SYLLABUS

B.COM/BBA – III YEAR

Cyber Crimes & Law

UNIT – I	Introduction to Cyber World : Introduction to Cyber World, Cyber Security V/s Cyber Law, Types of Cyber Threats, Difference between Cyber Crimes and Conventional Crimes, Areas Comes under Cyber Law, Jurisdiction area of cyber law. Type of Cyber Crimes like - Piracy, Phishing, Hacking of information, Data Breach, CSS Attacks, Cyber Harassments, SQL Injection, Identity Hack, Cyber terrorism, DOS, Insider Attacks, Dark Web using TOR, Credit Card/Debit Card/UPI Hackings, Cyber Stalking, Cyber bullying, Eaves dropping attack, online libel/slander, Social Engineering, Cryptojacking, Virtual Currency Fraud, Vishing (Voice phising), IOT Attacks, Phone Hacking, Child Pornography, Human Trafficking, Malicious Advertisement Campaign(Malvertising), online gambling, Hacking into voting systems, Breach of IPR, patent & Copyright etc
UNIT – II	Definitions under IT Act, 2000 : Concept of Internet, Web Centric Business, E Business , Electronic Governance, Cyber jurisdiction. Contemporary Business Issues in Cyber Space, Security risks: Instant messaging platform, social networking sites, mobile applications and Internet of Things (IOT). Domain name dispute and their resolution, E- forms; EMoney, regulations of PPI (Pre-Payment Instruments) by RBI, Electronic Money Transfer, Privacy of Data and Secure Ways of Operation in Cyber Space.
UNIT – III	Electronic Records : Authentication of Electronic Records; Legal Recognition of Electronic Records; Legal Recognition of Digital Signatures; Applications and usage of electronic records and Digital Signatures in Government and its Agencies; Retention of Electronic Records, Intermediaries and their liabilities; Attribution, Acknowledgement and Dispatch of Electronic Records, Secure Electronic Records and Digital Signatures
UNIT - IV	Regulatory Framework : Regulation of Certifying Authorities; Appointment and Functions of Controller; License to issue Digital Signatures Certificate; Renewal of License; Controller's Powers; Procedure to be Followed by Certifying Authority; Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers; Penalties and Adjudication; Appellate Tribunal; Offences; Overview of GDPR and Indian data protection regime

Unit I

Cyber World

The "cyber world" refers to the virtual space created by computers, the internet, and digital technologies. It includes everything related to online communication, websites, social media, gaming, and other digital activities. It is a space where people connect, share information, and interact using technology.

The **cyber world** refers to the virtual space created by computers, the internet, and digital technology. It includes all online platforms, websites, social media, and communication systems where people connect, share information, and perform activities. In the cyber world, users can work, shop, learn, and interact from anywhere in the real world.

This virtual space is powered by networks, servers, and software, making it accessible through devices like computers, smartphones, and tablets. The cyber world has transformed modern life, making tasks faster and communication easier. However, it also comes with challenges, such as cybersecurity threats, data privacy concerns, and misinformation.

Despite these challenges, the cyber world plays a vital role in education, business, and entertainment. It continues to grow, connecting people globally and shaping the future of technology. Proper use and awareness are important to ensure its benefits outweigh its risks.

Difference between Cyber Security and Cyber Law

Cyber security focuses on protecting computers, networks, data, and systems from cyber threats like hacking, viruses, and unauthorized access. It involves using technologies, processes, and practices to secure digital infrastructure. Cyber security professionals work to prevent attacks, detect vulnerabilities, and ensure the safe functioning of systems.

Cyber law, on the other hand, deals with the legal aspects of cyberspace. It involves regulations and laws governing online activities, digital rights, and the use of the internet. Cyber law addresses issues like cybercrimes, intellectual property rights, online privacy, and e-commerce disputes. Lawyers specializing in cyber law ensure compliance with legal standards and provide remedies for cyber-related offenses.

In summary, cyber security is about protecting the digital world from threats, while cyber law is about creating legal frameworks to regulate and resolve issues arising in cyberspace. Both are crucial for a safe and lawful online environment.

Cyber Treats

Cyber threats refer to any potential dangers or attacks that target digital systems, networks, or devices. These threats come from malicious actors who attempt to gain unauthorized access, steal data, disrupt services, or cause harm to individuals or organizations. Some common types of cyber threats include malware, which refers to harmful software designed to damage or disrupt systems; phishing, where attackers deceive individuals into revealing sensitive information like passwords or credit card numbers; and ransomware, which locks a victim's files and demands payment to restore access. Cyber threats can also involve denial-of-service attacks, where websites or networks are overwhelmed with traffic to make them unusable. The rise of the internet and connected devices has made cyber threats more common and dangerous, affecting businesses, governments, and individuals. Protecting against these threats involves using strong security measures, keeping software up to date, and being aware of potential risks when online.

Types of Cyber Treats

Cyber threats are malicious activities designed to damage or steal data from individuals or organizations. They can be categorized into several types:

1. **Malware**: This includes viruses, worms, and Trojans, which infect and damage devices or networks. They can steal information or cause system failures.
2. **Phishing**: Fraudulent attempts to acquire sensitive data like passwords or credit card numbers by pretending to be a trustworthy entity.
3. **Ransomware**: A type of malware that encrypts a user’s data and demands a ransom for the decryption key.
4. **Denial-of-Service (DoS) Attacks**: Overloading a system with traffic to make it unavailable to users.
5. **Man-in-the-Middle (MitM) Attacks**: Intercepting and altering communications between two parties to steal or manipulate data.
6. **SQL Injection**: Injecting malicious code into a website's database to steal or corrupt data.

These threats can have severe consequences, making cyber security essential for protection.

Difference between cyber crime and Conventional Crimes

Cybercrimes and conventional crimes differ in the nature of their occurrence, methods, and impact.

1. **Cybercrimes**: These involve illegal activities committed through the internet or digital platforms. Examples include hacking, phishing, identity theft, cyberbullying, and data breaches. Cybercriminals use technology to access, manipulate, or steal information, often targeting individuals or organizations remotely. The crimes are often difficult to trace and can have a global reach.
2. **Conventional Crimes**: These are traditional crimes that occur in the physical world, such as theft, assault, robbery, and murder. They typically involve direct interaction between the criminal and the victim. Conventional crimes are easier to investigate with physical evidence and witnesses but can be geographically limited.

While both types of crimes cause harm, cybercrimes are growing due to increasing reliance on technology, while conventional crimes are more rooted in physical actions and human interaction. Both require effective law enforcement but differ in their tools and methods.

Here are the key differences between cyber crimes and conventional crimes:

1. **Nature**:
   - **Cyber Crimes**: Involve the use of technology, particularly computers and the internet, to commit illegal activities (e.g., hacking, phishing, cyberstalking).
   - **Conventional Crimes**: Traditional crimes that occur in the physical world (e.g., theft, assault, murder).
2. **Medium**:
   - **Cyber Crimes**: Committed through digital devices, networks, and online platforms.
   - **Conventional Crimes**: Involve physical presence and direct interaction between the criminal and victim.
3. **Geographical Boundaries**:
   - **Cyber Crimes**: Can occur across borders, affecting individuals globally.
   - **Conventional Crimes**: Typically occur in a specific location or jurisdiction.
4. **Detection and Investigation**:
   - **Cyber Crimes**: More complex, requiring technical expertise and digital tools.
   - **Conventional Crimes**: Often easier to detect with physical evidence and eyewitness testimony.
5. **Anonymity**:
   - **Cyber Crimes**: Perpetrators can remain anonymous online.
   - **Conventional Crimes**: Typically involve identifiable individuals.

Areas comes under cyber law

Cyber law covers various legal aspects related to the internet, digital transactions, and online activities. Some key areas under cyber law include:

1. **Data Protection and Privacy**: Ensures the security and privacy of personal and sensitive data stored online, preventing unauthorized access or misuse.
2. **Intellectual Property Rights (IPR)**: Protects copyrights, trademarks, and patents in the digital space, addressing issues like software piracy and online plagiarism.
3. **Cybercrime**: Covers illegal activities like hacking, identity theft, fraud, cyberbullying, and cyberstalking. It also includes offenses related to online defamation and obscenity.
4. **E-Commerce and Online Contracts**: Regulates online transactions, contracts, and agreements made through websites or digital platforms, ensuring they are legally binding.
5. **Digital Signatures**: Legislation around the use of electronic signatures, which serve as legal substitutes for handwritten ones in online transactions.
6. **Regulation of Online Content**: Addresses laws concerning online speech, fake news, and content censorship.

Cyber law is essential for regulating the growing digital world and ensuring legal protection for all online activities.

Types of Cyber Crimes

1. Hacking: Hacking is unauthorized access to computer systems, networks, or devices. Hackers exploit security vulnerabilities to gain control over systems. They can steal, alter, or destroy data, leading to financial losses or identity theft. Hackers use various methods, such as brute force attacks, exploiting software vulnerabilities, or phishing to bypass security measures. While some hackers act with malicious intent, others, known as "ethical hackers," find and report security flaws to improve cybersecurity. However, unauthorized hacking is illegal and punishable by law in most countries.

2. Phishing: Phishing involves tricking individuals into revealing sensitive information, such as passwords, credit card numbers, or social security details. Cybercriminals often use fake emails, websites, or messages that appear legitimate. These deceptive messages may look like they're from trusted organizations, such as banks or online stores, urging victims to click on malicious links. Once the victim submits their information, it can be used for identity theft or financial fraud. Phishing attacks are widespread and can be difficult to detect without careful scrutiny of suspicious communications.

3. Cyber bullying: Cyber bullying refers to the use of digital platforms, like social media, texting, or online forums, to harass, intimidate, or threaten someone. This form of bullying can be especially harmful due to its 24/7 nature, causing emotional distress to victims. Perpetrators may spread rumors, share embarrassing photos, or send hurtful messages to damage a person’s reputation or mental health. Unlike traditional bullying, cyber bullying allows anonymity, making it harder to identify the perpetrator. Legal frameworks in many countries now address cyber bullying, requiring social media platforms to take action.

4. Identity Theft: Identity theft is the act of obtaining someone’s personal information—such as social security numbers, credit card details, or banking information—and using it to commit fraud.

Cybercriminals can steal identity through data breaches, phishing attacks, or by accessing public records. Once they have access to sensitive data, they can open fraudulent accounts, make purchases, or even file false tax returns. The victim is often left to deal with the financial and legal consequences, which can take years to resolve. Protecting personal information and using encryption are essential in preventing identity theft.

5. Cyber stalking : Cyber stalking involves the repeated use of the internet or other electronic means to stalk or harass an individual. The stalker may monitor a victim's online activity, send threatening messages, or engage in other intrusive behaviors. Unlike traditional stalking, cyber stalking can reach a global audience and is harder to escape because it can happen continuously. Victims often experience fear, anxiety, and distress due to the stalker's persistence and the potential for their personal information to be shared publicly. Many countries have specific laws against cyber stalking to protect victims.

6. Online Fraud: Online fraud refers to any fraudulent activity conducted over the internet. This can involve selling fake products, auction scams, or tricking individuals into making payments for services that do not exist. One common form is e-commerce fraud, where cybercriminals set up fake online stores to steal payment information. Other types include credit card fraud and investment scams, where victims are persuaded to share financial details or invest in fraudulent schemes. The rise of e-commerce has made it crucial for both consumers and businesses to adopt secure online transaction methods.

Insider attacks

Insider attacks in cyber security refer to malicious or negligent actions by individuals within an organization who have authorized access to its systems, data, or networks. These individuals can be employees, contractors, or business partners. Insider attacks can be deliberate (malicious) or accidental (unintentional) but often result in significant harm.

Types of Insider Attacks:

1. **Malicious Insiders**: Intentionally misuse access to steal data, sabotage systems, or leak information for personal gain or revenge.
2. **Negligent Insiders**: Carelessly cause breaches by ignoring security policies, falling for phishing attacks, or miss configuring systems.
3. **Compromised Insiders**: Legitimate accounts hijacked by external attackers.

In cyber security, **DoS** (Denial of Service) refers to a malicious attack that disrupts the normal functioning of a network, server, or website by overwhelming it with excessive traffic or resource requests. The goal is to make the targeted system unavailable to legitimate users.

Types of DoS Attacks:

1. **Volume-Based Attacks**: Overload a system with massive amounts of data.
2. **Protocol Attacks**: Exploit weaknesses in network protocols, such as TCP/IP.
3. **Application Layer Attacks**: Target specific applications or services.

Common Examples:

- **Ping Flood**: Sending a large number of ICMP requests.
- **SYN Flood**: Exploiting the TCP handshake process.

Preventing DoS attacks is vital for maintaining uninterrupted online services.

Dark web using TOR

The **dark web** refers to a hidden part of the internet that requires special tools like **TOR (The Onion Router)** to access. Unlike the surface web, it is not indexed by standard search engines. TOR enables anonymity by routing internet traffic through multiple layers of encryption across a network of volunteer-operated servers.

While the dark web hosts legitimate uses, such as anonymous communication for activists or journalists in oppressive regimes, it is also associated with illegal activities like black markets, hacking forums, and cybercrime. Cybersecurity experts use TOR to research threats, monitor illegal activities, and improve privacy measures online.

Human trafficking

Human trafficking is the illegal act of recruiting, transporting, harboring, or exploiting individuals through force, fraud, or coercion for purposes like forced labor, sexual exploitation, or organ trade. Victims are often vulnerable individuals, including women, children, and migrants, targeted due to poverty, conflict, or lack of awareness.

Traffickers manipulate or threaten their victims, depriving them of basic rights and freedoms. Human trafficking is a global issue, affecting millions annually, and is considered a severe violation of human rights. Governments, NGOs, and international organizations work together to combat trafficking through awareness, stronger laws, and victim rehabilitation programs.

A **malicious advertisement campaign**, or malvertising, involves embedding harmful code or deceptive content in online ads. These campaigns exploit legitimate ad networks to deliver malware, phishing links, or fraudulent schemes to users without their knowledge.

Key Features:

1. **Hidden Malware**: Ads contain malicious scripts that infect devices when clicked or sometimes without interaction (drive-by downloads).
2. **Phishing**: Ads redirect users to fake websites to steal sensitive information.
3. **Fraudulent Content**: Promotes scams, fake products, or services.

Malvertising poses significant risks to users and platforms, making robust ad network vetting, secure browsing, and ad-blockers essential for protection.

Breach of Intellectual Property Rights (IPR)

A **breach of Intellectual Property Rights (IPR)** occurs when someone uses, copies, or distributes protected intellectual property without the owner's permission, violating their legal rights. This includes copyright, trademark, patent, and trade secret infringements.

Examples of IPR breaches include unauthorized reproduction of books, music, or films (copyright), using a logo similar to a registered trademark, replicating patented inventions without approval, and disclosing confidential trade secrets.

Such breaches harm creators, disrupt fair competition, and may lead to financial losses or reputational damage. Legal actions, fines, or penalties can be enforced to protect IPR and ensure fair use of intellectual property.

Patent

A **Patent** is a legal right granted to an inventor or assignee, giving them exclusive rights to make, use, sell, or distribute their invention for a specific period, usually 20 years. Patents protect innovations that are new, useful, and non-obvious, encouraging technological advancements and investment in research and development.

To obtain a patent, the invention must be disclosed in detail, enabling others to replicate it once the patent expires. Patents are territorial, meaning they apply only in the granting country or region. Examples include inventions in machinery, pharmaceuticals, and technology. They foster innovation by rewarding creativity and ensuring fair competition.

Copyright

Copyright is a legal right that grants the creator of original works—such as books, music, films, art, and software—the exclusive authority to reproduce, distribute, display, or perform their work. It protects intellectual property and ensures creators can control how their works are used or monetized. Copyright does not cover ideas or facts but protects the expression of those ideas.

It typically lasts for the creator's lifetime plus additional years (e.g., 70 years in many countries). Copyright laws aim to balance creators' rights with public access, promoting creativity while preventing unauthorized use or duplication of copyrighted material.

Each type of cybercrime poses a unique set of challenges, highlighting the need for robust cyber security measures and awareness.

Unit – II

About IT Act 2000

The **Information Technology (IT) Act, 2000**, came into existence on **17th October 2000**. It was enacted to address the growing challenges of cyberspace, regulate electronic commerce, and combat cybercrimes in India.

The **Information Technology Act, 2000**, is a significant legislation in India that provides a legal framework for electronic commerce, cybercrime, and digital transactions. It was enacted to promote and regulate activities in cyberspace while ensuring secure online interactions.

The Act recognizes electronic records and digital signatures as legally valid, facilitating smoother e-governance and online business. It defines offenses like hacking, identity theft, phishing, and spreading viruses, prescribing penalties for such activities.

One of its key features is the establishment of the **Certifying Authority** to issue digital certificates, ensuring secure digital communication. The Act also empowers the government to monitor, intercept, and decrypt data for national security or legal purposes.

Amended in 2008, it introduced provisions to address newer challenges like data protection, cyber terrorism, and offensive online content. The IT Act is pivotal in combating cybercrime and enabling India's transition to a digital economy.

Reasons for Its Introduction:

1. **Legal Recognition of Electronic Transactions**: With the rise of the internet, there was a need to give legal recognition to digital records and signatures for promoting e-commerce.
2. **Prevention of Cybercrimes**: The Act was introduced to define and penalize cybercrimes such as hacking, identity theft, and data breaches.
3. **Data Protection and Privacy**: It aimed to ensure the security of sensitive personal and corporate data exchanged online.
4. **Facilitating E-Governance**: The Act enabled electronic filing of documents and transactions with government bodies.

It was a landmark step to strengthen India's legal framework in the digital era.

Concept of Internet

The Internet is a vast global network that connects millions of private, public, academic, business, and government devices worldwide. It operates using standardized protocols, primarily the Internet Protocol (IP) and Transmission Control Protocol (TCP), which ensure data is transmitted accurately between devices. The Internet enables various services such as the World Wide Web, email, streaming, and online gaming, allowing users to access and share information instantly across the globe.

At its core, the Internet is a collection of interconnected networks facilitated by routers and servers that direct and store data. Users access the Internet through Internet Service Providers (ISPs) using devices like computers, smartphones, and tablets. The decentralized nature of the Internet promotes resilience and scalability, supporting continuous growth and innovation.

Beyond communication, the Internet has revolutionized commerce, education, healthcare, and entertainment, making it an essential infrastructure in modern society. Its ability to connect people and information seamlessly has transformed how we live, work, and interact on a daily basis.

Web Centric Business

A web-centric business operates primarily through the internet, leveraging online platforms to deliver products or services, engage with customers, and manage operations. This type of business is designed around web technologies and digital tools, making it highly adaptable to global markets.

Key features of web-centric businesses include online presence, such as websites or e-commerce platforms, for direct sales and customer interaction. Social media, email marketing, and search engine optimization (SEO) are used to attract and retain customers. Cloud-based tools support operations like inventory management, communication, and data storage.

Examples of web-centric businesses include e-commerce stores (e.g., Amazon), online service providers (e.g., streaming platforms like Netflix), and SaaS companies (e.g., Dropbox).

The benefits include cost-effectiveness, scalability, and 24/7 accessibility for customers worldwide. However, challenges like cybersecurity, competition, and technology dependency require strategic planning and innovation to succeed.

e business

E-business, or electronic business, refers to conducting business activities using digital platforms and the internet. It encompasses a wide range of activities, including buying and selling products or services, managing supply chains, and interacting with customers and partners online.

E-business includes **e-commerce**, which focuses on online transactions, but extends beyond that to cover operations like online marketing, customer relationship management (CRM), and enterprise resource planning (ERP). Popular examples include online retail platforms like Amazon and Flipkart, where customers can browse, purchase, and get products delivered.

Advantages of e-business include wider reach, 24/7 availability, reduced operational costs, and streamlined processes. Businesses can leverage social media and digital marketing to attract customers globally. However, challenges like cybersecurity threats, competition, and ensuring customer trust must be managed effectively.

E-business has transformed how companies operate, offering convenience and efficiency in a digital-first world.

Electronic governance, or e-governance, refers to the use of digital technology to deliver government services, improve administration, and engage citizens. It enables transparency, efficiency, and accessibility in government processes by using online platforms, mobile apps, and other digital tools.

Electronic Governance

E-governance operates in four main areas:

1. **Government-to-Citizen (G2C)**: Providing services like tax payments, bill payments, and online portals for public grievances.
2. **Government-to-Business (G2B)**: Facilitating business interactions such as licensing, tenders, and compliance processes.
3. **Government-to-Government (G2G)**: Streamlining communication and data sharing among government departments for better coordination.
4. **Government-to-Employee (G2E)**: Enhancing internal operations like payroll management and employee benefits.

Key benefits of e-governance include reduced paperwork, quicker service delivery, and greater accountability. Examples include India's Digital India initiative and Aadhaar-linked services. E-governance empowers citizens and promotes inclusive development by bridging the digital divide.

Cyber Jurisdiction

Cyber jurisdiction refers to the legal authority of a government or court to regulate, enforce laws, and resolve disputes related to activities in cyberspace. Unlike physical jurisdictions, cyber jurisdiction involves the virtual realm, where geographical boundaries are unclear.

It covers issues such as cybercrimes, data breaches, online contracts, intellectual property disputes, and more. Jurisdiction is determined by factors like the location of the parties involved, the location of servers, or the impact of online activities.

Challenges arise due to the global nature of the internet. For instance, a cybercrime may be committed in one country, target victims in another, and use servers in a third. This creates jurisdictional conflicts and complicates enforcement.

International agreements, like the Budapest Convention on Cybercrime, aim to harmonize laws and facilitate cross-border cooperation. Effective cyber jurisdiction ensures accountability and legal remedies while addressing the complexities of a borderless digital world.

Instant Messaging Platform

An **instant messaging platform** is a digital application or service that allows users to exchange real-time messages over the internet. These platforms enable communication through text, voice, video, and multimedia sharing. They are widely used for personal, professional, and group interactions due to their speed and convenience.

Key Features:

1. **Text Messaging**: Real-time text communication.
2. **Voice and Video Calls**: Instant voice or video connections.
3. **File Sharing**: Sending images, documents, and other media.
4. **Group Chats**: Conversations with multiple participants.
5. **End-to-End Encryption**: Security to protect user privacy.

Examples:

1. **WhatsApp**: A popular app with end-to-end encryption and multimedia sharing.
2. **Telegram**: Known for its cloud-based system and secure chats.
3. **Facebook Messenger**: Integrated with Facebook for seamless communication.
4. **Signal**: Focused on high-level security and privacy.
5. **Slack**: Used mainly for workplace collaboration.
6. **Skype**: Offers messaging along with voice and video calls.

Social Networking Sites

Social networking sites are online platforms that allow users to create profiles, connect with others, and share content such as messages, photos, videos, and updates. These sites are designed to foster social interaction and build virtual communities based on shared interests, relationships, or professional connections.

Key Features:

1. **User Profiles**: Personal or business accounts showcasing information and interests.
2. **Friends/Followers**: Connections with other users to share and view content.
3. **Content Sharing**: Ability to post updates, photos, videos, and links.
4. **Messaging**: Direct communication through private or group chats.
5. **Communities and Groups**: Forums for discussions on shared interests or causes.

Examples:

1. **Facebook**: For personal connections, groups, and multimedia sharing.
2. **Twitter (X)**: A microblogging site for short updates and news.
3. **Instagram**: Focused on photo and video sharing.
4. **LinkedIn**: Geared towards professional networking.
5. **Snapchat**: Offers disappearing messages and creative content.
6. **Pinterest**: A platform for discovering and saving creative ideas.

Mobile Applications

Mobile applications (or mobile apps) are software programs designed to run on smartphones, tablets, or other portable devices. These apps are created for specific functions, such as communication, entertainment, education, or productivity, and are typically downloaded from app stores like the **Google Play Store** or **Apple App Store**. Mobile apps can be native (built for specific operating systems), web-based, or hybrid.

Key Features:

1. **User-Friendly Interfaces**: Easy to navigate and interact with.
2. **Customization**: Apps tailored to user preferences.
3. **Offline Functionality**: Some apps work even without an internet connection.
4. **Push Notifications**: Real-time alerts and updates.

Popular Mobile Apps:

1. **WhatsApp**: For instant messaging and video calls.
2. **Facebook**: Social networking and content sharing.
3. **Instagram**: For photo and video sharing.
4. **YouTube**: Streaming and sharing videos.
5. **Google Maps**: Navigation and location services.
6. **Spotify**: Music streaming and podcasts.
7. **TikTok**: Short video creation and sharing.
8. **Zoom**: Virtual meetings and collaboration.

Internet of Things (IoT)

The Internet of Things (IoT) refers to the network of physical devices, vehicles, appliances, and other objects embedded with sensors, software, and connectivity, enabling them to collect and exchange data over the internet. These devices can communicate with each other and with centralized systems to automate processes, enhance functionality, and improve decision-making.

Their Specialty:

1. **Connectivity**: Devices are connected via the internet or other communication networks.
2. **Automation**: IoT enables automation of tasks based on collected data, like adjusting thermostat settings or controlling lighting.
3. **Real-Time Data**: Continuous data collection and monitoring for improved decision-making.
4. **Remote Control**: Users can control IoT devices remotely, such as smart home appliances or security systems.

Examples:

1. **Smart Homes**: Devices like smart thermostats, lights, and security cameras.
2. **Wearables**: Fitness trackers and smartwatches that monitor health data.
3. **Smart Cities**: Infrastructure like traffic lights, waste management, and street lighting controlled via IoT.
4. **Connected Cars**: Vehicles equipped with IoT to provide features like navigation, emergency alerts, and remote diagnostics.
5. **Industrial IoT**: Sensors and devices used in manufacturing to monitor equipment, improve efficiency, and reduce downtime.

E-money

E-money (electronic money) refers to digital currency or funds stored and transacted electronically. It allows individuals and businesses to make financial transactions without the need for physical cash. E-money is typically stored in a digital wallet or account and can be used for online purchases, transferring funds, or paying for services.

Advantages:

1. **Digital Transactions**: Allows payments and transfers through the internet or mobile devices.
2. **Stored Value**: Money is stored in digital wallets or accounts.
3. **Security**: Transactions are often secured with encryption or other security measures.
4. **Fast and Convenient**: Instant payments and easy access to funds.

Types of E-money:

1. **E-Wallets**: Apps like PayPal, Apple Pay, and Google Pay store and manage funds digitally.
2. **Cryptocurrencies**: Digital currencies like Bitcoin and Ethereum, which use blockchain technology.
3. **Prepaid Cards**: Cards like Visa or MasterCard prepaid cards that can be loaded with e-money.
4. **Mobile Money**: Services like Paytm and M-Pesa that allow users to send or receive money via mobile phones.

E-money offers a convenient, fast, and secure way of managing financial transactions in the digital age.

Prepaid payment instruments (PPIs)

Prepaid payment instruments (PPIs) are financial tools that allow users to make payments or store value in advance. These instruments are typically loaded with a specific amount of money and can be used for various transactions, such as buying goods, services, or transferring money. They are not linked to a bank account, and users can only spend the balance available in the instrument.

Advantages:

1. **Pre-loaded Value**: The user loads a fixed amount of money onto the instrument.
2. **Restricted Spending**: Payments are limited to the pre-loaded balance.
3. **No Credit Link**: Unlike credit cards, they do not offer credit facilities.
4. **Convenient and Secure**: Ideal for budgeting and making secure online or offline purchases.
5. **Reloadable**: Some PPIs allow users to add funds again once the balance is used up.

Examples of Prepaid Payment Instruments:

1. **Prepaid Debit Cards**: Cards that can be loaded with funds and used like debit cards (e.g., Visa, MasterCard prepaid cards).

2. **Mobile Wallets**: Apps that store money for online payments and transfers (e.g., Paytm, PhonePe, Google Pay).
3. **Gift Cards**: Cards for specific stores or services, pre-loaded with an amount (e.g., Amazon gift card, Starbucks card).
4. **Travel Cards**: Prepaid cards for travel-related expenses (e.g., rail pass cards, travel money cards).

Electronic money transfer

Electronic money transfer is the process of transferring funds electronically between accounts using digital systems. It eliminates the need for physical cash or checks, providing a fast, secure, and convenient way to send and receive money. Common methods include online banking, mobile payment apps, and wire transfers.

Key technologies enabling this include NEFT (National Electronic Funds Transfer), RTGS (Real-Time Gross Settlement), and IMPS (Immediate Payment Service). Mobile wallets like Paytm, Google Pay, and Apple Pay are also popular for quick transfers.

Electronic money transfer is widely used for personal transactions, bill payments, and business operations, ensuring efficiency and traceability.

Privacy of data

Privacy of data refers to the protection of personal or sensitive information from unauthorized access, use, or disclosure. It ensures that individuals and organizations have control over how their data is collected, shared, and stored. Data privacy involves implementing policies, technologies, and practices to safeguard information, such as encryption, secure passwords, and access controls.

With increasing digital activities, protecting data privacy has become crucial to prevent identity theft, fraud, and breaches. Laws like GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) regulate how companies handle data. Respecting privacy builds trust and ensures ethical handling of information.

Secure Ways of Operation in Cyber Space

Operating securely in cyberspace involves adopting practices to protect personal information and digital assets. Key measures include:

1. **Strong Passwords**: Use unique, complex passwords and enable two-factor authentication.
2. **Updated Software**: Regularly update devices and apps to fix security vulnerabilities.
3. **Secure Networks**: Avoid public Wi-Fi or use VPNs for encrypted connections.
4. **Antivirus Software**: Install and update antivirus programs to detect threats.
5. **Be Cautious with Links**: Avoid clicking on unknown links or downloading files from untrusted sources.
6. **Data Backup**: Regularly back up important data.
7. **Privacy Settings**: Limit personal information shared online and adjust privacy settings on social media.

Unit III

Electronic records

Electronic records are digital versions of information or documents that are created, stored, and accessed on electronic devices like computers, smartphones, or servers. These records can include emails, text files, spreadsheets, images, or databases.

Instead of being written or printed on paper, electronic records exist in a digital format, making them easy to store, search, and share. They are commonly used in offices, schools, hospitals, and other organizations to keep important data organized and safe.

For example, a doctor's notes about a patient stored on a computer or an invoice sent via email are electronic records.

Authentication of electronic records

Authentication of electronic records involves verifying that an electronic document is genuine, unaltered, and created or sent by the claimed source. It ensures the integrity, reliability, and credibility of digital information for legal, financial, or organizational purposes.

Key Methods of Authentication:

1. **Digital Signatures**: Cryptographic tools that confirm the sender's identity and ensure the document hasn't been tampered with.
2. **Biometric Authentication**: Using fingerprints, facial recognition, or iris scans to verify access to records.
3. **Two-Factor Authentication (2FA)**: A secondary layer of security using a password and a one-time code.
4. **Encryption**: Securing data with algorithms to ensure only authorized parties can access it.
5. **Audit Trails**: Logs that record access and modifications to electronic records.

Authentication safeguards electronic records, making them admissible as evidence in courts or reliable for official purposes.

Legal Recognition of Electronic Records

The **legal recognition of electronic records** refers to the acceptance of digital documents as valid and enforceable evidence under the law. This concept ensures that electronic records, like emails, digital contracts, and scanned copies, are treated similarly to traditional paper documents in legal and business contexts.

Key Aspects:

1. **Validity**: Laws like the **Information Technology Act, 2000 (India)** and **Electronic Signatures in Global and National Commerce Act (E-SIGN, USA)** grant electronic records the same legal status as physical records.
2. **Electronic Signatures**: Digital signatures validate the authenticity of electronic records.
3. **Conditions**: For recognition, records must be retrievable, tamper-proof, and meet prescribed standards.
4. **Applications**: Used in contracts, invoices, court evidence, and official communication.

Legal recognition of electronic records simplifies processes, reduces paperwork, and supports digital transformation while ensuring accountability and authenticity.

Legal Recognition of Digital Signature

A **digital signature** is a secure electronic method of verifying the authenticity and integrity of digital documents or messages. It serves as a virtual fingerprint, ensuring that the document was signed by the intended party and has not been tampered with. Legal recognition of digital signatures varies globally but is increasingly standardized.

Key Points of Legal Recognition:

1. **Authenticity**: Confirms the signer's identity.
2. **Integrity**: Ensures the document has not been altered after signing.
3. **Non-repudiation**: The signer cannot deny their signature.

Digital signatures are legally binding and widely used for contracts, government services, and secure transactions.

Intermediaries and their Liabilities

Intermediaries are entities that facilitate the exchange of information between users on digital platforms. Examples include social media platforms, e-commerce websites, search engines, and internet service providers (ISPs). They provide the infrastructure or services enabling users to communicate, share, and access content online.

Liabilities of Intermediaries:

1. **Safe Harbor Protection**: Many legal frameworks, like India's IT Act, 2000, and the US DMCA, provide intermediaries limited liability for user-generated content, as long as they follow specific guidelines.
2. **Duty to Act**: Intermediaries must act promptly to remove illegal content, such as copyright violations or hate speech, upon notification.
3. **Compliance**: They are liable if they fail to comply with laws regarding data protection, privacy, or cybersecurity.

4. **No Immunity for Active Involvement**: If intermediaries actively participate in or encourage illegal activities, they lose protection and become liable.

Secure Electronic Records

Secure electronic records refer to digital documents or data that are protected using various security measures to ensure their authenticity, confidentiality, and integrity. These records are often used in legal, financial, and business transactions where trust and accuracy are crucial.

To ensure security, electronic records are typically encrypted, meaning they are encoded to prevent unauthorized access. Digital signatures are used to verify the identity of the person or entity that created the record, ensuring non-repudiation. Additionally, timestamps can be added to confirm the exact time of creation or modification.

Security features also include access controls, ensuring only authorized individuals can view or modify the record. Backup and storage in secure systems protect against data loss or tampering. Compliance with relevant legal standards, such as the **Electronic Signatures in Global and National Commerce (ESIGN) Act** or **eIDAS regulation**, guarantees that secure electronic records are recognized legally, making them enforceable in court. These measures foster trust in electronic transactions.

Digital Signature

A **digital signature** is a cryptographic technique used to authenticate the identity of the sender and ensure the integrity of a digital document or message. It is created using a private key to encrypt the data, which can only be decrypted by the corresponding public key, proving that the sender is the legitimate author of the document.

Digital signatures provide **non-repudiation**, meaning the signer cannot deny having signed the document. They also ensure **data integrity** by verifying that the content has not been altered after signing. Typically, a hash function is applied to the document to create a unique identifier, which is then encrypted with the private key.

Digital signatures are legally recognized in many countries, such as under the **Electronic Signatures in Global and National Commerce (ESIGN) Act** in the USA or the **eIDAS Regulation** in the EU. They are widely used in contracts, government transactions, and secure communications, offering enhanced security and trust in digital transactions.

Unit IV

Controllers

Controllers play a crucial role in overseeing and ensuring compliance with laws, regulations, and standards within a specific sector or industry. Their appointment and functions are vital for maintaining order, transparency, and accountability. Here's an overview:

Appointment of Controllers:

Controllers are typically appointed by a **governing body**, **legislative authority**, or **regulatory agency**. Their appointment is based on their expertise, experience, and qualifications relevant to the sector they are overseeing. In some cases, appointments are made for a fixed tenure or until a certain goal is achieved. The process may involve public appointments, selection committees, or nominations.

Functions of Controllers:

1. **Regulatory Oversight**: Ensure compliance with legal and regulatory frameworks.
2. **Monitoring and Reporting**: Track the activities of regulated entities and ensure they operate within set guidelines.
3. **Enforcement of Rules**: Take corrective or punitive actions against non-compliance.
4. **Licensing and Authorization**: Approve and issue licenses or permits for entities to operate legally.
5. **Conflict Resolution**: Resolve disputes and issues within the industry or sector they oversee.
6. **Policy Advice**: Provide recommendations to the government or regulatory authorities for improvements in policy or regulation.

Controllers ensure the smooth functioning of regulated industries, protecting public interest and maintaining trust.

License to Issue a Digital Signature Certificate

A **license to issue a digital signature certificate** is granted to authorized entities or **Certification Authorities (CAs)** by relevant regulatory bodies or government agencies. These entities are responsible for verifying the identity of individuals or organizations and issuing digital signature certificates, which are used to digitally sign documents and verify the signer's identity and the document's integrity.

Licensing Process:

1. **Application**: The entity wishing to issue digital signatures must apply to the relevant regulatory authority, such as the **Controller of Certifying Authorities (CCA)** in India.
2. **Eligibility Criteria**: The applicant must meet specific legal, technical, and security requirements, including the ability to maintain secure infrastructure and processes for identity verification.

3. **Audits and Compliance**: The applicant must undergo regular audits to ensure they meet security standards, and they must comply with regulations like **eIDAS** in the EU or **ESIGN** and **UETA** in the US.
4. **Approval**: Upon meeting the required criteria, the regulatory authority grants the license, allowing the entity to issue digital signature certificates.

These licensed Certification Authorities play a critical role in ensuring the security and legality of digital signatures for electronic transactions.

Renewal of a License

The **renewal of a license** to issue digital signature certificates is the process by which Certification Authorities (CAs) extend their ability to provide digital signature services after the initial license period expires. This process ensures that the CA continues to meet the required standards and remains in compliance with relevant regulations.

Steps for License Renewal:

1. **Application for Renewal**:
   - The CA must submit an application for renewal to the relevant regulatory authority (e.g., Controller of Certifying Authorities in India, or other regulatory bodies depending on the country).
   - The application must include any updated information regarding the CA's operations, security measures, and infrastructure.
2. **Compliance Check**:
   - The regulatory body will review the CA's adherence to regulatory guidelines, including the maintenance of secure infrastructure and up-to-date identity verification protocols.
   - The CA may also be subject to audits or inspections to verify compliance.
3. **Security Standards**:
   - The CA must continue to meet specific technical and security standards related to encryption, key management, and data protection.
4. **Payment of Fees**:
   - Renewal may require the payment of applicable fees to the regulatory authority.
5. **Approval and Renewal**:
   - If the CA meets all the criteria, the regulatory authority grants the renewal, allowing the CA to continue issuing digital signature certificates.

Failure to renew the license can lead to suspension or revocation of the CA's ability to issue digital signatures, which can impact its customers.

Suspension and Revocation of Digital Signature Certificate

Suspension and **revocation** of a **digital signature certificate (DSC)** are actions taken to invalidate the certificate, often due to security concerns, misuse, or non-compliance with regulations. Both processes ensure that digital signatures remain trustworthy and secure, and are usually governed by the **Certification Authority (CA)** and regulatory authorities.

Suspension of Digital Signature Certificate:

Suspension temporarily invalidates a digital signature certificate, usually when there are doubts about its security or use but not enough evidence for permanent revocation. Suspension can occur under the following circumstances:

1. **Loss or Compromise**: If the private key or other credentials are lost or compromised.
2. **Suspicious Activity**: If there is a suspicion that the certificate was used inappropriately or fraudulently.
3. **User Request**: The certificate holder may request suspension in cases such as unintentional misuse or theft.

Suspension can be reversed if the issues are resolved, and the certificate is reinstated.

Revocation of Digital Signature Certificate

Revocation is the permanent invalidation of a DSC, often due to more serious issues that cannot be corrected. Revocation occurs when:

1. **Misuse or Fraud**: The certificate was used for illegal activities or to commit fraud.
2. **Incorrect Information**: The information provided during the certificate issuance process is found to be false or misleading.
3. **Failure to Comply**: The certificate holder fails to follow necessary security protocols or regulatory requirements.
4. **User Request**: The certificate holder may request revocation in case of inactivity, termination of business, or change of identity.

Once revoked, the digital signature certificate cannot be used for signing or authentication. The revocation status is published in the **Certificate Revocation List (CRL)**, which can be accessed by other users and entities to ensure the certificate is no longer trusted.

The suspension and revocation process is managed by the Certification Authority (CA) and overseen by regulatory bodies such as the **Controller of Certifying Authorities (CCA)** in India or equivalent bodies in other countries. These actions ensure the integrity of digital transactions and protect against misuse.

Overview of GDPR

The **General Data Protection Regulation (GDPR)** is a comprehensive data privacy and protection law enacted by the European Union (EU) in May 2018. Its primary purpose is to enhance individuals' control over their personal data while imposing strict regulations on how organizations collect, process, store, and share personal information. The GDPR applies to all organizations that process personal data of EU citizens, regardless of the organization's location.

Key Principles of GDPR:

1. **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and transparently.
2. **Purpose Limitation**: Data should be collected for specific, legitimate purposes and not used beyond those purposes.
3. **Data Minimization**: Only the data necessary for the intended purpose should be collected and processed.
4. **Accuracy**: Personal data should be accurate and kept up-to-date.
5. **Storage Limitation**: Data should not be kept longer than necessary for the purposes it was collected.
6. **Integrity and Confidentiality**: Personal data must be securely protected against unauthorized access, loss, or damage.

Key Rights Under GDPR:

1. **Right to Access**: Individuals can request access to their personal data held by organizations.
2. **Right to Rectification**: Individuals can correct inaccurate or incomplete data.
3. **Right to Erasure (Right to be Forgotten)**: Individuals can request the deletion of their personal data under certain conditions.
4. **Right to Restrict Processing**: Individuals can limit how their data is processed.
5. **Right to Data Portability**: Individuals can transfer their data from one service provider to another.
6. **Right to Object**: Individuals can object to the processing of their data for certain purposes, such as direct marketing.

Enforcement and Penalties

Organizations found non-compliant with GDPR can face significant fines, up to **€20 million** or **4% of global annual turnover**, whichever is greater.

GDPR has set a global standard for data privacy and protection, influencing data protection laws in other countries and regions. It emphasizes transparency, accountability, and individuals' rights, ensuring that personal data is handled responsibly and securely.

Indian Data protection regime

India's **data protection regime** is governed by the **Personal Data Protection Bill (PDPB)**, which is designed to regulate the collection, processing, and storage of personal data by businesses and organizations. The Bill was first introduced in 2019 and is inspired by the EU's GDPR but adapted to India's unique context.

Key features of the PDPB include:

1. **Data Protection Authority (DPA)**: A central authority responsible for monitoring compliance, investigating data breaches, and ensuring enforcement of the law.
2. **Consent**: Organizations must obtain explicit consent from individuals before collecting or processing their data.
3. **Rights of Individuals**: Includes rights to access, correct, and delete personal data, as well as the right to data portability.
4. **Data Localization**: Certain sensitive data must be stored within India.
5. **Penalties**: Non-compliance with the PDPB can result in significant fines.

This regime aims to safeguard personal privacy, promote transparency in data handling, and align India with global data protection standards.