TY BTech CSE (CSF) Semester (AY 2023-2024)

Computer Science and Engineering

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Unit 4: Legal Framework and Cyber Law

Introduction, Cybercrime and the Legal Landscape around the World, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Digital Signatures and the Indian IT Act, Amendments to the Indian IT Act.

Cybercrime

Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs.

Cyber Criminals used:

a. The computer as a Target: using a computer to attack other computers. E.g. Hacking, virus, DoS

b. The computer as a weapon: using a computer to commit real world crimes. E.g Cyber terrorisum, credit card frauds, child pornography etc.

Categories:

a. Against Person:- Harassment via email, cyber stalking, email spoofing.

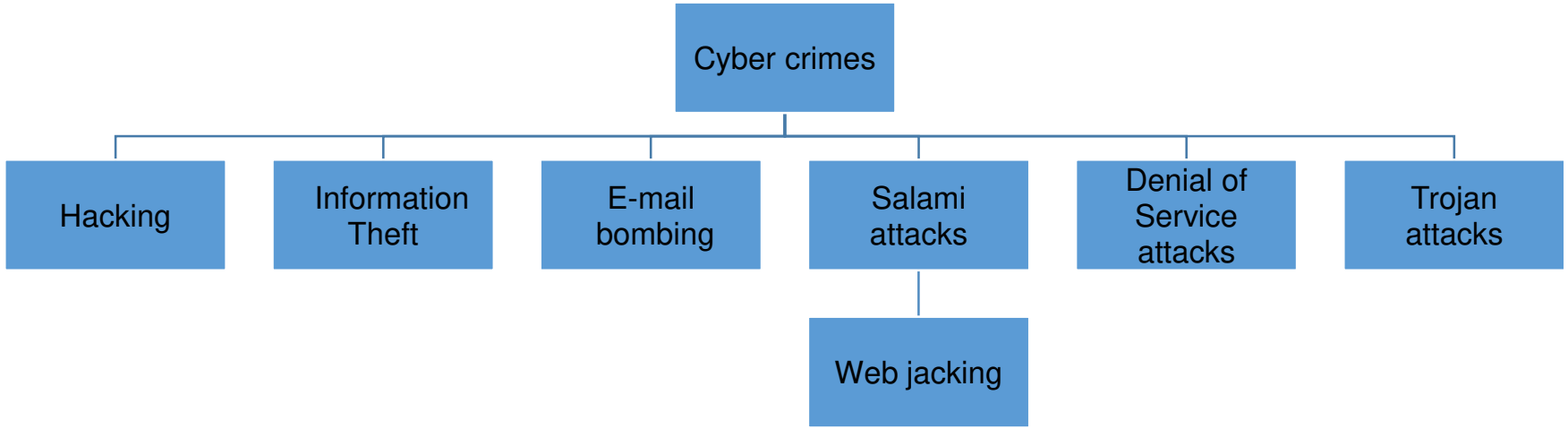
b. Against Property:- Unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs and unauthorized possession of computerized information.

c. Against Government:- Cyber terrorism, Damaging critical information infrastructure. This crime manifests itself into terrorism when an individual cracks into government or military maintained website

Types of cybercrime

Hacking:- Hacking in simple terms means an illegal intrusion into a computer system and/or network.
Denial of service attack:- Act by criminal, who floods the bandwidth of the victims network. Its an attempt to make a machine/network resources unavailable to its intended users.
Virus Dissemination:- Malicious software that attaches itself to other software.
Computer Vandalism :- Damaging or destroying data rather than stealing, transmitting virus
Cyber Terrorism:-Use of internet based attacks in terrorist activities.
Software Privacy:- Theft of software through the illegal copying of genuine programs.
Identity theft:- As per cyber law, is the stealing of someone's identity and passing it off as your own in an online forum.
Cyberstalking:- as per cyber law, is the usage of an entity's social media or online information to threaten, stalk, or extort money from them.
Social engineering:- The concept of Social engineering in cyber law is stealing by gaining confidence.
Potentially unwanted programs (PUPs.):- It is usually popular advice by cyber law experts to avoid installing unknown software for the simple reason that malware can be installed into your computer and files can be stolen.

Types of cybercrime



- Financial fraud: 11%
- Sabotage of data/networks: 17%
- Theft of proprietary information: 20%
- System penetration from the outside: 25%
- Denial of service: 27%
- Unauthorized access by insiders: 71%
- Employee abuse of internet privileges 79%
- Viruses 85%

Cyber Crime and the Legal Landscape around the World

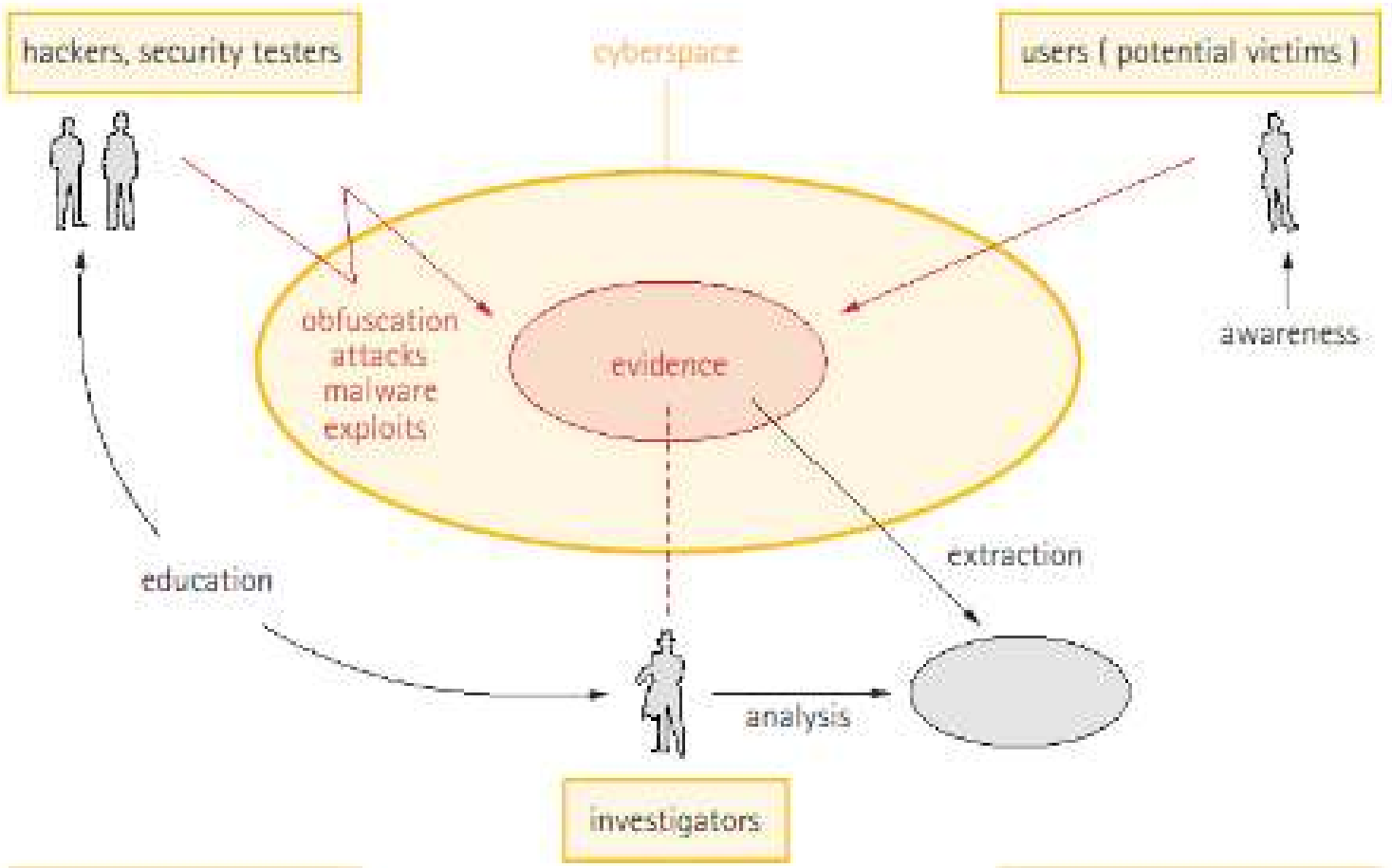


Figure 1. The Landscape of Cybercrime with its Actors.

Cyber Crime and the Legal Landscape around the World

https://www.itechlaw.org/survey/the-cyber-crime-regulations---landscape-of-the-world---countries

1 Are there any dedicated laws and / or administrative measures regulating IT – Security? If yes, which are those? (Please provide a list)?

1.1 Are there any general dedicated laws and / or administrative measures regulating IT-Security? If yes, which are those and what is the content? (Please identify the most important obligations as to IT- Security standards, notification duties, obligatio

1.2 Are there any specific dedicated laws and / or administrative measures regulating IT-Security regarding critical infrastructures (such as energy, transportation, financial institutions/banks, water supply etc.)? If yes, which are those and what is the

1.3 Which authorities are responsible for enforcing the regulations under 1.1 and 1.2? What kind of legal instruments / rights are they furnished with (fines, audit/investigation rights, etc.)?

2 Are there any laws and / or administrative measures regarding privacy/data protection, which also impose obligations concerning IT - Security? If yes, which are those (Please provide a list)?

2.1 Please specify the obligations regarding IT – Security according to 2 above, e.g. Security standards, obligations in case of data breach, etc.)?

2.2 Which authorities are responsible for enforcing the regulations under 2 and 2.1? What kind of legal instruments / rights are they furnished with (fines, audit/investigation rights, etc.)?

1 Are there any dedicated laws and / or administrative measures regulating IT – Security? If yes, which are those? (Please provide a list)?

India

Indian rules relating to IT-security is primarily prescribed under the Information Technology Act, 2000 ("IT Act"). Additionally, the following rules framed under the IT Act enumerates the specific legislations and rules pertaining to IT-Security:

i. The Information Technology (Certifying Authority) Regulations, 2000
ii. The Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004
iii. The Information Technology (Security Procedures) Rules , 2004 as amended by (Amendment) Rules, 2015
iv. The Information Technology (Other Standards) Rules, 2009
v. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
vi. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
vii. The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2011
viii. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
ix. The Information Technology (Guidelines for Cyber Café) Rules, 2011
x. The Information Technology (Intermediaries Guidelines) Rules, 2011
xi. The Information Technology (Electronic Service Delivery) Rules, 2011
xii. The Information Technology (National Critical Information Infrastructure Protection centre and manner of performing function and duties) Rules, 2013
xiii. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013

Answer provided by: G.V. Anand Bhushan: Shardul Amarchand Mangaldas & Co.

Key regulation: **IT Act 2000** (https://www.indiacode.nic.in/handle/123456789/1999)

- The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with electronic documents, e-signature, digital authentication and cybercrime.

- 1986- internet was introduced, 1995- launched in India (education, research community), 1999- Indian Railway reservation, 2000- arrival of cable internet (rediffmail, yahoo, ebay)

- Due to increase crime in cyber space, Govt. of India understood the problems of internet user and for safeguarding the interest of internet users, this act was made.

The IT Act, 2000 has two schedules:

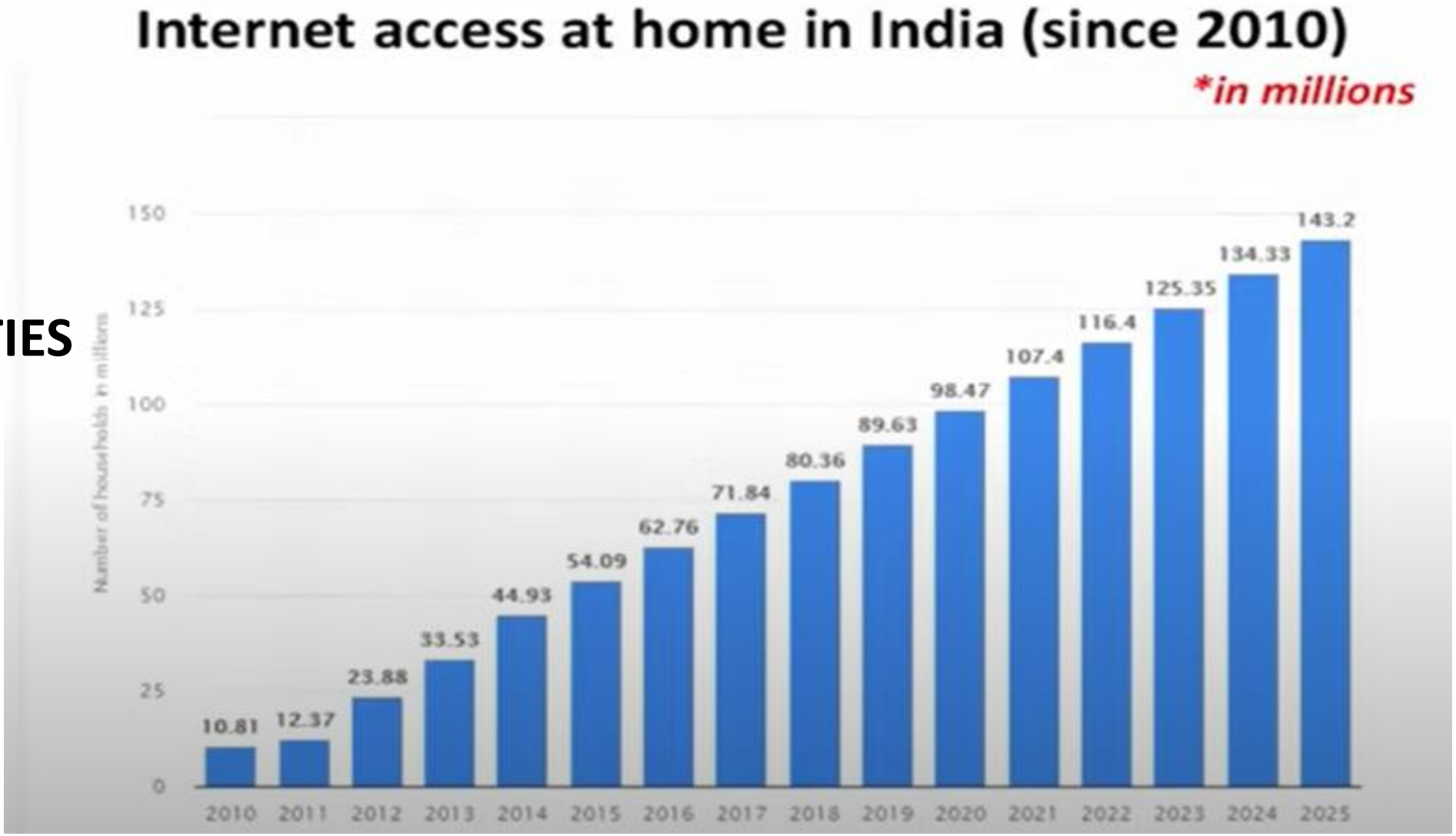
First Schedule –
Deals with documents to which the Act shall not apply.
Second Schedule –
Deals with electronic signature or electronic authentication method.

Objectives

- It is objective of IT Act 2000 to give legal recognition to any transaction which is done by electronic way or use of internet.
- To give legal recognition to digital signature for accepting any agreement via computer.
- To provide facility of filling document online relating to school admission or registration in employment exchange.
- According to IT Act 2000, any company can store their data in electronic storage.
- To stop computer crime and protect privacy of internet users.
- To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.

New IT Rules 2021

- **VULNERABILITIES**



The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce.

1. The act was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime.

2. Under this law, for any crime involving a computer or a network located in India, foreign nationals can also be charged.

3. The law prescribes penalties for various cybercrimes and fraud through digital/electronic format.

4. It also gives legal recognition to digital signatures.

5. The IT Act also amended certain provisions of the Indian Penal Code (IPC), the Banker's Book Evidence Act, 1891, the Indian Evidence Act, 1872 and the Reserve Bank of India Act, 1934 to modify these laws to make them compliant with new digital technologies.

6. In the wake of the recent Indo-China border clash, the Government of India banned various Chinese apps under the Information Technology Act.

List of offences and the corresponding penalties:

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹2,00,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹5,00,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to ₹1,00,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to ₹1,00,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹1,00,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹2,00,000
66F	Acts of cyberterrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to ₹10,00,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to ₹10,00,000
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to ₹1,00,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to 2 years, or/and with fine up to ₹1,00,000
72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to ₹1,00,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to ₹5,00,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to ₹1,00,000
74	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to ₹1,00,000

Amendments to the Indian IT Act

Amendment of 2008:

- Introduced provisions related to the punishment for cyber terrorism under Section 66F, ensuring stringent action against those engaging in cyber warfare activities.
- Strengthened the regulatory framework for Certifying Authorities (CAs) and their functioning to enhance the security of digital signatures.

Amendment of 2013:

- Enhanced provisions related to electronic signatures, enabling their usage for various government services and documents.
- Introduced Section 66A, which dealt with punishment for sending offensive messages through communication services, although this section was later struck down by the Supreme Court in 2015 for being unconstitutional.
- Established the National Critical Information Infrastructure Protection Centre (NCIIPC) to safeguard critical information infrastructure from cyber threats.

Recent amendments and Impact

Amendment of 2021:

- Strengthened data protection laws, emphasizing the importance of personal data privacy and defining stricter penalties for data breaches and violations.
- Introduced regulations for intermediaries, holding them accountable for content moderation and user data protection.

Impact of Amendments:

- **Enhanced Cybersecurity:** Stricter provisions deter cybercrimes and protect sensitive data, fostering a safer digital environment.
- **Promotion of Digital Transactions:** Clear regulations regarding electronic signatures and online transactions encourage digital adoption in various sectors.
- **Improved User Confidence:** Robust legal frameworks instill trust in digital interactions, boosting user confidence in online services and transactions.

IT Rules Background

In 2018, the Supreme Court had observed that the Indian Government may frame necessary guidelines .

In 2020, an Ad-hoc committee of the Rajya Sabha submitted its report on the issue of social media pornography and its effect on children and society. The report recommended tracing the originator of such content.

In 2020, the GOI also brought OTT platforms under the ambit of the Information and Broadcasting Ministry.

These new rules supersede the previously enacted Information Technology (Intermediary Guidelines) Rules 2011.

- The Rules aim to provide a robust complaint mechanism for the users of social media and over-the-top (OTT) platforms to address their grievances.
- They place special emphasis on the protection of women and children from sexual offences on social media.
- The rules stress the point that online content publishers and social media intermediaries should follow the Constitution of the country and subject themselves to domestic laws.
- With these rules, India joins other international regimes that have provisions for digital media regulation and provides a comprehensive mechanism for the protection of digital media consumers.

- The Central Government enacted the Information Technology (Guidelines For Intermediaries And Digital Media Ethics Code) Rules, in February 2021. The Rules largely cover OTT platforms and social media.

The new Rules have been passed under

1. Section 69 A(2) :- New Guidelines for Social Media Intermediaries
2. Section 79 (2) (c): - New Guidelines for OTT Platforms, News Publishers & Digital Media
3. Section 87:- New IT Rules Concerns

New Guidelines for Social Media Intermediaries

I. The new rules classify social media intermediaries into two categories:

1. Social media intermediaries – (< 50 lakh or < 5 million)
2. Significant social media intermediaries - registered users (=/> 50 lakh or 5 million)

The above classification is based on the user size and once it has been defined through the notification of the Government, it would act as the threshold between the two. This is because there are additional compliance measures for significant social media intermediaries given the large number of users and the volume of content they process.

II. Due diligence to be followed by intermediaries under the new rules

- According to the new rules, in case due diligence is not followed by the intermediary, the safe harbor provisions would not apply to them.

III. Mandatory grievance redressal mechanism

- Intermediaries shall appoint a Grievance Officer to deal with complaints and share the name and contact details of such officers.
- This officer should acknowledge the complaint received within 24 hours and resolve the issue within 15 days.

IV. Ensuring online safety and dignity of users

- Intermediaries should remove or disable, within 24 hours of the complaint received for the content which are not acceptable.
- Complaints of such nature can be filed either by individuals or any person on behalf of the individuals.

V. Additional due diligence for significant social media intermediaries

- They must appoint a Chief Compliance Officer, a Nodal Contact Person and a Resident Grievance Officer, and all these officers should be Indian residents.
- They should publish a monthly compliance report detailing the complaints received.

VI. Establishing the identity of the originator of the message/content

- Such intermediaries offering services chiefly in messaging shall enable identification of the first originator of the information.
- The purpose of this identification is for the prevention, detection, investigation, punishment of an offence related to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or in relation to rape, sexually explicit material or child sexual abuse material punishable with custody for a term of not less than five years.
- Here, the social media intermediaries offering messaging services will have the responsibility to help law enforcement agencies identify and track the first originator of any contentious or problematic information.
- This can only be executed through an order of a competent court or the Competent Authority under Section 69 of the Act and must only be employed as a measure of last resort.

VII. Unlawful information removal

- An intermediary upon receiving actual knowledge in the form of an order by a court or being notified by the appropriate govt. or its agencies through authorized officer should not host or publish any information which is prohibited under any law in relation to the interest of the sovereignty and integrity of India, public order, friendly relations with foreign countries, etc.

New Guidelines for OTT Platforms, News Publishers & Digital Media

I. Over-the-top (OTT) Platforms

- The new rules call OTT platforms 'publishers of online curated content.
- They would have to self-classify the content into five categories based on age.
  - U (Universal) , U/A 7+ , U/A 13+ , U/A 16+, A (Adult)
- OTT platforms would be required to provide parental lock systems for content classified U/A 13+ or higher and have age verification mechanism for content classified as 'Adult'.
- The rating for the content should be prominently displayed before the programme starts so that users can make informed decisions based on suitability. Along with the rating, the content's description should also be provided with a viewer discretion message if applicable.

II. News Publishers

- Publishers of news on digital media should observe Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation Act 1995 to provide a level playing field between the offline (Print, TV) and digital media.

III. Grievance redressal mechanism

A three-level grievance redressal mechanism has been mandated with different levels of self-regulation. They are:

- **Level-I: Self-regulation by the publishers**
  - Publisher should appoint a Grievance Redressal Officer who is a resident of India.
  - This officer should take his/her decision on complaints within 15 days.
- **Level-II: Self-regulation by the self-regulating bodies of the publishers**
  - The self-regulating bodies of the publishers should register themselves with the Ministry of Information & Broadcasting.
  - One publisher can have more than one self-regulating bodies.
  - Such bodies would be headed by a retired judge of the Supreme Court, a High Court, or an eminent independent person and shall not have more than six members.
  - This body should oversee that the publisher adheres to the Code of Ethics.
  - The body will also address grievances that are not resolved within 15 days by the publisher.
- **Level-III: Oversight mechanism**
  - An oversight mechanism will be framed by the Information and Broadcasting Ministry.
  - It shall publish a charter for self-regulating bodies, including Codes of Practices.
  - It shall also establish an Inter-Departmental Committee for hearing grievances.

New IT Rules Concerns

- Some people say that instead of soft-touch monitoring, the government has opted for predatory new rules.
- The mandate that social media intermediaries should help authorities trace the first originator of contentious messages can be problematic, experts opine. Tracking the first originator would entail storing sensitive information or breaking end-to-end encryption protocol, moves that could fail overall security. Here, the users' right to privacy could be potentially violated. The issue gets even more complicated if the message originator is outside India.

Challenges to Indian Law

1. Rapid Technological Advancements:
   - Cyber criminals exploit new technologies faster than laws can be updated.

2. Jurisdictional Issues:
   - Cyber crimes often transcend national borders, making jurisdiction and extradition complex.

3. Anonymous Nature of the Internet:
   - Perpetrators can hide behind anonymity, making it difficult to identify and prosecute them.

4. Complexity of Cyber Attacks:
   - Advanced tactics like phishing, ransomware, and DDoS attacks challenge traditional legal frameworks.

5. Data Protection Challenges:
   - Ensuring privacy and security of sensitive data among growing digital transactions.

6. Capacity Building and Training:
   - Limited expertise and resources in law enforcement agencies to tackle sophisticated cyber crimes.

7. International Cooperation:
   - Collaborative efforts required between nations to combat cross-border cyber threats effective

Real-life Examples of cybercrime in INDIA

- **ATM Skimming:** Criminals install skimming devices on ATMs to capture card information. In 2018, a gang was arrested in Delhi for stealing over ₹25 lakh using skimming devices.

- **Phishing Attacks:** Cybercriminals often send fraudulent emails or messages to trick individuals into revealing sensitive information. In 2017, several Indian banks faced phishing attacks, leading to financial losses for customers.

- **Social Media Hacking:** High-profile social media accounts, including celebrities and politicians, have been hacked. In 2020, the XYZ accounts of several prominent personalities were hacked to promote a cryptocurrency scam.

- **Online Banking Fraud:** Cybercriminals exploit vulnerabilities in online banking systems. In 2016, the Union Bank of India faced a cyberattack where hackers siphoned off $170 million.

- **Ransomware Attacks:** Ransomware infects computer systems and demands a ransom for decryption keys. In 2017, the WannaCry ransomware affected computers worldwide, including those in India, disrupting various services.

- **Cyberbullying:** Cases of cyberbullying and online harassment have been reported. In 2015, a Mumbai resident was arrested for harassing a woman on social media platforms.

- **Data Breaches:** Companies have faced data breaches where customer information is compromised. In 2020, a data breach at JustPay, a payment processor, exposed the data of millions of users in India.

Digital Signatures

Digital signatures are electronic signatures that ensure the authenticity, integrity, and non-repudiation of digital documents or messages.

Components:

- **Private Key:** Unique to the signer, kept secure. Used for creating the digital signature.
- **Public Key:** Available publicly, used for verifying the digital signature.
- **Hash Function:** Generates a fixed-size hash value representing the data, ensuring integrity.
- **Certificate Authority (CA):** Verifies the identity of the signer and issues digital certificates.

Advantages

- Security
- Non-Repudiation
- Efficiency
- Cost-Effectiveness

Applications

- Legal Documents
- Financial Transactions
- Government Documents
- Business Communication
- Software distribution

Challenges

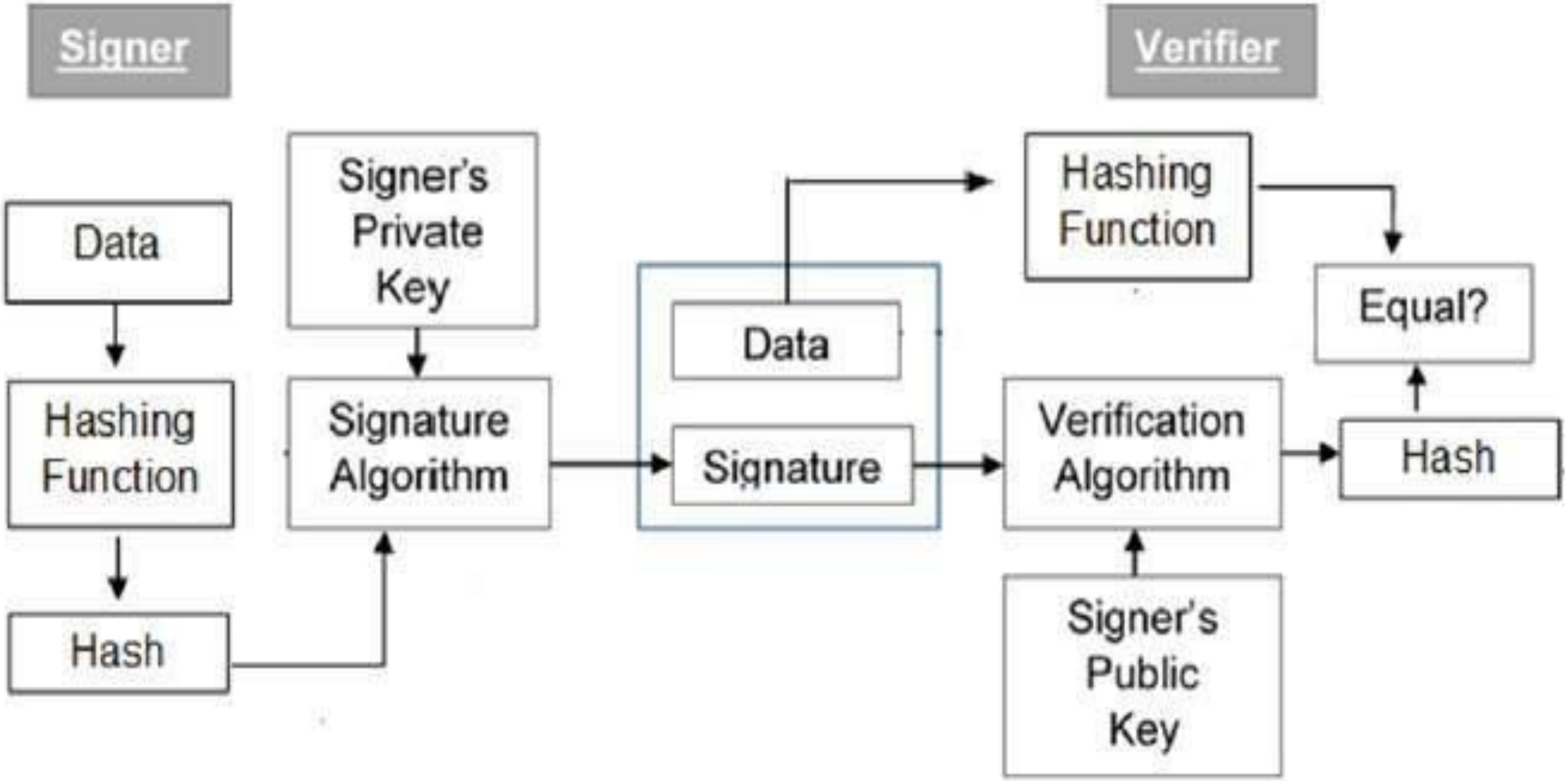
- Key Management
- Regulatory Compliance

DIGITAL SIGNATURE & ENCRYPTION

Under the provisions of IT Act 2000, digital signature may be used by any subscriber for the purpose of authentication of an electronic record. The electronic record is authenticated with the help of “asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. (Section 2(1)(p) of the Information Technology Act, 2000).”

The creation of digital signature requires application of encryption to specific information. The process involves following steps:

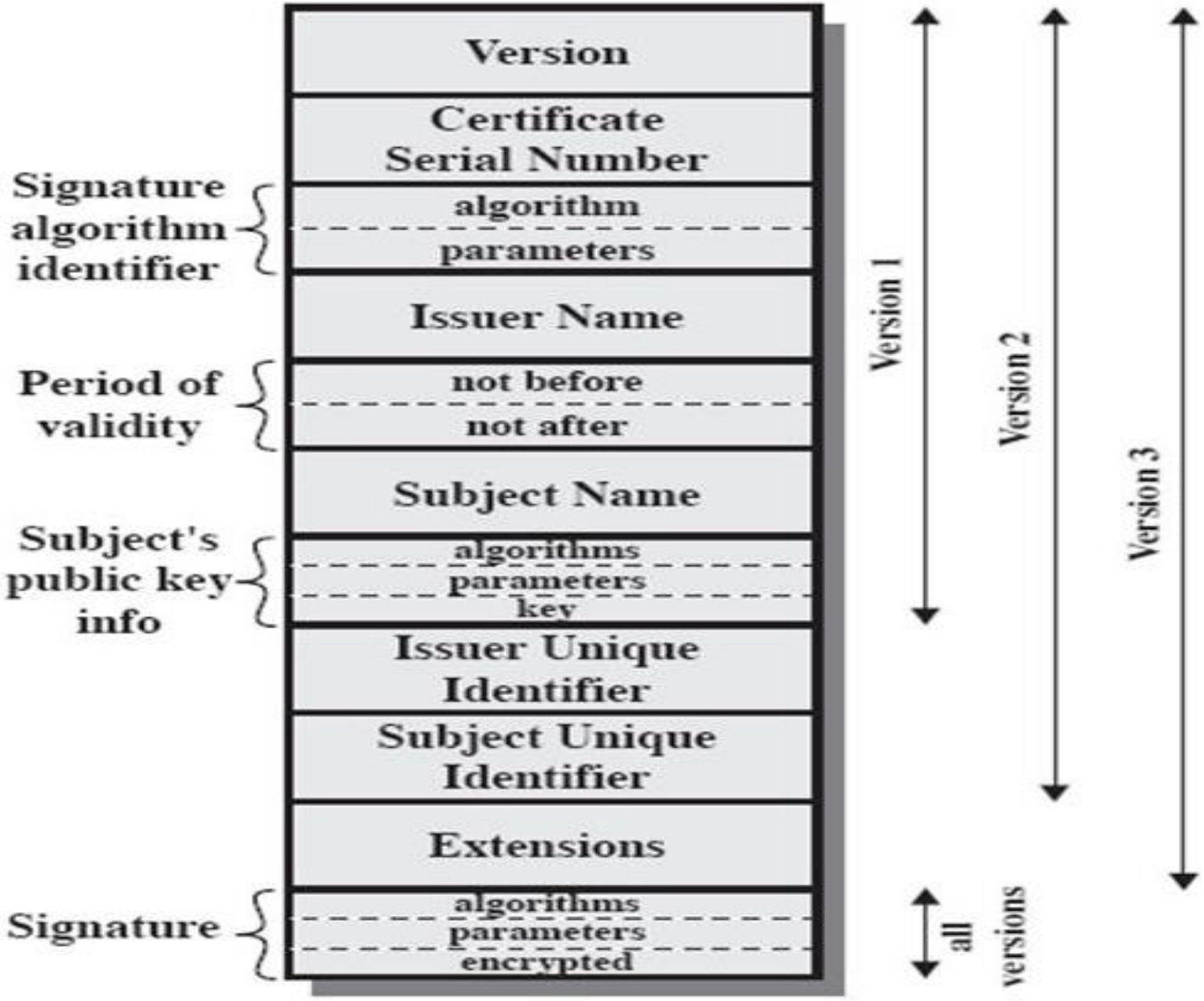
- The message that has to be signed using digital signature is outlined, and then processed with the help of an algorithm called hash function. The processed output thus received is called the hash result which is unique to the message.
- This hash result so produced is encrypted using the private key of the sender. This is the Digital Signature.
- The Digital Signature is then attached to the message which is then transmitted over to the receiver through internet.
- Once the message is received at the receiver’s end, he uses the public key of the sender to decrypt the message. If the sender’s message is successfully decrypted using his public key and the hash result is computed and compared with the output of the digital signature, then the receiver is assured of the authenticity and integrity of the message.


Signer
Verifier
Data
Hashing Function
Hash
Signer's Private Key
Signature Algorithm
Data
Signature
Hashing Function
Verification Algorithm
Signer's Public Key
Equal?
Hash

Digital Certificate

- Certificates are the framework for identification information, and bind identities with public keys.
- They provide a foundation for
  - identification,
  - authentication and
  - non-repudiation.
- Trusted organization (i.e. **Certificate Authority** (CA)) that issues certificates and maintains status information about certificates.
- The most popular CA's are VeriSign and Entrust.
- CA issues new certificates, maintain old ones, and revoke the certificate that has become invalid for some sort of reasons, etc.
- The CA can delegate some of its tasks to this third-party called as a **Registration Authority (RA).**
- A Standard called **X.509** define a structure of a digital certificate.

Structure of X.509 digital certificate.



BASIS FOR COMPARISON	DIGITAL SIGNATURE	DIGITAL CERTIFICATE
Basic	It verifies the authenticity and source of a particular document.	It creates an identity of a website and also increases its trustworthiness.
Process	The document is encrypted at the sending end and decrypted at the receiving end using asymmetric keys.	A certificate is issued by a trusted agency known as CA which follow particular steps to do so that are - key generation, registration, verification and creation.
Security	It provides authentication, non-repudiation and integrity.	It provides identification, authentication, non-repudiation and security.

Digital Signatures and the Indian IT Act

Digital Signatures in Indian IT Act (2000):

- The Information Technology Act, 2000, provides legal recognition to digital signatures in India.
- Under Section 3, digital signatures are considered authentic and secure, promoting e-governance and digital transactions.

Digital Signature Certificates (DSC):

- DSCs are issued by Certifying Authorities (CAs) accredited by the Controller of Certifying Authorities (CCA).
- Section 35 of the IT Act recognizes DSCs as proof of identity and electronic signatures, ensuring their legal validity.

Role in Electronic Transactions:

- DSCs facilitate secure online transactions, electronic contracts, and digital communication, ensuring the integrity and authenticity of digital documents.

Important Chapters under IT Act 2000
Chapter V
Chapter VIII
Chapter IX
Chapter XII

https://www.indiacode.nic.in/handle/123456789/1999

Tutorial 3 – Sample example

1. A unauthorized accesses the computer of X and obtains her email password and afterwards fraudulently sends a message to B, X's uncle in India through x's email and under x's email signature for transferring a sum of Rs. 2 lakhs in account number mentioned in the email. Has A committed any crime under the Information Technology Law? Elucidate referring to judicial decisions.

Tutorial 3 – Sample example

2. X had a bank account in ABC Bank. The account was linked with her mobile number, issued by A2Z Company. An amount of Rs. 19 lakhs was transferred from the bank by an unknown person in three days' time. During this period X's mobile phone stopped functioning. This was due to the issue of duplicate SIM cards of X's number by A2Z company on the forged passport to an unknown person. X filed a complaint to the adjudicating officer against the ABC bank and A2Z mobile service for being negligent in handling sensitive personal data and therefore liable to pay compensation. The bank contended that it had been sending the SMS for every transaction to the customer mobile number. Decide applying the relevant law and judicial.