CHAPTER SIX
FINDINGS, CONCLUSIONS AND SUGGESTIONS

6.1 Findings
6.2 Conclusions
6.3 Suggestions
6.4 Scope for further research
Research study, findings and conclusions to the problems of cyber law especially IT Act 2000 is presented in this chapter. Similarly, the researcher has made certain suggestions based on observations in the light of the conclusions for strengthening the effectiveness of IT Act 2000. These conclusions and suggestions will definitely increase the use of e-commerce and decrease the number of cyber crimes.

6.1 Findings

By reviewing the data analysis, interpretation and onsite observations the researcher observed the following findings

- It is observed that, majority of the respondents (69.3%) were hesitant to lodge a complaint about the dispute regarding cyber crime. There are various reasons such as people are worried about their reputation, people don’t have time for lodging the complaint regarding cyber crime, people are not sure about whether they will get justice, it requires more time to decide the case due to technicality and people think that the goodwill of the business in the market may diminish. According to category of respondents such as gender, profession, age wise etc, stated that all the reasons for the hesitation are supporting that people are hesitating to approach the court in case of cyber crimes.

- It is found that majority of the respondent said that the time required to get the justice for the case registered under IT Act 2000 is less than one year and one to two years. Average time to get justice regarding cyber crime is 1.82, approximately two years. By observing actual cyber cases filed in the court of law and considering the pending cases the average time required is in between two to three years.

- It is observed that there are various reasons such as poor enforcement of IT Act, peoples are not sure about security, poor knowledge about how
to use E-commerce, non availability of infrastructure facility (i.e. Computer machine, internet connection, etc) and lack of awareness of IT Act 2000 are affecting on the uses of e-commerce instead of enactment of IT Act 2000. According to category of respondents such as gender, profession and age wise etc, stated that all the reasons for not using e-commerce widely even enactment of IT Act.

- It is observed that the average time for getting justice for the cases registered under IT Act 2000 is 1.82 year along with Standard Deviation time is 1.012. Where as Mean time for getting justice for the cases registered under non IT related matter (General) is 2.58 years and Standard Deviation time is 1.329.

- It is observed that there are eight parameters which are affecting the speedy disposal of the matters. Theses parameters are lodging early complaint, role of police as investigation authority, role of prosecutor, role of advocate of accused, role of Judicial Officer, appointment of Special tribunal, non availability of number of Cyber Forensic Labs in comparison with population, and no proper machinery for implementation of the Cyber law. According to category, respondents stated that all the parameters are affecting the speedy disposal of the matters registered under IT Act.

- During the visit at Cyber cell of commissioner office at Mumbai and Pune it is observed that the number of staff appointed at the cell is very less as compare to the registration of the cyber cases. While for other districts like Kolhapur, Satara, Sangli there is no such cyber cell.

- It is found that the staffs in the cyber cell of Police commissioner office are not much qualified where technicality is concerned. They have been given the training of how to investigate the cyber crime but still due to shortfall in technicality they are not comfortable about the cyber crime investigation.
• It is observed that the software and hardware available in the Cyber cell are not up to the mark so the staff of Cyber cell has become handicapped in case of emergency investigation. They need to depend upon the cyber forensic lab which is time consuming, and during this case evidence may get tampered with the offender.

• Numbers of Cyber forensic labs are very less as compared to the number of Cyber Crimes taking place in the country.

• There is dependency on Police of Cyber cell that until the forensic report is not received they are not able to take further step of making charge sheet and approaching the concerned court of law. It is observed that there is much delay in this step. So after making complaint in the Police the case may take few months for registration of case in the court of law.

• It is observed that as Police is under state government authority and their service is transferable, the transfer of officer may break link of cases and the new place of transfer may or may not be related to cyber crimes. In this regard even though the willingness of the officer does nothing if he is transferred from any another department to cyber cell or vice versa.

• As U/S 48 of IT Act Cyber Appellate tribunal will consider the cases registered under IT Act but there is no such court existing till date. So it is affecting on getting the justice regarding cyber crime.

• It is found that Cyber law practitioners as an Advocate are less in number and those who are doing this practice they are doing by accidently i.e. when a relevant brief is there the lawyer will buy the IT Act book for it and he will study the case as well as related provisions. It shows that what ever the justice the people are getting might be biased or offender may escape due to non availability of evidence beyond
doubt.

- Security for the e-commerce is not up to the mark, VPN-SSL (Virtual Private Network - Secure Socket Layer) technology is not being used by every e-commerce transactions.

- The use of digital signature in the country is very less or negligible even though the lack of awareness of digital signature, they do not know how to take digital signature. Getting digital signature is a complex and expensive procedure and its use for common man is approximately nil.

- It is observed that unsecured Wi-Fi connections and networks invite the hackers and terrorists to do their job very easily. It is found that two major terror incidents including the Ahmedabad serial blasts and Mumbai attacks, where the terrorists had used Internet and communication networks in their operations. Unsecured networks and unprotected IP address are misused by terror outfits and other cyber criminals.

- It is observed that because of jurisdiction problem, criminal sitting at out of country can do any offence and no government can arrest the offender if there is no such treaty of exchange of criminals in between these countries.

- As International law is considered as a weak law, the crimes related to cyber space also some what related to international category because the offender may be in or out of country, if it is out of country and doing against the sovereignty of the nation it is very difficulty to arrest the offender and punish accordingly.
6.2 Conclusions

Based on the observations, analysis and statistical techniques the researcher made following conclusions:

6.2.1 Hesitation to approach court of law in case of Cyber Crimes

- It is concluded that people are reluctant to lodge complaint about cyber crime due to various reasons that their reputation is at stake, People don't get time to lodge complaint about the dispute regarding Cyber Crime, much time will be required to decide the case due to technicalities and people were not too sure that they would get justice but in matters of grave seriousness they have no choice, and they do have faith in the justice. It is also concluding that all categories of respondents have supported for the above mentioned reasons for approaching the court of law in case of cyber crimes. Few of the categories conclusions mentioned here are, Professionals do not believe about surety of justice in case of cyber crime cases. Judiciary, Police and advocates are more worried about their reputation than Business Person and experts in case of cyber crime cases due to lack of awareness of cyber law. Respondents between age group 37 to 54 are more worried about their reputation as they are at the peak point of career making.

6.2.2 Time of Disposal for Cyber Crime

- It is concluded that the time required to get justice in case of cyber crime is less than three years, exceptionally it may go above three years.

6.2.3 Reasons for not using E-commerce widely instead of enactment of IT

- It is concluded that there are four reasons why people are not using e-commerce widely instead of enactment of IT Act. Those reasons are a poor enforcement of IT Act 2000, People are not sure about security, Poor knowledge about how to use e-commerce., Non availability of
infrastructure facility (i.e. Computer machine, internet connection, etc) and Lack of awareness of IT Act 2000.

6.2.4 Comparison of General matter with matter registered under IT Act.

- It is concluded that the time requires to decide the cases registered under IT Act 2000 is less than that of the case registered under other than that of IT related (General) matter. Once the forensic lab report is received i.e. expert opinion then the cyber case doesn’t take much time to decide the case.

6.2.5 Parameters for speedy disposal for the matter registered under IT Act.

- It is concluded that there are eight parameters those are affecting on speedy disposal of the matter registered under IT Act. The lodging of early complaint is the main parameter. Role of four persons is affecting on the speed of disposal of cyber case, these four persons are Role of police as an investigation authority, Role of prosecutor, Role of advocate of accused and finally Role of Judicial officer. Other three parameters are also affecting like Appointment of Special Tribunal, Non availability of number of cyber forensic labs and No proper machinery available for implementation of cyber law.
6.3 Suggestions

6.3.1 Hesitation to approach court of law in case of Cyber Crimes

- By using parameters of speedy disposal mentioned in this research; time for the disposal of the matter should be reduced to the months instead of years so that people will not hesitate to approach court of law in case of cyber crimes. If it happens truly for cyber cases then the people will not hesitate to approach the court of law.

- The information about pornography cases should be kept confidential, so that people will not hesitate to approach court of law and the question of reputation can be solved some what.

- People are not having time to approach court of law in case of cyber cases then Online Dispute Resolution System (ODRS) should be applied so that the attendance can be disallowed for the victim. He can approach ODRS from any remote place. Here victim can get relief without going to the court of law & lot of time will be saved. This system is applied for the civil cases and not for criminal cases.

6.3.2 Time of Disposal for Cyber Crime

- To reduce the time of disposal of cyber crime it is needed to have separate tribunal for the cyber cases.

- There should be separate cyber cell office with trained staff and well equipped office with latest software and hardware at every district police commissioner office. Region wise Cyber forensic labs should be present.
6.3.3 Reasons for not using E-commerce widely instead of enactment of IT

- Procedure of getting digital signature needs to be made simple because many people don't know the procedure to acquire digital signature.
  - Fees which is mentioned in sec of 35 (2) of IT Act is not exceeding twenty-five thousand rupees needs to be reduced up to Rs. 5000/- for getting digital signature
  - Section 35(1) of the IT Act says that an application needs to be submitted to the Certifying Authority for the digital signature certificate; the provision should be such that an application can be submitted to the Collector Office of each district of India. Government will take adequate care to send that application to the Certifying Authority.
  - Free training should be given by the Certifying Authority to the public in general for awareness of the digital signature.
- Government should make the infrastructure facility available at remote places to increase e-commerce.
- Government should arrange seminars at district level for training on how to use e-commerce and make people aware about the IT Act 2000.
- VPN-SSL technology should be made compulsory for the traders to trade their business through e-commerce.
- Enforcement of IT Act should be in such way by the authority so that people should feel secure while using e-commerce transaction.

6.3.4 Parameters for speedy disposal for the matter registered under IT Act.
- Cyber Appellate Tribunal which is mentioned in U/S 48 of IT Act 2000 which is in black and white it needs to be implemented. At least in the Special Cyber Appellate tribunal needs to be established minimum at capital city of state on the experimental basis.
• The presiding officer working at this cyber Appellate tribunal must possess minimum bachelor degree of computer science or engineering.

• The investigating authority, like cyber cell of Police Commissioner office and Cyber forensic Labs should be equipped with latest software like Header analyzing software, Advanced Search software, Steganography software, Password cracking tools, Disc imaging tools, image recovery tools and hardware like Powerful computer systems with standard peripherals like CD-ROM drives and CD-writers, desktop and laser printers, scanners, Card readers for examination of various kinds of cards that store data used for authentication and communication e.g. SMART cards, Micro Drives, GSM SIM cards etc. and latest software required for investigation.

• The number of cyber forensic labs need to be increased on the basis of population & use of network in particular area.

• Implementation of IT Act by the authority should be in such a way that people will not hesitate to approach the court of law, so that people will lodge the complaint early regarding cyber crime and it will help to resolve the case early.

• The subject of IT Act 2000 should be made compulsory in the syllabus of LL.B. so that the up coming lawyers will be aware about the cyber law. This will help both the prosecutor as well as the advocate of accused.

• The number of Forensic labs should be increased by considering cyber crime cases. The latest software should be equipped in the cyber forensic labs so that the forensic report can be sent back to the police authority as early as possible. So that police can file charge sheet in the concerned court of law according to the jurisdiction.
Following are some of the software tools that need to be available in the lab.

- Byte Back- Data recovery and computer investigation program software.
- Digit- Digital information and gathering and investigation technologies.
- Drive spy- It is a forensic dos shell. It is designed to evaluate and extend the capabilities of dos to meet forensic needs.
- Encase- It is capable of making forensic quality, recording of data stored on pc’s and of recovering some insecurely deleted data.
- Forensic Tool Kit (FTK) - Access data product.
- Gdisk- For Re-portioning purpose.
- Ghost- Create a new record from old file.
- Drive works- Reuse of drives.
- Linux DD (SMART)- Self monitoring, analysis and reporting technology.
- Hash Keeper- Password manager or create.
- Ilook (LEOs only)- Used to acquire and analyse digital media.
- Maresware- Date analysis and electronic data security.
- Microsoft Technet- Is a Microsoft program and resource for technical information news and events for IT.
- Password Recovery Toolkit (PRTK)- Password recovery purposes.
- Safeback- for the purpose of maintaining file..
- Thumbs Plus- For graphics maintaining purpose.
- Drive Image- Disk image
6.3.5 General suggestions

- There should be provision in cyber law throughout the entire world for creation of e-mail account. The provision should be like the procedure of getting phone number. So that e-mail can be treated as evidence. It will help in for reducing the number of cyber crimes.

- The Police officers appointed at the cyber cell of commissioner office should possess at least bachelor’s degree in computer science or engineering along with latest training about how to investigate the cyber crimes.

- Cyber space is available across the whole world. So the problem of jurisdiction becomes very complex. This problem can be solved by all the nations together. There should be one law throughout the world for cyber crimes.

- Government should make public announcement about Nigerian Fraud. So that the innocent citizens of India will not be cheated by the criminals.

- For Cyber law instead of Criminal Procedure Court (Cr. P. C), there should be separate procedural law which the whole world should accept and recognize.

6.4 Scope for further Research

- Further Research can be done on the topic of Nigerian Fraud which is not in the ambit of this research.

- Research can be done to solve the problem of Jurisdiction in case of Cyber Crime, because the area is not binding to the internet, any one sitting at any place, can commit cyber crime and the nation out of their territory can not do much.
Online Dispute Resolution System can be studied more critically; additional parameters can be suggested to establish this ODRS system world wide.

A common law which is uniformly implemented through out the world should be developed. A research can be done in this regard.

CONCLUDING REMARK:
It is concluded that, Cyber Law is not effectively implemented and hence the main objective of enactment of IT Act 2000 is not achieved. If the suggestions given by the researcher are properly incorporated; the Cyber Law will be implemented more effectively.