine sites, where the victim is tricked to reveal personal information to be later used for malicious purpose.

- **Online frauds**: In online frauds, the victim is deceived to gain financial benefit. Lottery scam, Nigerian scam, auction scams, etc. are some forms of online frauds.
- **Fake profile**: Fake profile similar to the victim’s profile is created by the offender using the picture or personal details of the victim downloaded from the victim’s social networking home page.

- **Posting/ Circulating photos and personal information**: Victim’s personal information along with the photo is uploaded in some pornographic site or dating sites by the offender as if posted by the victim offering for service.

- **Vulgar / Obscene SMS/MMS**: Texting messages via mobile phones containing defamatory and unsolicited content are sent to the victim’s mobile phone demanding sexual favour.

- **Credit card frauds**: The credit card details and the pin number is stolen using handheld card reader. Later, the offender purchases goods online with the identity of the victim using the card details. Sometimes, card is cloned and used in local shops during purchase.

- **Email/IP spoofing**: Altering the email headers, so as to misrepresent the origin of the email is email spoofing. Similarly, IP address of the computer system is altered in such a way that the communication seems to have come from a different source.

- **Distributed denial-of-service attack**: A local system, in order to establish a connection with the remote server for internet access, handshaking messages were exchanged between the two systems. The hacker manipulates the message to constantly bombard the server with multiple messages by employing zombies called intermediary computers, to down the server and restrict access to server. Sometimes, hackers threaten the service provider for financial gain.
- **Virus, Worm and Trojan attacks**: Computer virus and worm are malicious program codes written with the intention to damage other computer systems. Most of the contents downloaded from the internet from free sources contain viruses. Later, this virus infects other files. Worms are similar to virus but they automatically get replicated. Trojan horse looks like a genuine program but creates a backdoor to steal important information from the system.

- **Cybersquatting** (Intellectual property crimes): Domain name will be registered with the name of reputed company violating intellectual property rights intentionally to demand money from the original owner.

- **Bank frauds**: Victim’s bank account is manipulated by an unauthorized user either by stealing the identity of the victim or by hacking into the bank’s website for financial gain.

- **Cyber pornography**: Pornography refers to sexually explicit pictures which are obscene in nature. Cyber pornography refers to transmitting or receiving or storing of obscene pictures of women online.

- **Cyber terrorism**: Cyber terrorism against government organizations is a serious issue to be taken care of as it can cause grievous damage to a country’s strategic assets and to general public safety. Sometimes, government websites are hacked to steal sensitive information and even the contents are altered, creating a mess.

### 1.4 CYBERCRIMES AGAINST WOMEN

Anyone can be a victim in cyberspace, but certain demographic characteristics like gender and age increase the vulnerability of a person in cyberspace. The belief that women may not retaliate against the offender as they
are often considered a weaker section is the major reason for the increase of cybercrimes against them. Basically, India is a patriarchal society where men dominate women in every aspect of life. This traditional practice is the root cause for the victimization of women and cyberspace is not an exception. Online services need identity of the user and other related information for authentication. In addition, the users of Social Networking Sites reveal their personal details at the time of profile creation. The hacker or cyber criminals misuse this information to harass the victim.

The term ‘cybercrime against women’ in India is mostly used to denote sexual crimes and sexual abuse on the internet, such as morphing the picture and using it for purposes of pornography, harassing women with threatening mails or messages, cyber stalking, etc. This is also evident from the fact that majority of the cases reported to the police are of sexual nature and most of them are booked under the erstwhile Section 67 (which deals with pornography and obscenity in the internet) of the Information Technology Act, 2000 (Balakrishnan, 2009). As the offender and the victim are apart in cyberspace, chances for physical attacks are very low. Therefore, the effect of cybercrime on women victims will be in a form of mental and emotional stress.

1.5 THE EXTENT OF THE PROBLEM

This part of the chapter discusses the magnitude of cybercrime victimization at international, national and state levels.

1.5.1 Cybercrime Victimization: A Global Scenario

According to Internet Crime Complaint Center (IC3, 2015), in US total cybercrime cases reported in 2015 were 288,012, of which 135,614 (47.09%) were
reported by women. The total number of cybercrime complaints reported to IC3 since its inception is 3,463,620. The IC3 report reveals that the total cybercrimes reported in US shows a steady rise from 2013 to 2015. In 2013, the number of cybercrimes reported were 262,813; in 2014 it increased to 269,422 and in 2015 it further increased to 288,012.

The Office for National Statistics (2015) reported that there were 5.1 million estimated cybercrimes and frauds last year in England and Wales. It also revealed that more than 2.5 million offences under the Computer Misuse Act such as hacking, identity theft, malware, and so on were reported.

The UN Broadband Commission (2015) reported that cyber violence against women and children is rising at an alarming pace and 73% of women have already been exposed to or have experienced some form of online violence, which shows the severity of the problem. Further, the report says that 18 per cent of women (9 million) have experienced at least one form of serious Internet violence since the age of 15.

BBC World and GlobeScan Poll (2014) conducted a survey across 17 countries revealed a growing sense of insecurity among users. The poll indicates that people are of the opinion that the two pillars of the modern democracies such as media and internet are at risk. The survey further stated that France is among the countries where respondents do not feel they can express their opinions safely online (76%), alongside South Korea (72%), Spain (66%), Canada, the USA, and Germany (65%) each. Only six surveyed countries have majorities that feel they can express their opinions online safely: Nigeria (71%), India (67%), Indonesia (57%), Kenya (52%), Pakistan and Peru (both 51%) – all of them emerging or developing countries.
Kenya’s office of the Director of Public Prosecutions (2014) acknowledges that only 35% of the women have reported about their victimization, 46.7% have not reported and 18.3% have been unaware of the fact that they have been victimized.

According to Working to Halt Abuse, a non-profitable organization, from 2000 to 2014, 4043 cases were reported to them from all around the world. Out of the total number of cases reported, 70% of the victims were females, 47% of the offenders were males, 1% of the victims were aged below 18 years, 42% of the victims belong to the age group of 18-30 years, 25% of the victims belong to the age group of 31-40 years and 20% of the victims belong to the age group of 41 years and above. The organization further stated that 42% of the victims have not reported their victimization.

The majority of internet users in the EU (61%) are concerned about experiencing identity theft, accidentally discovering child pornography online (51%), online fraud (49%) and scam emails (48%). In addition, 43% are concerned about not being able to access online services because of cyber-attacks and 41% are concerned about accidentally encountering material which promotes racial hatred or religious extremism. 38% of the Internet users stated that they have received emails fraudulently asking for money or personal details (European Commission, 2012).

According to Cybercrime Watch (2011), 25% of the cybercrimes remain unresolved, 75 million scam emails are sent every day claiming 200 victims. The reports said that 73% of Americans have experienced some form of cybercrime.

Statista (n.d.) reported that 60% of the cyber stalking victims in US were female. The statistics also shows that most of the cyber stalking offences were committed using Facebook. Also the prevalence of cyber bullying victimization
among teens is 17.3% and prevalence of sexual and nonsexual cyber dating victimization among teenagers is 26.3%.

1.5.2 Cybercrime Victimization in India

The Symantec Corporation (2016), a security solutions provider, pointed out that due to various developments in information technology like rapid adoption of cloud and integration of Information and Communication Technology in critical infrastructure, India continues to be a top source as well as destination of cyber-attacks. The study also stated that India is the third top source of overall malicious activities including spam, malware, phishing hosts and bots etc.

According to Crime in India (2014), total number of cybercrime cases reported under the IT Act, 2000 in 2010 were 1322 and in the year 2011 it went up to 2213 and in the year 2012 it increased to 3477 cases. A total of 9,622 cases were registered under the cybercrimes in 2014 and 5,693 cases were registered in 2013, which shows an increase of 69% over the previous year. The above report clearly shows the increasing trend of cybercrimes. In addition, in the year 2013, 14.4% (821 out of 5693) of the cases were related to financial gain which increased to 18% in the year 2014.

According to the National Crime Records Bureau (2013), the cybercrime cases registered under the IT Act, 2000 in various states of India in the year 2013 showed an increasing pattern. In 2013, 681 cybercrime cases have been registered in Maharashtra, with an increase of 44.6% when compared to 2012; 635 cases registered in Andhra Pradesh in 2013 with an increase of 48% compared to 2012; 513 cases registered in Karnataka in 2013 with an increase of 24.5% compared to 2012; 372 cases registered in Uttar Pradesh in 2013 with an increase of 81.5%. Kerala was
in the 5th place with 349 cases registered in 2013. The national capital Delhi has registered 131 cybercrime cases with a rise of 72.4% compared to 2012. Gujarat and Odisha have also registered 61 and 63 cases respectively in 2013. Tamil Nadu and Bihar have registered 54 and 23 cases respectively.

The Press Trust of India (2012) reported that as many as 80,000 cybercrime related complaints have been registered with police in Kerala in 2012, of which 50,000 complaints relate to harassment of women through new hi-tech devices. Anandan (2015) observed that some 35,000 complaints were lodged annually with the cyber police in Kerala.

Nanjappa (2015) pointed out that there is a steady increase in the number of cybercrimes in India. Around 13% of the cases were targeted against outraging or blackmailing a woman. Also, 749 cases related to crime in social networking had been reported. In Kerala, 29 cases registered with the cybercrime wing were against women. These were cases of revenge, fraud and blackmail the police found during their investigation.

A study conducted by the Associated Chambers of Commerce and Industry of India (ASSOCHAM) and the Cyber and Network Security Framework (2015) predicted that the number of cybercrimes in India may touch 3,00,000 in 2015, almost double the quantum of previous year. As per the study findings, during the years 2011, 2012, 2013 and 2014, a total number of cybercrimes registered were 13,301, 22,060, 71,780 and 62,189 respectively. The findings indicated that every month nearly 12,456 cybercrime cases were registered in India.
1.5.3 Cybercrimes against Women in Tamil Nadu

According to the State Crime Records Bureau (2009), in the year 2007, 70% of the total 10 cases registered under the IT Act 2000 were related to obscene publication/transmission in electronic form, generally known as cyber pornography. 88% of the persons arrested were under obscene publication/transmission in electronic form. In 2009, three persons were arrested for obscene publication/transmission in electronic form and they were in the age group of 18-30 years. It is also to be noted that out of the total number of cybercrimes registered under the Information Technology Act in the above period clearly indicates that significant number of cases were pertaining to pornography. From this data it can be inferred that women in India are victimized more than men in cyberspace.

Arora (2007) highlighted that victims of cyber violence suffer in silence, preferring not to approach law enforcers. He pointed out that the Chennai city police had received nearly 90 complaints, many of them from women. In 2010, 19 cases were registered in Chennai on Facebook-related complaints. This went up to 35 in 2011 and dipped to 29 in 2012.

The Hindu (2014) reported that the Cyber Crime Cell of Crime Branch-Criminal Investigation Department (CB-CID) received 17,060 complaints related to cybercrimes across the State of Tamil Nadu. Significantly, 2556 cases were related to women. Further, the data revealed that the complaints had been increasing steadily since 2004. In the year 2004, cybercrime cells across the State received 341 complaints. Out of which, 76 were related to women. Moreover, 98 out of 467 cases in 2005, 103 out of 554 in 2006, 97 out of 581 in 2007, 100 out of 539 in 2008, 154 out of 699 in 2009, 204 out of 1,359 in 2010, 278 out of 2,165 in 2011, 501 out of 3,309 in 2012 and 683 out of 4,066 in 2013 were cases related to women. The above
statistics clearly indicate that there has been a consistent increase in the cases of cybercrime victimization against women in the last one decade in Tamil Nadu. However it is also to be pointed out that the hidden criminality or dark figure is relatively more for crime victimization of women in general and cybercrime victimization in particular. It is an irrefutable fact that though women victims of cybercrime come forward to lodge complaints regarding their victimization, it is least likely to result in proper registration of their complaints by the police. It is more appropriate here to note the serious concern expressed by the National Human Rights Commission (NHRC) in the context of the lethargic attitude of the police in dealing with cybercrime cases, particularly against women. According to the NHRC (2015), non-registration of FIRs in cognizable offences, like cybercrimes, amounts to gross violation of human rights as it denies setting the law into motion.

1.6 THE INFORMATION TECHNOLOGY ACT

The Information Technology Act was drafted by the Ministry of Communications and Information Technology, Government of India, in the year 2000. The Act is basically a short version of “United Nations Commission on International Trade Law” (UNCITRAL), a model law on electronic commerce. Earlier, verification of government documents and identity of the individual was manual using paper documents duly signed and issued by the government officers. With the advent of the internet and information technology, everyone started to use the technology, and as a result of it, government office and bank employees need legal verification online. With this objective in mind, Government of India planned to initiate a strong and stringent law to legally accept and verify the identity of the individual online.
The IT Act gives more focus on e-commerce rather than controlling cybercrimes in general. Except some sections (Section 65-72), most of the sections of the IT Act deals with Electronic Governance, to legally accept electronic records and digital signatures in the government offices and its agencies. In order to overcome the above stated issue, the IT Act 2000 was amended again in 2008 so as to accompany certain provisions to control cybercrimes.

The following are some of the sections under the IT Act, 2008 related to cybercrimes:

- **Section 65**: Tampering with computer source.
- **Section 66**: Computer Related offences.
- **Section 66 A**: Punishment for sending offensive messages through communication service, etc.
- **Section 66 C**: Punishment for identity theft.
- **Section 66D**: Punishment for cheating by personation by using computer resource.
- **Section 66 E**: Punishment for violation of privacy.
- **Section 66 F**: Punishment for cyber terrorism.
- **Section 67**: Punishment for publishing or transmitting obscene material in electronic form.
- **Section 67A**: Punishment for publishing or transmitting of material containing sexually explicit act in electronic form.
• Section 67 B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

• Section 67 C: Preservation and retention of information by intermediaries.

• Section 72: Protects an individual’s privacy and confidentiality.

(\textit{The Information Technology Act, 2000})

1.7 LIMITATIONS OF THE INFORMATION TECHNOLOGY ACT

Some of cybercrimes are booked under the Information Technology Act, 2000 (amended in 2008). In addition, some cybercrimes have also been booked under the Indian Penal Code and the Special and Local Laws (SLL). Significantly, it is to be noted that the term cybercrime is nowhere defined in the IT Act 2000 or its amendment in 2008 and the sections used to book cybercrimes are not clearly defined so as to fit the crime within the ambit of law. There is no mention of terms ‘stalking’ and ‘harassment’ in the IT Act. Moreover, there is not even a single word “women” or not even a single section in the IT Act either to safeguard the interest of women or to give legal protection for women in cyberspace. This legal loophole is the cause for the victimization of women as cyber offenders can take advantage to commit crimes hassle free.

1.8 CYBERCRIME CELL

Cybercrime cell is a part of crime branch headed by the Superintendent of Police, to deal with issues of cybercrimes. In Cybercrime cell, cybercrime cases can be lodged for investigation. Unlike traditional criminal cases which have been reported in police stations, cybercrimes cases have exclusively been reported in
cybercrime cell to deal with cybercrime investigation. Unlike traditional crimes which can be dealt in a direct way through police enquiry with the victim and the accused, cybercrime investigation needs a lot of expertise in the digital technology, as cybercrimes are committed in cyberspace using information technology tools. Cyber forensics techniques should be used to bring out the hidden evidence to deal with cybercrimes. As cybercrimes are borderless crimes, Cybercrime cell needs to coordinate with other investigating agencies established in other parts of India and other countries. In addition, Cybercrime cell needs coordination with Internet service providers and cyber forensics lab. Due to tremendous increase of cybercrimes, Cybercrime cell is established in almost all metropolitan cities in India like Bangalore, Chennai, Pune, Trivandrum, Mumbai, Hyderabad, Thane, Delhi, Gujarat, etc.

With the advancement in information technology and increased users of mobile phones, many people started to use the technology irrespective of age and gender which ultimately resulted in a great shift from traditional communication methods to digital communication practice. People started to use Internet and other associated technology to pay their bills and other transactions. On the other side, hacker and cyber criminals started to misuse the cyberspace for various reasons like financial gain, revenge and to control others. Consequently, this resulted in increase of cybercrimes, especially against women. In order to deal with the issue, people started to approach local police stations to lodge complaints. As cybercrimes are committed in cyberspace, police officers in the local police station found it difficult to handle cybercrimes as they lack expertise in digital technology. Taking into account the factors of increase of cybercrime and inefficiency to handle cybercrimes by the police officers, a special unit to address the issues of cybercrime is the need of the hour.
In the year 2002, two cybercrime cells have been established in Tamil Nadu exclusively to detect and investigate cybercrimes. One is established under Chennai City Police to investigate cybercrime cases within the jurisdiction of Chennai city. Another at CB-CID, having jurisdiction throughout the State of Tamil Nadu. Duty of the investigating officers in the cybercrime cell includes receiving complaints from the public, investigate and find out the offender and book cases under the Information Technology Act, 2000. In addition to the IT Act, some of the cases are also booked under the Indian Penal Code (IPC) and the Special and Local Laws (SLL).

1.9 SIGNIFICANCE OF THE STUDY

With the advent of social networking sites, cybercrimes are sprouting and rampant, it has become an issue of concern among the internet community especially among women which is evident from statistics evolved from various organizations. In addition to this, most of the studies clearly pointed out the increase of cybercrimes against women. Though there are many studies conducted by various researchers across the world, in India, the literature regarding cybercrimes is very limited. Hence, the present study is significant to gain insight into the issues of cybercrimes against women and to gain more knowledge about the problems and challenges faced by the victims. Further, accurate victimization rate is impossible since most crimes of such nature go unreported (Yadav, 2010). Hence, the present study is significant to understand the extent of cybercrime victimization. Further, the impact of the cybercrime victimization is not given due importance, as law enforcement personnel trivialize this issue. In addition to this, others blame the victims for their victimization. Hence, the present study is significant to understand the psychological problems the women undergo due to their cybercrime victimization. Also, most of the studies conducted earlier, concentrated less on the
reporting behaviour. Hence, the present study has made an attempt to study the reporting behaviour of the women victims of cybercrime and their attitude towards the police. The findings of the present study would be a significant addition to the existing literature relating to cybercrime victimization of women in India.

1.10 STATEMENT OF THE PROBLEM

The present study aims to understand the nature and extent of cybercrime victimization against women and its impact on them.

1.11 OBJECTIVES OF THE STUDY

The following are the objectives of the study:

1. To study the demographic characteristics of the women victims of cybercrime in Chennai city.

2. To analyze the nature, extent and causes of the victimization of women.

3. To study the victim – offender relationship.

4. To understand the impact of victimization on women.

5. To study the reporting behaviour of the victims and their attitude towards the police.

1.12 SCOPE OF THE STUDY

The study is confined to the city of Chennai, Tamil Nadu. The respondents of the study were women victims of cybercrimes and reported their victimization to the police during the period 2009 - 2013. The word cybercrime is a general term which includes various offences such as crimes against organizations, crimes against
society and crimes against individuals. The present study focuses on cybercrimes against women which range from financial frauds to cyber stalking and harassment. The primary focus of the present research includes the nature and the extent of cybercrime victimization of women, impact of the victimization, reporting behaviour of the victims and the victim’s attitude towards the police.

The review of literature related to the present research has been presented in the ensuing chapter.