PREFACE

Banking is the oldest form of trade and business in the world and has its survival from ancient times in India. Since 1980, the economic and financial sector reforms were introduced in India. Banking industry has gone through significant changes in recent past. Almost all the banks in India have adopted Information Technology solutions for rendering the banking services to their customers by using the IT tools & techniques to fulfill the needs of the customers. In the age of information technology the swift expansion of, telecommunications, computers and other technologies has led to new forms of worldwide crimes known as “Cyber Crimes”. Cyber crimes have practically no boundaries and may affect every country in the world. Mounting Cyber crimes across the world is a very severe warning in the up-coming time and produces one of the most complicated challenges before the law enforcement machinery.

The transformation in committing crimes with the help of information technology; the law should not be a mute spectator but to transform itself according to the changing environment. There was a need to redefine the old laws in the changing environment. Most of the existing laws in India are either created by the British Government or enacted after the independence within the first three decades and based on physical environment, geographical boundaries, tangible documents and records.

To curb & control the crimes arising out of the Internet & Computer Technology, in the year 2000, the fundamental law for electronic transactions in India has come forward in the form of the Information Technology Act, 2000. The IT Act 2000 was amended in the year 2008. The reason for amendment of IT Act 2000 was certain lacunas and shortcoming in it. The IT Act 2000 provides the legal infrastructure for Information Technology in India in general and Banking & Financial Institutions in particular. The Information technology Act, 2000 and The Information Technology Amendment Act 2008 provides the safeguard against the cyber crimes up to certain extent but does not provides the absolute protection and does not covers all the aspects of Information Technology. A careful analysis of the IT Act 2000 and ITAA2008 reveals that the new amendments to the IT Act 2000 are not at all sufficient in the context of growing needs
of India and have various noticeable loopholes in it. Therefore the miscreants are getting the benefit due to prominent shortcomings in the law.

As the user of E-banking grows and the range of online interaction expands, cyber crime incidents of fraud in the Commercial Banks in India are enormously increased. The present research work is the critical study of how badly Indian e-banking is affected by cyber-crime and to test whether the newly enacted laws will help in preventing and prosecuting the cyber crimes. This study is an effort to find out whether IT Act, 2000 & IT Amendment Act, 2008 is effective and efficient enough for controlling the recent developments in cyber crimes against e-banking in India. It is also an attempt to expose up to what extent does the other law (new and old) in India having legal control over cyber crime against e-banking in India.

The cyber crime has the global impact and it affects the people of every nook & corner of the world. Nobody will deny that there is an urgent need to bring changes in the Information Technology Act to make it more effective to combat with cyber crime. I hope that the suggestions may throw light on the insufficiency of legal regulations and remedy available thereof for e- banking in India. I suggested where the full proof amendments in legal provisions are required to facilitate legal control of cyber crimes against e- banking in India.