Module -1

1. What is cloud computing?
Ans: the on-demand delivery of IT resources—including servers, storage, databases, networking, software, and AI-powered analytics—over the internet with pay-as-you-go pricing.

Service Models

Cloud resources are typically provided through four primary service models, often referred to as the cloud "stack":

- **Software as a Service (SaaS):** Delivers ready-to-use, fully managed applications through a browser.
- **Platform as a Service (PaaS):** Provides a framework (hardware and software tools) that allows developers to build, test, and deploy applications without managing underlying infrastructure.
- **Infrastructure as a Service (IaaS):** Offers the basic building blocks of cloud IT, such as virtual servers, networking, and raw storage.
- **Serverless Computing (FaaS):** A newer model that allows developers to run code in response to specific triggers or events without managing or scaling any servers.

Key Deployment Models

Organizations choose how to deploy these services based on security, cost, and control needs:

- **Public Cloud:** Resources are owned and operated by third-party providers (like **AWS, Microsoft Azure, or Google Cloud**) and shared among multiple customers over the public internet.
- **Private Cloud:** Computing resources are used exclusively by a single organization, offering higher security and control; these can be hosted on-premises or by a third party.
- **Hybrid Cloud:** Combines public and private clouds, allowing data and applications to be shared between them to balance scalability and security.

- **Multicloud:** A dominant strategy in 2026 where an organization uses services from two or more different public cloud providers to avoid vendor lock-in and optimize specific workloads.

Cloud Computing is Essential

- **AI Integration:** By 2026, AI is no longer just an "add-on" but is embedded into every layer of cloud platforms for autonomous resource optimization, predictive scaling, and advanced security.
- **Cost Efficiency:** It shifts IT costs from large upfront capital expenditures (CapEx) to manageable, variable operational expenses (OpEx).
- **Elasticity & Scalability:** Organizations can instantly scale resources up or down to meet traffic spikes (e.g., during product launches) or quiet periods.
- **Sustainability:** By 2026, a majority of organizations use sustainability-enabled monitoring to manage their energy consumption, as cloud migration can reduce carbon footprints by up to 90%

2. Describe cloud computing deploy model.

Ans: defines how a cloud environment is structured, who owns the infrastructure, and who has access to its resources.

Deployment Models

- **Public Cloud:** Computing resources (servers, storage) are owned and operated by third-party providers (e.g., AWS, Microsoft Azure, Google Cloud) and shared among multiple organizations over the internet. It is highly scalable and uses a **pay-as-you-go** pricing model.
- **Private Cloud:** A cloud environment used exclusively by a single organization. It can be hosted on-site or by a third party, offering higher security, control, and customization for sensitive data or regulated industries.
- **Hybrid Cloud:** Integrates private and public cloud environments, allowing data and applications to move seamlessly between them. By 2026, it is a dominant architecture for balancing scalability with strict data sovereignty requirements.

- **Community Cloud:** Shared by several organizations with common concerns, such as specific compliance (HIPAA for healthcare) or security needs. Costs are shared among the community members.

Modern Trends

- **Multi-cloud Strategy:** The use of services from multiple cloud vendors (e.g., combining AWS for hosting and Azure for AI) has become the "new normal" to avoid vendor lock-in and increase resilience.
- **Distributed and Edge Cloud:** Extending cloud services to the "edge" (closer to where data is generated) to support real-time, low-latency applications like IoT and autonomous systems.
- **Industry-Specific Clouds:** The rise of "vertical clouds" tailored with built-in compliance for specific sectors like finance, healthcare, and manufacturing.
- **Sovereign Cloud:** An increasing focus on region-restricted clouds to meet global data localization laws and maintain national data security.

3. What are components of cloud computing?

Ans:

1. Front-End

This is the interface that the end-user interacts with to access cloud services.

- **User Interface (UI):** Graphical interfaces such as web browsers (Chrome, Firefox) or mobile applications used to send requests to the cloud.
- **Client Infrastructure:** The hardware on the user's side, such as laptops, smartphones, or local network routers, that facilitates the connection.

2. Back-End

This refers to the "cloud" itself—the resources managed by the provider to fulfill user requests.

- **Infrastructure:** The physical hardware in data centers, including servers, CPU/GPUs, and storage arrays.

- **Virtualization Layer:** A critical component that uses hypervisors to split physical hardware into multiple virtual machines (VMs), allowing many users to share the same resources efficiently.
- **Cloud Runtime:** Provides the execution environment for these virtual machines, acting essentially as a cloud-based operating system.
- **Storage:** Scalable repositories for data, typically categorized as **Block** (for databases), **File** (for shared workspaces), or **Object** storage (for unstructured data like images).
- **Management:** Middleware that coordinates communication between the front and back ends, allocates resources, and manages traffic.
- **Security:** Built-in mechanisms such as firewalls, data encryption, and Identity and Access Management (IAM) to protect resources and user data.

3. Modern Strategic Pillars

In addition to technical parts, modern cloud architecture is governed by "pillars" that ensure system health:

- **Operational Excellence:** Automated monitoring and AI-driven DevOps.
- **Reliability:** Redundancy and disaster recovery across multiple regions.
- **Sustainability:** A 2026 priority focusing on energy-efficient chips (like ARM-based processors) and carbon-neutral data centers.
- **Edge & AI Integration:** Specialized components like **Vector Databases** for AI context and **Edge Micro-Data Centers** to reduce latency for IoT devices.

4. cloud computing advantage and disadvantage Advantages of Cloud Computing.

Ans:

Advantages of Cloud Computing

- **Cost Efficiency & Financial Agility:** Eliminates large upfront capital expenditures (CapEx) for hardware. Instead, it uses a **pay-as-you-go** (OpEx) model where you pay only for resources used.

- **Scalability & Elasticity:** Resources can be scaled up or down instantly to meet fluctuating demand, such as handling traffic spikes during major sales events without over-provisioning.
- **Accessibility & Global Collaboration:** Data and applications are accessible from any device with an internet connection, facilitating real-time collaboration for remote and distributed teams.
- **Access to Cutting-Edge Tech:** Provides instant access to advanced technologies like **Generative AI**, machine learning, and big data analytics without needing specialized in-house infrastructure.
- **Reliability & Disaster Recovery:** Leading providers offer built-in redundancy across multiple geographic regions, ensuring business continuity even during local hardware failures.
- **Sustainability:** Large-scale cloud data centers are often more energy-efficient than on-premises setups, helping companies reduce their carbon footprint.

Disadvantages of Cloud Computing

- **Internet Dependency:** Full reliance on stable connectivity. Any internet outage or service disruption at the provider level can halt critical business operations.
- **Security & Privacy Risks:** While providers offer advanced security, the "shared responsibility model" means users are still responsible for securing their data. Misconfigurations account for a significant percentage of cloud breaches.
- **Vendor Lock-In:** It is often complex and expensive to migrate data or applications between different cloud providers due to proprietary tools, APIs, and high data egress (transfer) fees.
- **Rising & Unpredictable Costs:** While cost-effective at first, "bill shock" is common in 2026 due to unmanaged resource scaling, complex pricing tiers, and rising energy costs impacting provider fees.
- **Limited Control:** Users have minimal control over the underlying physical infrastructure and backend processes, which may not meet the needs of organizations with highly specific customization or compliance requirements.

- **Skill Shortage:** There is a significant gap in 2026 for IT professionals with specialized cloud architecture and security expertise, often requiring companies to invest heavily in upskilling.

Module 1 CS- Introduction

1. what is meaning of cyber security

Ans: the strategic practice of protecting people, digital assets, and critical infrastructure from increasingly sophisticated digital attacks.

1. Objective

Cybersecurity aims to safeguard the three pillars of data and system health:

- **Confidentiality:** Ensuring sensitive information (like medical records or trade secrets) is only accessible to authorized users.
- **Integrity:** Protecting data from being altered, manipulated, or deleted by unauthorized parties.
- **Availability:** Ensuring that systems and information are accessible to those who need them when they need them, preventing downtime from attacks like DDoS.

2. The Human-Process-Technology Intersection

Modern cybersecurity in 2026 is no longer just about software; it is the convergence of three distinct areas:

- **People:** Educated users who follow best practices and recognize threats like AI-powered phishing.
- **Processes:** Established frameworks (such as NIST) that guide how an organization identifies, protects, detects, responds to, and recovers from attacks.

- **Technology:** The actual tools used for defense, including firewalls, encryption, and AI-driven monitoring.

3. Strategic Shifts

As of 2026, the "meaning" of cybersecurity includes several advanced strategic concepts:

- **Zero Trust:** A model that operates on the principle of **"never trust, always verify,"** requiring continuous validation for every access request regardless of its origin.
- **Cyber Resilience:** A shift in focus from merely *preventing* attacks to ensuring a business can *withstand* and quickly recover from them with minimal disruption.
- **AI Integration:** The use of AI agents to autonomously detect and respond to threats in real-time, countering an "AI arms race" where attackers use similar automation.
- **Identity as the Perimeter:** With the rise of remote work and cloud services, protecting a user's digital identity has replaced the traditional office network boundary as the primary line of defense.

2. What is offensive and defensive in cyber security?
Ans:

Offensive Cybersecurity (OffSec)

Offensive security is a **proactive** approach that involves thinking and acting like an attacker to identify weaknesses before they are exploited by malicious actors.

- **Primary Goal:** To find, test, and validate vulnerabilities in a controlled, ethical manner.
- **Key Techniques:**
- **Penetration Testing:** Human-led, simulated attacks targeting specific systems or applications.

- **Red Teaming:** Adversarial simulations that mimic real-world threat actors to test an organization's detection and response capabilities.
- **Vulnerability Assessments:** Automated scanning to identify known security gaps.
- **Social Engineering:** Testing employee awareness through simulated phishing or pretexting.
- **Typical Roles:** Ethical hackers, red team analysts, and penetration testers.
- **Common Tools:** Kali Linux, Metasploit, Burp Suite, and Cobalt Strike.

Defensive Cybersecurity (DefSec)

Defensive security focuses on building and maintaining the infrastructure to **prevent, detect, and respond** to threats in real-time.

- **Primary Goal:** To shield assets, minimize damage, and ensure business continuity during or after an attack.
- **Key Techniques:**
- **Perimeter Defense:** Implementing firewalls, intrusion detection/prevention systems (IDS/IPS), and encryption.
- **Incident Response:** Following predefined playbooks to contain and recover from breaches.
- **Continuous Monitoring:** Using SIEM (Security Information and Event Management) and SOC (Security Operations Center) services to watch for suspicious activity.
- **Identity Management:** Enforcing **Zero Trust** models, Multi-Factor Authentication (MFA), and access controls.
- **Typical Roles:** SOC analysts, incident responders, and security engineers.
- **Common Tools:** Firewalls, antivirus software, Splunk, CrowdStrike, and SOAR platforms.

3. what is cyberspace and low.

Ans: cyberspace refers to the global, virtual environment where digital interactions occur across interconnected networks of computers and

electronic systems. It encompasses more than just the internet; it includes all communications, data exchange, and digital platforms like social media and cloud computing.

Cyber law (or the "laws of cyberspace") refers to the legal system and regulations that govern human activity and business transactions within this digital domain.

The Meaning of Cyberspace

- **Virtual Realm:** It is an immaterial "location" created by machine connections where users can interact and share information instantly, regardless of physical distance.
- **Layered Structure:** Modern definitions often view it in layers: the **physical** (cables, servers), the **logical** (software, protocols), and the **social/persona** (users and digital identities).
- **Key Characteristics:** It is borderless, dynamic, and continuously evolving due to technological innovations like AI and the Internet of Things (IoT).

Key Cyber Laws & Regulations

As of 2026, the legal landscape has shifted toward stricter, enforceable mandates focused on resilience and data protection.

- **Global Frameworks:**
- **EU NIS2 Directive:** Enforced across Europe from **April 2026**, this directive mandates robust cyber risk management and strict incident reporting for essential sectors.
- **EU AI Act:** Categorizes AI systems by risk and imposes strict oversight on "high-risk" applications.
- **UN Convention against Cybercrime:** The first comprehensive global treaty, signed by over 70 nations in late 2025, to harmonize international cooperation against digital threats.
- **Regional Examples:**

- **United States (CIRCIA):** Final rules expected in 2026 require critical infrastructure operators to report substantial cyber incidents to CISA within **72 hours**.
- **India:** The **Digital Personal Data Protection (DPDP) Act** is in active enforcement, requiring clear consent for data processing and localization of citizen data.
- **Sweden:** The new **Cyber Security Act** (implementing NIS2) comes into force on **January 15, 2026**, applying to municipalities and thousands of private operators.

The "Four Laws" of Cyberspace Governance

Experts often categorize how cyberspace is controlled using four forces:

1. **Law:** Formal legal regulations and statutes.
2. **Code:** The software architecture and programming that dictates what is technically possible.
3. **Markets:** Economic forces and pricing models.
4. **Norms:** Social expectations and ethical standards (Cyberethics).

4 . What is cyber welfare?

Ans: a term often used to describe the protection of citizens' digital lives and the proactive measures taken by governments or organizations to ensure a safe, inclusive, and equitable cyberspace.

Cyber Welfare

- **Digital Inclusion & Literacy:** Ensuring all citizens have access to the internet and the skills to use it safely, regardless of age, gender, or location.
- **Citizen Protection:** Implementing services and laws to protect individuals from cyberbullying, online scams, and digital identity theft.
- **Psychological Safety:** Combatting digital propaganda and disinformation that can cause public panic or erode trust in social and political systems.

- **Resilient Public Services:** Securing essential digital services—such as online banking, health records, and social security payments—to prevent disruptions that could harm a population's daily life.

Key Initiatives

As of 2026, many nations have integrated cyber welfare into their national security and public service agendas:

- **Cybercrime Roadmap 2026:** Focused on training thousands of law enforcement personnel in advanced forensic tools to better assist victims of digital crimes.
- **AI for Social Good:** Global summits like the India AI Impact Summit 2026 focus on using technology to solve public challenges in agriculture, health, and education while ensuring "Safe and Trusted AI".
- **Indigenous Security:** A shift toward developing home-grown software and AI-enabled tools to ensure that the infrastructure citizens depend on is free from foreign interference.

5 . Explain the Types of Hacker

Ans: hackers are classified based on their intent, the legality of their actions, and their level of expertise. The traditional "hat" color system remains the standard, but it has expanded to include specialized roles driven by AI and geopolitical shifts.

The Three Hackers

- **White Hat (Ethical Hackers):** These are security experts hired by organizations to find and fix vulnerabilities legally. They use their skills for defense and must have explicit permission before testing any system.
- **Black Hat (Cybercriminals):** These individuals break into systems illegally for personal or financial gain. They are responsible for most data breaches, ransomware attacks, and malware distribution.

- **Gray Hat:** These hackers operate in a moral middle ground. They may hack into a system without permission to find flaws, but they typically don't intend to cause harm. They often report the issue to the owner, sometimes asking for a fee in return.

Specialized Hacker Types

- **Red Hat (Vigilantes):** Unlike ethical hackers who report bugs, red hats aggressively hunt and attack black hat hackers to shut down their servers and destroy their resources.
- **Blue Hat:** In 2026, this term has two main uses:
- **External Testers:** Security experts invited by a company to test new software for bugs before its official launch.
- **Revenge Hackers:** Unskilled individuals who hack solely to get back at a person or institution.
- **Green Hat (The Learners):** Beginner hackers who are eager to learn and often frequent hacking forums. While not necessarily malicious, they can cause accidental damage due to lack of experience.
- **Purple Hat:** These hackers focus on improving their own security by testing their skills on their own systems or in controlled environments.
- **Yellow Hat:** A less common category referring to those who focus specifically on developing better digital defense tools rather than executing attacks.

Hacking Groups & Roles

- **Hacktivists:** Hackers motivated by political or social causes. They use digital attacks like website defacement or data leaks to protest against governments or corporations.
- **State-Sponsored Hackers:** Highly skilled professionals employed by national governments for international espionage, sabotage, or information gathering.
- **Script Kiddies:** Amateurs who use pre-written tools or "scripts" created by others because they lack the knowledge to write their own.
- **Insider Threats:** Employees, contractors, or partners who misuse their authorized access to steal data or sabotage an organization from within.

- **AI Hackers (New in 2026):** Specialists who use **agentic AI** to automate the discovery of vulnerabilities and conduct hyper-realistic social engineering attacks

6 . What is the full form of SOC in cyber security

Ans: It is a centralized function within an organization that uses people, processes, and technology to continuously monitor and improve security posture while preventing, detecting, and responding to cyber incidents.

Functions of a SOC

Modern SOCs in 2026 act as a "command center" for digital defense, performing several key duties:

- **Continuous Monitoring:** Scanning networks, servers, and endpoints 24/7 for suspicious activity or anomalies.
- **Incident Response:** Acting as first responders to isolate threats, such as ransomware or data breaches, and limit damage.
- **Threat Hunting:** Proactively searching for hidden threats that may have bypassed automated security tools.
- **Log Management:** Collecting and analyzing data from every network event to establish normal activity baselines.
- **Compliance Management:** Ensuring the organization meets regulatory standards like GDPR, HIPAA, or PCI-DSS.

Alternative Meaning: Compliance Reports

In the context of auditing and compliance, **SOC** also stands for **System and Organization Controls**.

- **SOC 1:** Focuses on financial reporting controls.
- **SOC 2:** Evaluates security, availability, and privacy controls (often required for SaaS vendors).
- **SOC 3:** A high-level, public version of a SOC 2 report.

7. What are the Challenges of Cyber Security

Ans: the challenges of cybersecurity have shifted from isolated technical issues to systemic, machine-speed risks. The convergence of artificial intelligence, geopolitical tensions, and an increasingly complex digital landscape has created a multi-dimensional battlefield.

1. AI-Driven "Arms Race"

- **Weaponized AI:** Attackers use **agentic AI** to autonomously scan networks, identify zero-day vulnerabilities, and launch hyper-personalized phishing campaigns at a scale and speed that human defenders cannot match.
- **Deepfakes and Synthetic Identity:** Sophisticated AI-generated audio and video are used to bypass biometric authentication and trick employees into authorizing fraudulent transactions.
- **Model Poisoning:** Adversaries target AI systems themselves through prompt injection or data poisoning to make corporate AI tools reveal secrets or perform malicious actions.

2. Sophisticated Extortion & Crime

- **Professionalized Ransomware:** The "Ransomware-as-a-Service" (RaaS) model has democratized high-level attacks, allowing non-technical criminals to launch sophisticated campaigns.
- **Multi-Stage Extortion:** Beyond just encrypting data, attackers now steal sensitive information and threaten to leak it (double extortion) or launch DDoS attacks (triple extortion) to force payment.
- **Commodity Cybercrime:** The underground market has become an industrial-scale economy, estimated to cost $20 trillion annually by 2026.

3. Infrastructure & Supply Chain Vulnerabilities

- **Supply Chain Exposures:** Modern businesses are only as secure as their weakest vendor. Attacks targeting third-party software providers or managed service providers (MSPs) can cause ripple effects across entire global ecosystems.

- **OT and IoT Insecurity:** Critical infrastructure—including energy grids and water facilities—is increasingly targeted as operational technology (OT) becomes more connected but remains difficult to patch.
- **Virtualization Targeting:** Attackers are pivoting from individual computers to the underlying virtualization layers (hypervisors), which can grant control over an entire digital estate in one breach.

4. Systemic Operational Hurdles

- **The Global Skills Gap:** There remains a critical shortage of millions of skilled cybersecurity professionals, making it difficult for organizations to maintain 24/7 proactive monitoring.
- **Cloud Misconfigurations:** Rapid cloud migration often results in "security drift" or improper setups that leave massive amounts of data exposed to public internet scanners.
- **The "Human Factor":** Despite technical advances, human error (such as poor password hygiene or falling for social engineering) remains the primary entry point for over 90% of attacks.

5. Emerging Global Risks

- **Geopolitical Cyber Warfare:** State-sponsored groups from nations like China, Russia, and Iran use cyberattacks as tools for espionage, intellectual property theft, and political influence.
- **The Quantum Threat:** The "Harvest Now, Decrypt Later" strategy involves attackers stealing encrypted data today to decrypt it once powerful quantum computers become available.
- **Regulatory Fragmentation:** Organizations must navigate an increasingly complex web of conflicting international regulations (like NIS2, DORA, and CIRCIA) that demand rapid breach reporting and high levels of accountability