PATENT LAW:

Patent law is a specific area of law that encompasses the legal regulation, jurisprudence, and enforcement of specific intellectual property rights known as *patent rights*. A patent is a government issued right granted to individuals or groups that protects their original inventions from being made, used, or sold by others without their permission for a set period of time. While patents can be legally obtained without the use of an attorney, an attorney who specializes in patent law can help ensure that their client's patent is enforceable by law. Because patent law pertains to intellectual property, which is like any other property in that it can be legally sold, exchanged, traded, or abandoned, the finer points of patent law are frequently amended as technology changes. This is another reason why an attorney specializing in patent law is of significant use to those seeking a patent.

Basically, A Patent is a legal monopoly, which is granted for a limited time by a country to the owner of an invention. Merely to have a patent does not give the owner the rights to use or exploit the patented invention. That right may still be affected by other laws such as health and safety regulation or the food and drugs regulation or even by other patents. The patent, in the eyes of the law, is a property right and it can be given away, inherited, sold, licensed and can even be abandoned. As it is conferred by the government, the government, in certain cases even after grant or even if it has been, in the meantime, sold or licensed, can revoke it.

- A Patent gives an inventor the right for a limited period to stop others from making, using, selling or importing an invention without the permission of the inventor. That is why patent is called a "negative right"
- Patents are generally concerned with functional and technical aspects of products and processes and must fulfill specific conditions to be granted.
- Most patents are for incremental improvements in known technology - evolution rather than revolution. The technology does not have to be complex.
- Patent rights are territorial; an Indian patent does not give rights outside of India.
- Patent rights last for up to 20 years in India and in most countries outside India.
- Depending on where you wish your patent to be in effect, you must apply to the appropriate body. In India, this is The Indian Patent Office. There are various Patent Offices around the world. Alternatively, a Patent Agent can apply on your behalf.

REQUIREMENTS OF PATENT LAW:

The invention must be useful, novel (new), and non obvious. If so, the inventor is entitled to patent protection, and the government is obliged to give it. Patent protection excludes all others except the patent holder from making, using, selling or offering to sell the patented invention. However if another invention which has patent is used in the actual physical creation of the new invention, the patent owner may have to obtain certain rights from the first patent holder.

ADVANTAGES OF PATENT LAW:

Some of the more obvious advantages of patent law is that the patent owner holds exclusive right to the invention and that others must pay either a license fee or obtain some other type of right to produce

or manufacture the patented item. Additionally a company may invent something that is not necessarily useful to the company's overall goals at the time, and then they would have to decide whether the lengthy and sometimes expensive patent application process is in their best interest.

COPYRIGHT LAW:

The Copyright Act, established in 1976, is located in Title 17 of the U.S. Code, from sections 101 through 122.Copyright refers to laws that regulate the use of the work of a creator, such as an artist or author. This includes copying, distributing, altering and displaying creative, literary and other types of work. Unless otherwise stated in a contract, the author or creator of a work retains the copyright.

For a copyright to apply to a work, it must be an original idea that is put to use. The idea alone cannot be protected by copyright. It is the physical use of that idea, such as an illustration or a written novel that is covered under copyright law.

It is also be defined as, "As a copyright holder, you have the exclusive right to reproduce or make copies of a creative work. You can also distribute or sell copies; make a derivative work (for example, turn a novel into a movie); and perform or display the work publicly".

Copyrightable Material are includes, Creative works, including literature, art and music, can be copyrighted if they are original and have been put in tangible form. A copyright is a form of protection by the laws of the United States to authors of "original works of authorship." This includes literary, dramatic, musical, artistic and certain other intellectual works. This protection is available to both published and unpublished works. Material not protected by copyright (or otherwise protected) is available for use by copyrighted work can prevent others from copying, performing or otherwise using the work without the author's consent.

There are four main forms of remedies in the event that copyright infringement takes place:

1. An injunction to stop the production of further copies.

2. A demand that all copies are surrendered to the copyright owner.

3. Damages for losses suffered by the copyright owner.

4. An account of profits made by the infringer.

ADVANTAGES OF COPYRIGHT LAW:

1. LEGAL RESOURSE:

Federal copyright law prohibits authors from suing for breaches of copyright law unless the work has been registered with the U.S. Copyright Office. This means that if someone steals your work, you cannot file a lawsuit until the work has been registered. While you might think that you'll be able to

register the work as soon as copyright infringement is an issue, there will be added expense and time lost. You'll have to pay more to expedite the copyrighting process, and filing your lawsuit will become more complicated. Not to mention, the judge or jury who hears your case will wonder why you didn't initially copyright your work, which can work in the favor of the defendant in your case.

2. **DAMAGES:**

The plaintiff in a copyright infringement case can sue for the actual infringement of the copyright even if the registration was completed after the infringement occurred. However, the plaintiff will not be entitled to statutory damages and court fees unless the registration was completed in a "timely manner". Currently, a timely manner is considered within three months of publication of the creative work. This means that if you don't copyright your work, you will not be entitled to statutory damages when and if an infringement occurs. In this case, the plaintiff will be required to prove actual damages.

3. **SPEED:**

Typically, copyright infringement cases involve the perpetrator's ability to profit from the use of a copyrighted creative work. If you win a copyright lawsuit in court, then the infringer will be required to take the copyrighted work off the market, but this could be months or years after the actual infringement took place. If, however, you have copyrighted your work by registration, then you are entitled to the removal of the copyrighted work from the market immediately. This means that gratification is much faster, and will expedite the process of removing the offending material from the market.

DATA MINING:

The term data mining has been stretched beyond its limits to apply to any form of data analysis. Some of the numerous definitions of Data Mining, or Knowledge Discovery in Databases are: Extraction of interesting information or patterns from data in large databases is known as data mining.

According to William J. Frawley, Gregory Piatetsky-Shapiro and Christopher J. Matheus 'Data Mining, or Knowledge Discovery in Databases (KDD) as it is also known, is the nontrivial extraction of implicit, previously unknown, and potentially useful information from data. This encompasses a number of different technical approaches, such as clustering, data summarization, learning classification rules, finding dependency networks, analyzing changes, and detecting anomalies'. According to Marcel Holshemier and Arno Siebes "Data mining is the search for relationships and global patterns that exist in large databases but are 'hidden' among the vast amount of data, such as a relationship between patient data and their medical diagnosis. These relationships represent valuable knowledge about the database and the objects in the database and, if the database is a faithful mirror, of the real world registered by the database".

Data mining refers to "using a variety of techniques to identify nuggets of information or decision-making knowledge in bodies of data, and extracting these in such a way that they can be put to use in the areas such as decision support, prediction, forecasting and estimation. The data is often voluminous, but as it stands of low value as no direct use can be made of it; it is the hidden information in the data that is useful".

Data mining is concerned with the analysis of data and the use of software techniques for finding patterns and regularities in sets of data. It is the computer which is responsible for finding the patterns by identifying the underlying rules and features in the data. The idea is that it is possible to strike gold in unexpected places as the data mining software extracts patterns not previously discernable or so obvious that no-one has noticed them before.

Data mining analysis tends to work from the data up and the best techniques are those developed with an orientation towards large volumes of data, making use of as much of the collected data as possible to arrive at reliable conclusions and decisions. The analysis process starts with a set of data, uses a methodology to develop an optimal representation of the structure of the data during which time knowledge is acquired. Once knowledge has been acquired this can be extended to larger sets of data working on the assumption that the larger data set has a structure similar to the sample data. Again this is analogous to a mining operation where large amounts of low-grade materials are sifted through in order to find something of value.

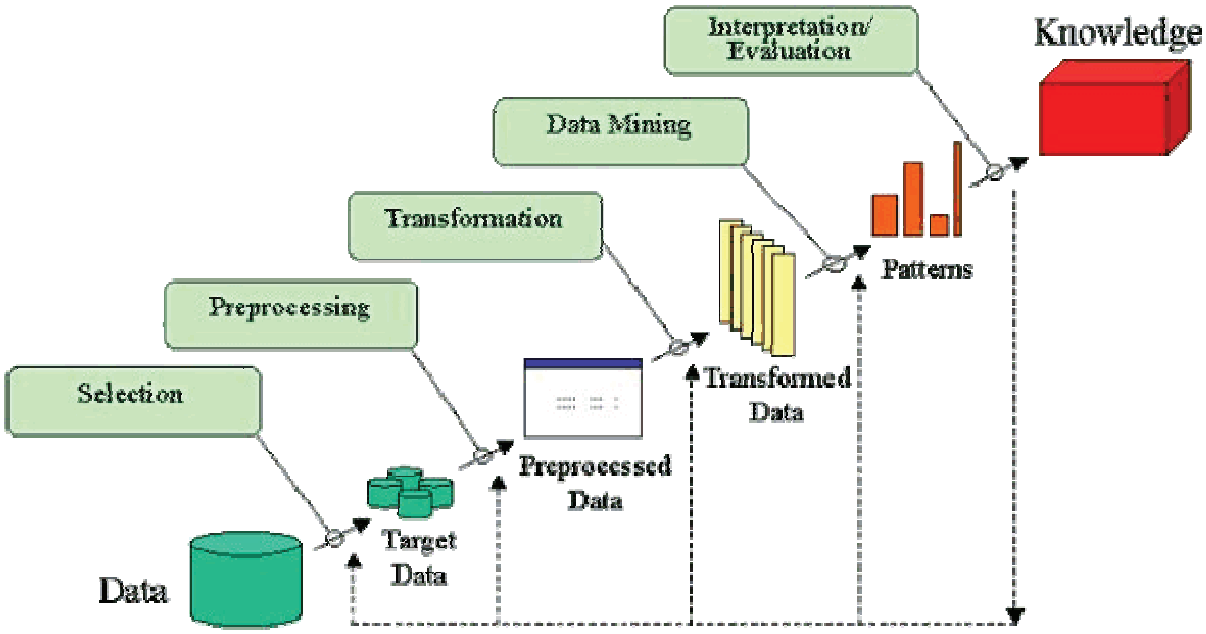

FIGURE: BASIC STEPS FOR DATA MINING

Data mining is defined as:

- It is the step in the process of knowledge discovery in databases, that inputs predominantly cleaned, transformed data, searches the data using algorithms, and outputs patterns and relationships to the interpretation/evaluation step of the whole knowledge discovery in databases process.

- The science of extracting useful information from large data sets or databases.

- Data mining is a new discipline lying at the interface of statistics, database technology, pattern recognition, machine learning, and other areas. It is concerned with the secondary analysis of large databases in order to find previously unsuspected relationships which are of interest or value to the database owners.

- It is the exploration and analysis, by automatic and semi-automatic means, of large quantities of data in order to discover meaningful patterns and rules

SECURITY IN SDLC:

The software development life cycle, or SDLC, encompasses all of the steps that an organization follows when it develops software tools or applications. Organizations that incorporate security in the SDLC benefit from products and applications that are secure by design. Those that fail to involve information security in the life cycle pay the price in the form of costly and disruptive events.

In an organization that's been around for several years or more, the SDLC is well-documented and usually includes the steps that are followed and in what order, the business functions and/or individuals responsible for carrying out the steps and information about where records are kept.

A typical SDLC model contains the following main functions:

Conceptual definition: This is a basic description of the new product or program being developed, so that anyone reading it can understand the proposed project.

Functional requirements and specifications: This is a list of requirements and specifications from a business function perspective.

Technical requirements and specifications: This is a detailed description of technical requirements.

Security issues are much more expensive to fix once a web application is in production. Security should be addressed at all stages of the software development life cycle (SDLC), also known as the systems life cycle (SLC).

Although there are many interpretations of the life cycle of a web system, the following list of stages is typical:

1. Requirements
2. Feasibility study
3. Design
4. Specification
5. Development (Coding)
6. Testing
7. Implementation
8. Operation and maintenance
9. Disposal

Every organization has its own culture and processes, so the generic model is only an illustration. The SDLC may also vary from project-to-project, and whether any work is out-sourced or not. Development teams may be using an agile approach. In all of these, there will be different considerations to make when considering how best to build security in to the development process.

Senior support for information security is necessary. Security requirements need to be defined as early as possible during the SDLC. From formation of a security policy, undertaking threat modeling and feeding this analysis into the system and architectural design, to create a security model and then a full security specification. Training of developers to help them write secure code combined with development of

coding guidelines and internal code reviews, project security reviews and rigorous security testing during the development, testing and implementation phases will lead to a software system which can potentially be properly certified and accredited.

The best approach and amount of effort, to build security into the SDLC will be different for each organization and application. An assessment of existing practices, tools, languages and frameworks, and the types of risks the software faces are a useful starting point. A gap analysis can also be undertaken to compare existing information assurance practices with those in other similar organizations. It is also common to perform a thorough application identification process and then rank them by risk, to determine where most effort should be spent. Not all applications are business critical; not all applications process sensitive data; not all applications are publicly accessible. This information is used to define a software security roadmap, which can then be subsequently implemented.

CYBER CRIME:

Information is a resource which has no value until it is extracted, processed and utilized. Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done.

Information technology is affecting us as individual and as a society. Information technology stands firmly on hardware and software of a computer and tele-communication infrastructure. But this is only one facet of the information Technology, today the other facets are the challenges for the whole world like cyber crimes and more over cyber terrorism. When Internet was first developed, the founding fathers hardly had any inkling that internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulations. With the emergence of the technology the misuse of the technology has also expanded to its optimum level the examples of it are:

- Cyber stalking
- Cyber harassment
- Cyber fraud
- Cyber defamation
- Spam
- Hacking
- Trafficking
- Distribution
- Posting and dissemination of obscene material including pornography
- Indecent exposure and child pornography etc.

The misuse of the technology has created the need of the enactment and implementation of the cyber laws but whether this cyber laws are capable to control the cyber crime activities, the question requires the at most attention.

There can be no one exhaustive definition about Cybercrime.

“Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against property, government and people at large.” OR

"Acts those are punishable by the Information Technology Act".

A simple sturdy definition of cyber crime would be, "unlawful acts wherein the computer is either a tool or a target or both".

TYPES OF CYBER CRIME:

1. **Privacy violation:**

The law of privacy is the recognition of the individual's right to be let alone and to have his personal space inviolate. The right to privacy as an independent and distinctive concept originated in the field of Tort law, under which a new cause of action for damages resulting from unlawful invasion of privacy was recognized. In recent times, however, this right has acquired a constitutional status, the violation of which attracts both civil as well as criminal consequences under the respective laws. The intensity and complexity of life have rendered necessary some retreat from the world. Man under the refining influence of culture, has become sensitive to publicity, so that solitude and privacy have become essential to the individual. Modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. With the advent of information technology the traditional concept of right to privacy has taken new dimensions, which require a different legal outlook. To meet this challenge recourse of Information Technology Act, 2000 can be taken.

The various provisions of the Act aptly protect the online privacy rights of the citizens. Certain acts have been categorized as offences and contraventions, which have tendency to intrude with the privacy rights of the citizens.

2. **Secret information appropriation and data theft:**

The information technology can be misused for appropriating the valuable Government secrets and data of private individuals and the Government and its agencies. A computer network owned by the Government may contain valuable information concerning defense and other top secrets, which the Government will not wish to share otherwise. The same can be targeted by the terrorists to facilitate their activities, including destruction of property. It must be noted that the definition of property is not restricted to moveables or immoveable alone.

3. **Demolition of e-governance base:**

The aim of e-governance is to make the interaction of the citizens with the government offices hassle free and to share information in a free and transparent manner. It further makes the right to information a meaningful reality. In a democracy, people govern themselves and they cannot govern themselves properly unless they are aware of social, political, economic and other issues confronting them. To enable them to make a proper judgment on those issues, they must have the benefit of a range of opinions on those issues. Right to receive and impart information is implicit in free speech. This, right to receive information is, however, not absolute but is subject to reasonable restrictions which may be imposed by the Government in public interest.

4. **Distributed denial of services attack:**

The cyber terrorists may also use the method of distributed denial of services (DDOS) to overburden the Government and its agencies electronic bases. This is made possible by first infecting several unprotected computers by way of virus attacks and then taking control of them. Once control is obtained, they can be manipulated from any locality by the terrorists. These infected computers are then made to send information or demand in such a large number that the server of the victim collapses. Further, due to this unnecessary Internet traffic the legitimate traffic is prohibited from reaching the Government or its agencies computers. This results in immense pecuniary and strategic loss to the government and its agencies.

It must be noted that thousands of compromised computers can be used to simultaneously attack a single host, thus making its electronic existence invisible to the genuine and legitimate citizens and end users. The law in this regard is crystal clear.

5. **Network damage and disruptions:**

The main aim of cyber terrorist activities is to cause networks damage and their disruptions. This activity may divert the attention of the security agencies for the time being thus giving the terrorists extra time and makes their task comparatively easier. This process may involve a combination of computer tampering, virus attacks, hacking, etc.

In India Information Technology Act, 2000 deals with the cyber crime problems. It has some positive as well as negative aspects.

Positive Aspects of the IT Act, 2000:

1. Prior to the enactment of the IT Act, 2000 even an e-mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the IT Act, 2000 changed this scenario by legal recognition of the electronic format. Indeed, the IT Act, 2000 is a step forward.

2. From the perspective of the corporate sector, companies shall be able to carry out electronic commerce using the legal infrastructure provided by the IT Act, 2000. Till the coming into effect of the Indian Cyber law, the growth of electronic commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.

3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the IT Act, 2000.

4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a back up. Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy if any one breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the IT Act, 2000 is in the form of monetary damages, by the way of compensation, not exceeding Rs. 1, 00, 00,000.

5. IT Act, 2000 has defined various cyber crimes which includes hacking and damage to the computer code. Prior to the coming into effect of the Indian Cyber law, the corporate were helpless as there was no legal redress for such issues. But the IT Act, 2000 changes the scene altogether.

The Grey Areas of the IT Act, 2000:

1. The IT Act, 2000 is likely to cause a conflict of jurisdiction.

2. Electronic commerce is based on the system of domain names. The IT Act, 2000 does not even touch the issues relating to domain names. Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law.

3. The IT Act, 2000 does not deal with any issues concerning the protection of Intellectual Property Rights I the context of the online environment. Contentious yet very important issues concerning online copyrights, trademarks and patents have been left untouched by the law, thereby leaving many loopholes.

4. As the cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act, 2000 makes it appear as if the offences detailed therein are the only cyber offences possible and existing. The IT Act, 2000 does not cove various kinds of cyber crimes and Internet related crimes. This Include:-

a) Theft of Internet hours
b) Cyber theft
c) Cyber stalking
d) Cyber harassment
e) Cyber defamation
f) Cyber fraud
g) Misuse of credit card numbers
h) Chat room abuse

5. The IT Act, 2000 has not tackled several vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few. Privacy issues have not been touched at all.