Toppersnotes®
Unleash the topper in you

Rajasthan – CET

स्नातक स्तर

सामान्य पात्रता परीक्षा (CET)

भाग - 6

सामान्य विज्ञान एवं कम्प्यूटर

SIERRA INNOVATIONS

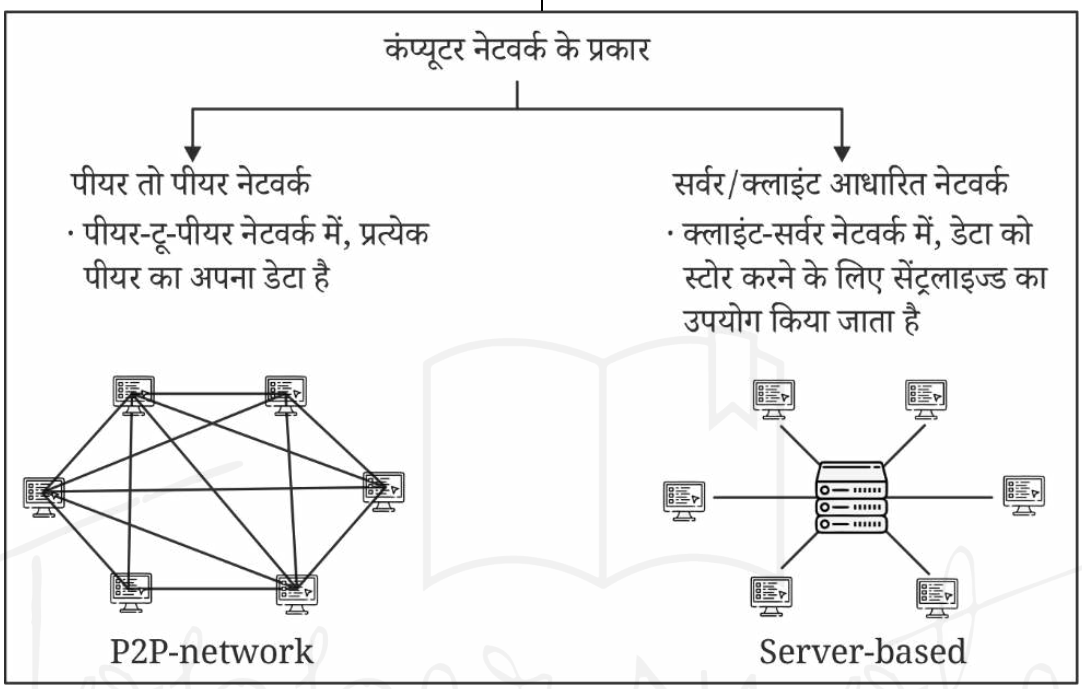
विषयसूची

1 CHAPTER

सूचना और संचार प्रौद्योगिकी (ICT)

कंप्यूटर नेटवर्क

कंप्यूटर नेटवर्क तब बनते हैं जब दो या अधिक कंप्यूटर आपस में सूचना और संसाधनों के आदान-प्रदान के लिए जुड़े होते हैं। यह विभिन्न दूरी और स्तरों पर संचार और सहयोग को सक्षम बनाता है।

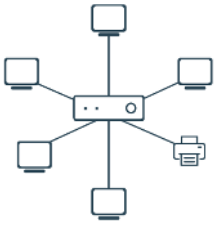
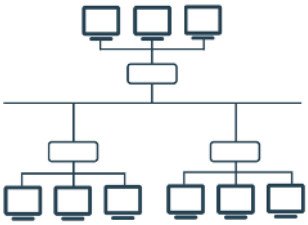
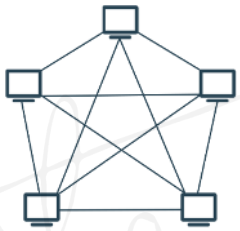


कंप्यूटर नेटवर्क के प्रकार (क्षेत्र/कवरेज के आधार पर)

1. LAN (लोकल एरिया नेटवर्क):
   - ✓ यह नेटवर्क एक छोटे भौगोलिक क्षेत्र (लगभग 1 किमी तक) में कंप्यूटरों को जोड़ने के लिए उपयोग किया जाता है।
   - ✓ उदाहरण: ईथरनेट (Ethernet)
2. MAN (मेट्रोपॉलिटन एरिया नेटवर्क):
   - ✓ यह नेटवर्क एक बड़े भौगोलिक क्षेत्र (लगभग 100 किमी तक) में कंप्यूटरों को जोड़ने के लिए उपयोग किया जाता है।
   - ✓ उदाहरण: शहर का नेटवर्क
3. WAN (वाइड एरिया नेटवर्क):
   - ✓ यह नेटवर्क लंबी भौतिक दूरी जैसे देश, महाद्वीप या पूरे विश्व को शामिल करता है।
   - ✓ उदाहरण: इंटरनेट
4. WLAN (वायरलेस लोकल एरिया नेटवर्क):
   - ✓ इसे *LAWN (लोकल एरिया वायरलेस नेटवर्क)* भी कहा जाता है।
5. HAN (होम एरिया नेटवर्क):
   - ✓ यह नेटवर्क घर में उपयोग किए जाने वाले कंप्यूटरों को जोड़ने के लिए उपयुक्त है।

नेटवर्क टोपोलॉजी (Network Topology)

- ➢ कंप्यूटर नेटवर्क में कंप्यूटरों को आपस में जोड़ने का माध्यम नेटवर्क टोपोलॉजी कहलाता है।

1. बस टोपोलॉजी (Bus Topology): ✓ इस टोपोलॉजी में कंप्यूटर एक केंद्रीय केबल के माध्यम से एक रेखा में जुड़े होते हैं।	
2. रिंग टोपोलॉजी (Ring Topology): ✓ इसमें कंप्यूटर एक सर्कुलर (गोलाकार) तरीके से केबल के माध्यम से जुड़े होते हैं।	
3. स्टार टोपोलॉजी (Star Topology) ✓ इस टोपोलॉजी में कंप्यूटर एक केंद्रीय डिवाइस (*हब*) के माध्यम से जुड़े होते हैं।	
4. ट्री टोपोलॉजी (Tree Topology): ✓ इसमें कंप्यूटर विभिन्न स्तरों पर एक-दूसरे से जुड़े होते हैं।	
5. मेश टोपोलॉजी (Mesh Topology): ✓ यह ज्यामिति में उपयोग की जाने वाली टोपोलॉजी है। ✓ यह टोपोलॉजी डेटा को सबसे तेज़ गति से ट्रांसफर करने के लिए उपयोग की जाती है।	

<u>नेटवर्किंग डिवाइस</u>

- कंप्यूटर नेटवर्क में, दो या अधिक कंप्यूटरों को आपस में जोड़ने के लिए उपयोग किए जाने वाले हार्डवेयर को नेटवर्किंग डिवाइस कहा जाता है।
- कंप्यूटर नेटवर्क में विभिन्न प्रकार के नेटवर्किंग डिवाइस उपयोग किए जाते हैं, जैसे:

(i) स्विच (Switch) – यह डिवाइस लोकल एरिया नेटवर्क (LAN) में उपयोग की जाती है और सुरक्षा भी प्रदान करती है।

✓ स्विच के माध्यम से कंप्यूटर, सर्वर और प्रिंटर साझा किए जाते हैं।

(ii) हब (Hub) – यह भी LAN में उपयोग किया जाता है, लेकिन स्विच की तरह सुरक्षा प्रदान नहीं करता।

✓ यह नेटवर्क से जुड़े सभी प्रकार के कंप्यूटरों को समान डेटा वितरित करता है।

(iii) ब्रिज (Bridge) – यह डिवाइस दो समान LANs को जोड़ने के लिए उपयोग की जाती है।

(iv) गेटवे (Gateway) – यह डिवाइस दो अलग-अलग LANs को जोड़ने के लिए उपयोग की जाती है।

(v) राउटर (Router) – यह डिवाइस इंटरनेट या वाइड एरिया नेटवर्क (WAN) पर विभिन्न कंप्यूटरों को जोड़ने के लिए उपयोग की जाती है।

(vi) रीपीटर (Repeater) – यह डिवाइस नेटवर्क से आने वाले कमजोर सिग्नल को कई सिग्नल में विभाजित करके डेटा प्रक्रिया को तेज करने के लिए उपयोग की जाती है।

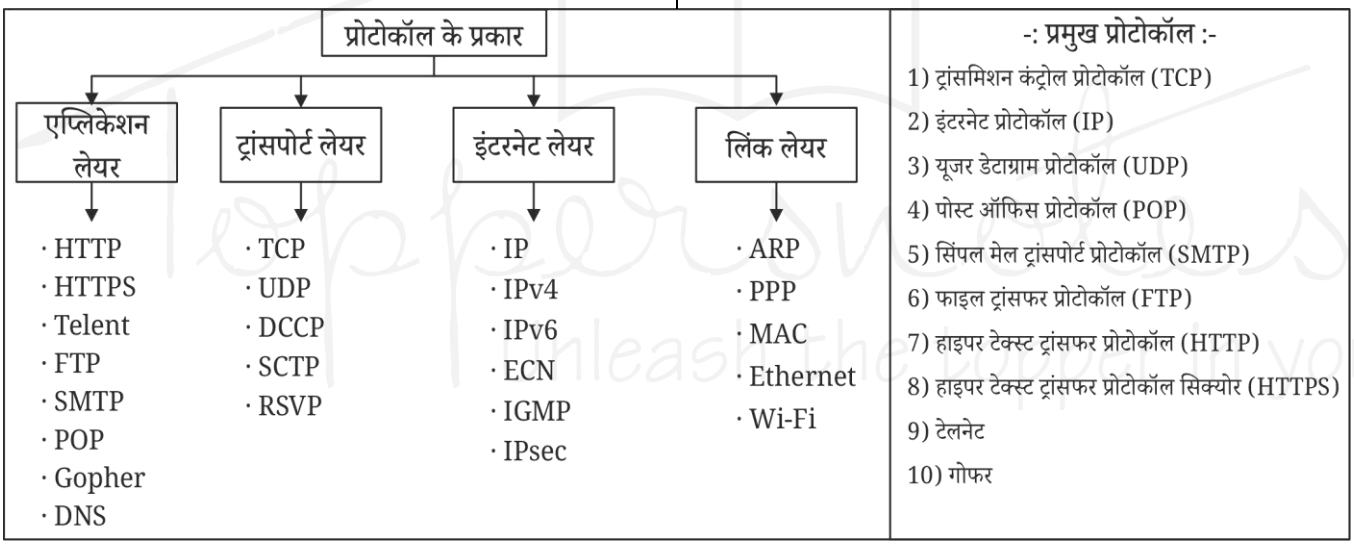
(vii) मोडेम (MODEM) – यह दूरसंचार डिवाइस है, जो डिजिटल डेटा को एनालॉग और एनालॉग डेटा को डिजिटल में परिवर्तित करने के लिए उपयोग की जाती है।

इंटरनेट

- इंटरनेट एक जटिल नेटवर्क है, जो उच्च-गति संचार प्रौद्योगिकियों द्वारा जुड़े कंप्यूटरों का समूह है। इसे कोई एक व्यक्ति या सरकार नियंत्रित नहीं करती है, जिससे यह एक स्वतंत्र और खुला संसाधन बनता है।
- उद्भव: इंटरनेट की शुरुआत 1960 के दशक के अंत में अमेरिकी रक्षा विभाग द्वारा वित्त पोषित ARPANET प्रोजेक्ट से हुई।
- 1980 और 1990 के दशक में इसका विस्तार हुआ और यह वैश्विक नेटवर्क बन गया।

इंटरनेट प्रोटोकॉल

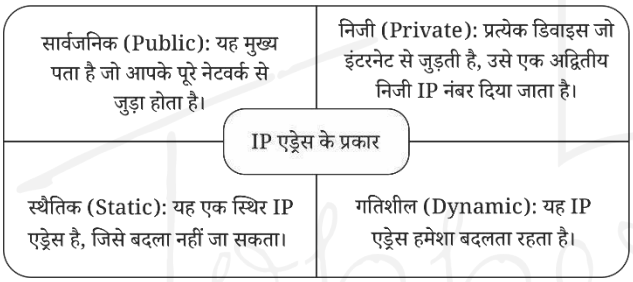
- इंटरनेट प्रोटोकॉल इंटरनेट और समान कंप्यूटर नेटवर्क में उपयोग किए जाने वाले संचार प्रोटोकॉल का समूह है।
- इसे आमतौर पर TCP/IP (ट्रांसमिशन कंट्रोल प्रोटोकॉल और इंटरनेट प्रोटोकॉल) कहा जाता है।
- यह डेटा को पैकेट में बदलने, एड्रेसिंग, ट्रांसमिशन, रूटिंग और रिसीविंग की प्रक्रिया को परिभाषित करता है।
- प्रोटोकॉल की चार परतें (Layers):
  1. लिंक लेयर
  2. इंटरनेट लेयर
  3. ट्रांसपोर्ट लेयर
  4. एप्लिकेशन लेयर



महत्वपूर्ण प्रोटोकॉल्स

1. TCP (ट्रांसमिशन कंट्रोल प्रोटोकॉल)
   - ✓ यह किसी भी संदेश को छोटे-छोटे पैकेट्स में विभाजित करके उन्हें स्रोत से गंतव्य तक भेजता है और वहां पुनः जोड़ता है।
   - ✓ यह IP के साथ मिलकर कार्य करता है, जो प्रत्येक कंप्यूटर को एक अद्वितीय नाम (IP एड्रेस) प्रदान करता है।
   - ✓ इसलिए इसे TCP/IP भी कहा जाता है।
2. IP (इंटरनेट प्रोटोकॉल)
   - ✓ यह इंटरनेट से जुड़े किसी भी डिवाइस के लिए एक अद्वितीय एड्रेस प्रदान करता है।
   - ✓ यह एड्रेस इंटरनेट सेवा प्रदाता (ISP) द्वारा दिया जाता है।
   - ✓ दो कंप्यूटर एक ही IP एड्रेस नहीं रख सकते।

IPv4 (इंटरनेट प्रोटोकॉल वर्शन 4)	IPv6 (इंटरनेट प्रोटोकॉल वर्शन 6)
➢ यह सबसे अधिक उपयोग किया जाने वाला इंटरनेट प्रोटोकॉल है, जो 1970 में विकसित हुआ। ➢ यह 32-बिट फॉर्मेट (4 बाइट्स) में IP एड्रेस को विभाजित करता है। ➢ प्रत्येक तीन-अंकों के समूह में 0-255 के बीच संख्या हो सकती है। ➢ समूह को डॉट (.) से अलग किया जाता है।	➢ यह 1998 में विकसित हुआ। ➢ यह 128-बिट फॉर्मेट (16 बाइट्स) में IP एड्रेस को विभाजित करता है। ➢ प्रत्येक समूह को कॉलन (:) से अलग किया जाता है।



FTP – फाइल ट्रांसफर प्रोटोकॉल

- यह प्रोटोकॉल एक सिस्टम से दूसरे सिस्टम पर फाइल ट्रांसफर करने के लिए उपयोग किया जाता है।
- इसके लिए एक विशेष सॉफ़्टवेयर (क्लाइंट) का उपयोग किया जाता है।
- इसके माध्यम से साधारण टेक्स्ट फाइल से लेकर मल्टीमीडिया फाइल तक को आसानी और तेजी से अपलोड और डाउनलोड किया जा सकता है।

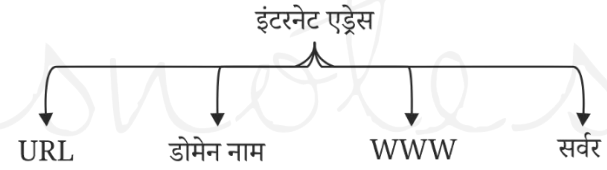
SMTP – सिंपल मेल ट्रांसफर प्रोटोकॉल

- SMTP एक लोकप्रिय ईमेल प्रोटोकॉल है, जिसका उपयोग ईमेल भेजने के लिए किया जाता है।
- यह प्रोटोकॉल एक कंप्यूटर से दूसरे कंप्यूटर पर ईमेल भेजने के लिए नियम निर्धारित करता है।

HTTP – हाइपर टेक्स्ट ट्रांसफर प्रोटोकॉल

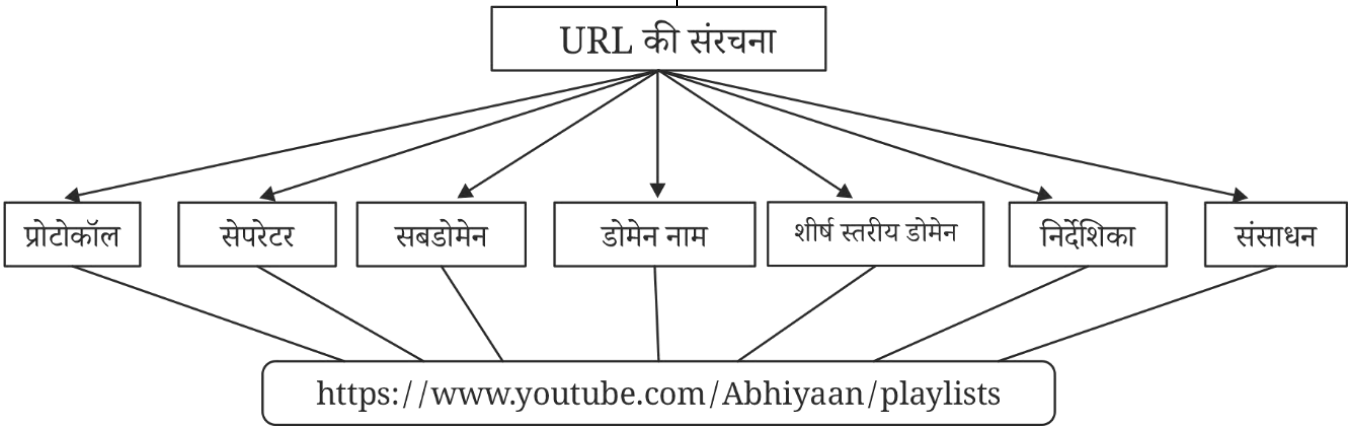
- HTTP (Hypertext Transfer Protocol) इंटरनेट पर वेब पेजों जैसे हाइपर टेक्स्ट डाक्यूमेंट्स को ट्रांसफर करने के लिए उपयोग किया जाने वाला प्रोटोकॉल है।
- यह संदेशों को प्रारूपित और ट्रांसमिट करने का तरीका और वेब सर्वर और ब्राउज़र को विभिन्न आदेशों पर प्रतिक्रिया देने के तरीके को परिभाषित करता है।

इंटरनेट एड्रेस



URL (यूनिफॉर्म रिसोर्स लोकेटर)

- इंटरनेट पर प्रदर्शित प्रत्येक वेब पेज का एक विशिष्ट पता होता है, जिसे URL कहते हैं।
- यह वेब पेज की स्थिति और उससे संबंधित अन्य जानकारी बताता है।



प्रोटोकॉल

- डेटा को वेब पर ट्रांसफर करने के लिए प्रोटोकॉल का उपयोग किया जाता है।
- सबसे लोकप्रिय प्रोटोकॉल HTTPS (हाइपर टेक्स्ट ट्रांसफर प्रोटोकॉल सिक्योर) है।
- HTTP, FTP, mailto, telnet और news जैसे प्रोटोकॉल भी मानक प्रोटोकॉल हैं।

सेपरेटर (Separator)

- ये विशेष संकेत हैं, जो URL के विभिन्न भागों को एक-दूसरे से अलग करने के लिए उपयोग किए जाते हैं।

डोमेन नेम

- डोमेन नेम एक वेबसाइट का नाम होता है, जो IP एड्रेस का उपनाम (Nickname) होता है।
- डोमेन नेम सिस्टम (DNS) IP एड्रेस को शब्दों से बने डोमेन नाम में परिवर्तित करता है।
- डोमेन नेम में अधिकतम 64 अक्षर हो सकते हैं।

डोमेन नेम सर्विस (DNS): इंटरनेट पर विभिन्न होस्ट के नाम और पते का डेटाबेस है।

www/ वर्ल्ड वाइड वेब

- वर्ल्ड वाइड वेब (WWW), जिसे आमतौर पर वेब कहा जाता है, एक सूचना प्रणाली है, जिसमें डाक्यूमेंट्स और अन्य वेब संसाधन Uniform Resource Locator (URL) द्वारा पहचाने जाते हैं।
- ये संसाधन हाइपरटेक्स्ट के माध्यम से इंटरलिंक किए जा सकते हैं और इंटरनेट के माध्यम से उपलब्ध होते हैं।

सर्वर (Server)

- सर्वर एक प्रकार का डेटा स्टोरेज डिवाइस है, जो क्लाइंट (कंप्यूटर या अन्य इंटरनेट से जुड़े डिवाइस) को सूचना या डेटा प्रदान करता है।
- हमारा कंप्यूटर एक होस्ट कंप्यूटर होता है क्योंकि यह सभी सर्वर्स से सूचना प्राप्त कर सकता है।

सर्वर के प्रकार और उनके उपयोग:

1. एप्लिकेशन सर्वर: वेब ऐप्स होस्ट करता है, जिससे नेटवर्क उपयोगकर्ता बिना इंस्टॉलेशन के उन्हें चला सकते हैं।
2. कैटलॉग सर्वर: वितरित नेटवर्क जानकारी के इंडेक्स को बनाए रखता है।
3. कम्युनिकेशन सर्वर: नेटवर्क के भीतर संचार को सक्षम करता है।
4. कंप्यूटिंग सर्वर: नेटवर्क पर CPU और RAM जैसी कंप्यूटिंग संसाधनों को साझा करता है।
5. डेटाबेस सर्वर: डेटाबेस को बनाए रखता है और आवश्यक डेटा साझा करता है।
6. फैक्स सर्वर: नेटवर्क पर फैक्स मशीनों को साझा करता है।
7. फाइल सर्वर: फाइल्स और स्टोरेज स्पेस को साझा करता है।
8. गेम सर्वर: मल्टीप्लेयर गेमिंग को सक्षम करता है।
9. मेल सर्वर: ईमेल संचार को सुविधाजनक बनाता है।
10. प्रिंट सर्वर: प्रिंटर को नेटवर्क पर साझा करता है।
11. प्रॉक्सी सर्वर: सामग्री को नियंत्रित करता है, ट्रैफ़िक प्रदर्शन सुधारता है और नेटवर्क की सुरक्षा करता है।
12. वेब सर्वर: वेब पेज होस्ट करता है और ब्राउज़र्स के लिए वर्ल्ड वाइड वेब को सुलभ बनाता है।

इंटरनेट कनेक्शन के प्रकार

इंटरनेट कनेक्शन चार प्रकार के हो सकते हैं:

1. डायल-अप कनेक्शन
   - ✓ यह दो डिवाइसों के बीच मानक टेलीफोन सेवा का उपयोग करके कनेक्शन बनाता है।
2. ब्रॉडबैंड कनेक्शन
   - ✓ ब्रॉडबैंड का पूर्ण रूप *ब्रॉड बैंडविड्थ* है।
   - ✓ यह एक उच्च-गति इंटरनेट कनेक्शन है, जो वाइड बैंड फ्रिक्वेंसी का उपयोग करता है।
   - ✓ यह कनेक्शन कॉक्सियल केबल, ऑप्टिकल फाइबर और ट्विस्टेड पेयर का उपयोग करता है।

- ✓ डिजिटल सब्सक्राइबर लाइन (DSL):
  - यह एक लोकप्रिय ब्रॉडबैंड कनेक्शन है, जो कॉपर तार का उपयोग करता है।
  - यह डायल सेवा की तरह कार्य करता है, लेकिन बहुत तेज गति पर।
- ✓ केबल मोडेम:
  - इसके तहत केबल ऑपरेटर को-एक्सियल केबल के माध्यम से इंटरनेट सुविधाएं प्रदान करते हैं।
  - इसकी गति 1.5 Mbps या उससे अधिक हो सकती है।
- ✓ फाइबर ऑप्टिक्स:
  - इसमें ऑप्टिकल फाइबर के माध्यम से प्रकाश संकेतों के रूप में जानकारी को एक स्थान से दूसरे स्थान पर भेजा जाता है।

3. वायरलेस कनेक्शन
   - ✓ इसमें इंटरनेट कनेक्शन के लिए रेडियो तरंगों का उपयोग किया जाता है।
4. इंटीग्रेटेड सर्विसेज डिजिटल नेटवर्क (ISDN)
   - ✓ यह डिजिटल नेटवर्क पर डेटा, आवाज़ और वीडियो के संचार की अनुमति देता है।

वायरलेस कनेक्शन (Wireless Connection)

- ➢ वायरलेस कनेक्शन एक प्रकार का ब्रॉडबैंड है, जिसमें इंटरनेट सुविधाएं रेडियो फ्रीक्वेंसी के माध्यम से तारों के बिना प्रदान की जाती हैं।
- ➢ वायरलेस कनेक्शन के विभिन्न रूप हो सकते हैं, जैसे:
- ➢ Wi-Fi (Wireless Fidelity)
- ➢ Li-Fi (Light Fidelity)
- ➢ सैटेलाइट इंटरनेट कनेक्शन

Wi-Fi (Wireless Fidelity)

- ➢ यह एक वायरलेस तकनीक है,जो रेडियो तरंगों के रूप में इंटरनेट सिग्नल का प्रसारण करती है।
- ➢ यह 2.4 GHz या 5 GHz की फ्रीक्वेंसी पर 11 मिलियन बिट्स प्रति सेकंड की उच्च गति पर कार्य करता है।
- ➢ इसकी रेंज 100 मीटर तक होती है।
- ➢ इसका उपयोग होम नेटवर्क, मोबाइल फोन, वीडियो गेम और अन्य इलेक्ट्रॉनिक उपकरणों में किया जाता है।
- ➢ कार्यप्रणाली: Wi-Fi तीन मुख्य तत्वों पर काम करता है:
  1. रेडियो तरंगें
  2. एंटीना
  3. राउटर
- ➢ रेडियो तरंगें - Wi-Fi नेटवर्किंग को संभव बनाती है।

Wi-Fi के मुख्य तत्व:

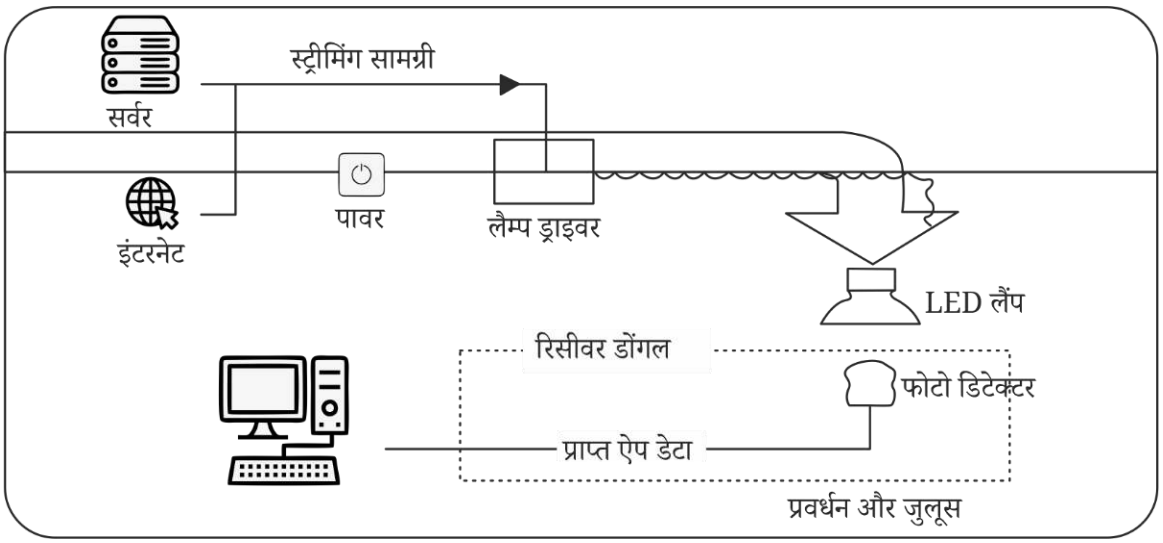
- ➢ वायरलेस एक्सेस पॉइंट:
  - ✓ वायरलेस डिवाइसों को नेटवर्क से जोड़ने की अनुमति देता है।
- ➢ Wi-Fi कार्ड्स:
  - ✓ यह वायरलेस सिग्नल और सूचना को रिले करता है (यह आंतरिक या बाहरी हो सकता है)।
  - ✓ इन्हें एडाप्टर भी कहा जाता है।
- ➢ सुरक्षा:
  - ✓ फ़ायरवॉल्स अनचाहे उपयोगकर्ताओं से नेटवर्क की सुरक्षा करते हैं और जानकारी को सुरक्षित रखते हैं।

वाई-फाई पीढ़ियाँ

पीढ़ी/IEEE मानक	अधिकतम लिंकरेट	अपनाया	आवृत्ति
Wi-Fi 6 (802.11ax)	600-9608 Mbit/s	2019	2.4/5 GHz 1-6 GHz ISM
Wi-Fi 5 (802.11ac)	433-6922 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72-600 Mbit/s	2009	2.4/5 GHz
Wi-Fi 3 (802.11g)	3-54 Mbit/s	2003	2.4 GHz
Wi-Fi 2 (802.11a)	1.5 to 54 Mbit/s	1999	5 GHz
Wi-Fi 1 (802.11b)	1 to 11 Mbit/s	1999	2.4 GHz

Li-Fi (Light Fidelity)

- यह एक तकनीक है जो डेटा और स्थिति को उपकरणों के बीच प्रसारित करने के लिए प्रकाश का उपयोग करती है।
- यह दृश्य प्रकाश, पराबैंगनी (Ultraviolet) और अवरक्त (Infrared) स्पेक्ट्रम पर उच्च गति से डेटा ट्रांसमिट करने में सक्षम है।



कार्यप्रणाली:

- एक साधारण LED बल्ब को इंटरनेट से जुड़े डिवाइस से जोड़ा जाता है।
- डिवाइस से डेटा बल्ब तक आता है और प्रकाश तरंगों द्वारा प्रसारित किया जाता है।
- यह डेटा रिसीवर या डोंगल पर गिरता है, जो कंप्यूटर से जुड़ा होता है।

इंटरनेट शब्दावली (Internet Terminology)

- वेब ब्राउज़र (Web Browser)
  - ✓ एक सॉफ्टवेयर एप्लिकेशन जो उपयोगकर्ताओं को वेबसाइट्स तक पहुंचने, नेविगेट करने और उनसे इंटरैक्ट करने में सक्षम बनाता है।
  - ✓ प्रमुख ब्राउज़र: Chrome, Firefox, Safari, Edge, और Opera
- वेब सर्वर (Web Server)
  - ✓ यह सॉफ्टवेयर या हार्डवेयर है जो वेबसाइट्स को होस्ट करता है और उपयोगकर्ताओं के ब्राउज़रों तक कंटेंट पहुंचाता है।
  - ✓ प्रमुख वेब सर्वर: Apache, Nginx, Microsoft IIS
- सर्च इंजन (Search Engine)
  - ✓ एक सॉफ्टवेयर प्रणाली जो इंटरनेट पर जानकारी खोजने के लिए डिज़ाइन की गई है।
  - ✓ प्रमुख सर्च इंजन: Google, Bing, Yahoo, और DuckDuckGo
- ई-मेल (Email)
  - ✓ एक डिजिटल संचार माध्यम है, जो संदेशों को भेजने और प्राप्त करने की अनुमति देता है।
  - ✓ प्रमुख सेवाएं: Gmail, Outlook, Yahoo Mail

सोशल नेटवर्किंग साइट्स

- यह एक इलेक्ट्रॉनिक संचार का रूप है जिसके माध्यम से उपयोगकर्ता तुरंत जानकारी, विचार, व्यक्तिगत संदेश, वीडियो और चित्र साझा कर सकते हैं। उदाहरण: Facebook, Twitter

सोशल नेटवर्किंग साइट्स के प्रकार:

- सोशल नेटवर्क्स: समान रुचियों और पृष्ठभूमि वाले लोगों से जुड़ने की सेवाएं। जैसे: Facebook और LinkedIn
- बुकमार्किंग साइट्स: इंटरनेट पर विभिन्न वेबसाइट्स और संसाधनों को संगठित और प्रबंधित करने की सेवाएं। जैसे: Delicious और StumbleUpon

- सोशल न्यूज: समाचार या लेख पोस्ट करने और उपयोगकर्ताओं द्वारा उन पर वोट करने की सेवाएं। जैसे: Digg और Reddit
- मीडिया शेयरिंग: मीडिया (जैसे: चित्र और वीडियो) अपलोड और साझा करने की सेवाएं। जैसे: YouTube, Instagram
- माइक्रोब्लॉगिंग: छोटी अपडेट्स साझा करने की सेवाएं। जैसे: Twitter

सोशल मीडिया के सकारात्मक प्रभाव

- वैश्विक संपर्क: सोशल मीडिया वैश्विक स्तर पर लोगों को जोड़ता है, संचार में बदलाव लाता है और सीमाओं के पार रिश्तों को बढ़ावा देता है।
- हाशिये पर रहने वाले लोगों की आवाज़: यह हाशिये पर रहने वाले समूहों की आवाज़ को सशक्त बनाता है, जिससे वे अपने विचार व्यक्त कर सकें और व्यापक दर्शकों तक पहुँच सकें।
- व्यापार में वृद्धि: सोशल मीडिया ऑप्टिमाइजेशन (SMO) व्यवसायों को उनके ऑनलाइन उपस्थिति को बेहतर बनाने, दृश्यता बढ़ाने और सही दर्शकों तक पहुंचने में मदद करता है।
- रोजगार के अवसर: सोशल मीडिया ने डिजिटल मार्केटिंग, कंटेंट क्रिएशन, और सोशल मीडिया प्रबंधन जैसे क्षेत्रों में नई नौकरियां पैदा की हैं।
- जानकारी और जागरूकता: यह महत्वपूर्ण जानकारी फैलाने और विभिन्न सामाजिक मुद्दों पर जागरूकता बढ़ाने में मदद करता है, जिससे वैश्विक समुदाय सशक्त बनते हैं।

सोशल मीडिया के नकारात्मक प्रभाव

- मानसिक स्वास्थ्य समस्याएँ: सोशल मीडिया का अत्यधिक उपयोग मानसिक स्वास्थ्य पर नकारात्मक प्रभाव डाल सकता है, जिससे डिप्रेशन और भावनात्मक तनाव हो सकता है।
- साइबरबुलिंग: सोशल मीडिया प्लेटफ़ॉर्म साइबरबुलिंग जैसे हानिकारक व्यवहार को प्रोत्साहित कर सकते हैं, जिससे व्यक्तियों की भलाई प्रभावित होती है।
- फेक न्यूज़ और घृणा फैलाना: सोशल मीडिया गलत जानकारी और घृणा फैलाने वाले भाषण के तेजी से प्रसार में प्रमुख भूमिका निभाता है, जो सार्वजनिक राय को प्रभावित करता है।
- प्राइवेसी की चिंताएँ: सोशल मीडिया प्लेटफॉर्म अक्सर पर्याप्त गोपनीयता उपायों की कमी के कारण उपयोगकर्ता डेटा को जोखिम में डालते हैं।
- साइबर अपराधों में वृद्धि: सोशल मीडिया प्लेटफॉर्म की कमजोरियों के कारण हैकिंग और फ़िशिंग जैसे साइबर अपराधों का जोखिम बढ़ गया है।
- कानूनी और नियामक चुनौतियाँ: फेक न्यूज़, गोपनीयता, और सामग्री हटाने जैसे मुद्दों पर विभिन्न देशों में अलग-अलग कानूनों के कारण सोशल मीडिया को नियमन से संबंधित चुनौतियों का सामना करना पड़ता है।

साइबर सुरक्षा

साइबर स्पेस (Cyber Space)

- साइबर स्पेस एक वर्चुअल वातावरण है, जहाँ कंप्यूटर नेटवर्क, इंटरनेट और अन्य डिजिटल सिस्टम के माध्यम से संचार, डेटा का आदान-प्रदान और सूचना प्रसंस्करण होता है।
- यह सभी जुड़े हुए डिजिटल सिस्टम और नेटवर्क को समाहित करता है, जो उपयोगकर्ताओं को वैश्विक स्तर पर बातचीत करने की अनुमति देता है। उदाहरण: इंटरनेट।

साइबर अपराध (Cybercrime)

- साइबर अपराध से तात्पर्य उन आपराधिक गतिविधियों से है, जिनमें कंप्यूटर, नेटवर्क, या इंटरनेट का उपयोग होता है।
- इसमें हैकिंग, पहचान की चोरी, ऑनलाइन धोखाधड़ी, साइबरबुलिंग और डेटा उल्लंघन जैसी गतिविधियाँ शामिल होती हैं।

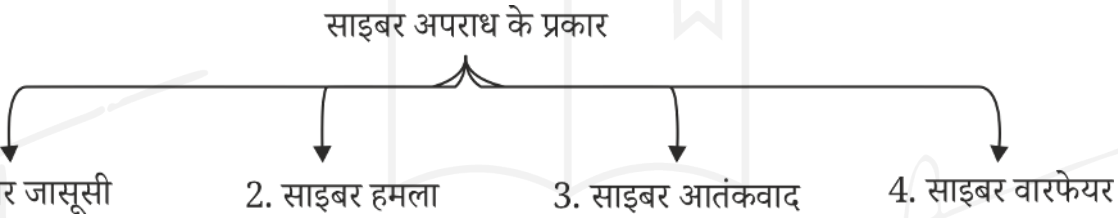
साइबर सुरक्षा (Cybersecurity)

- साइबर सुरक्षा का अर्थ उन प्रथाओं, प्रौद्योगिकियों और प्रक्रियाओं से है, जो कंप्यूटर, नेटवर्क और डेटा को अनधिकृत पहुँच, हमलों, या क्षति से सुरक्षित रखने के लिए डिज़ाइन किए गए हैं।
- इसका उद्देश्य साइबर खतरों जैसे वायरस, हैकर्स और अन्य दुर्भावनापूर्ण गतिविधियों से सिस्टम को सुरक्षित रखना है।

साइबर सुरक्षा की विशेषताएँ

- अनुपालन (Compliance): डेटा गोपनीयता की रक्षा के लिए GDPR और HIPAA जैसे कानूनी, नियामक और उद्योग मानकों का पालन सुनिश्चित करता है।
- आंतरिक खतरों के खिलाफ सुरक्षा (Defense Against Internal Threats): उपयोगकर्ता पहुँच को नियंत्रित करने और गतिविधियों की निगरानी के माध्यम से आंतरिक खतरों, जैसे अंदरूनी हमलों, से सुरक्षा प्रदान करता है।
- खतरों की रोकथाम (Threat Prevention): फ़ायरवॉल, एन्क्रिप्शन, एंटीवायरस सॉफ़्टवेयर और सिस्टम अपडेट का उपयोग करके साइबर खतरों का पता लगाना और उन्हें रोकना।
- डेटा की अखंडता (Data Integrity): डेटा को सटीक, विश्वसनीय और अछूता बनाए रखना, यहाँ तक कि प्रसारण के दौरान भी।
- घटनाओं पर प्रतिक्रिया (Incident Response): साइबर हमलों से होने वाले नुकसान और डाउनटाइम को कम करने के लिए एक संरचित दृष्टिकोण के माध्यम से प्रतिक्रिया देना और पुनर्प्राप्ति करना।
- जोखिम प्रबंधन (Risk Management): नेटवर्क और सिस्टम की अखंडता बनाए रखने के लिए साइबर सुरक्षा जोखिमों की पहचान, मूल्यांकन और उन्हें कम करना।
- निरंतर निगरानी (Continuous Monitoring): संभावित सुरक्षा उल्लंघनों या कमजोरियों का वास्तविक समय में पता लगाने के लिए सिस्टम की सतत निगरानी।

साइबर अपराधों के प्रकार:



- साइबर जासूसी (Cyber Espionage): साइबर जासूसी में डिजिटल उपकरणों और तकनीकों का उपयोग करके गोपनीय डेटा या खुफिया जानकारी तक बिना अनुमति पहुंचने की कोशिश की जाती है। इसका उपयोग राजनीतिक, सैन्य या आर्थिक लाभ के लिए किया जाता है।
- साइबर हमला (Cyber Attack): साइबर हमला वह आक्रामक कार्रवाई है, जिसमें किसी कंप्यूटर सिस्टम या नेटवर्क की कार्यक्षमता, अखंडता, या गोपनीयता को नुकसान पहुंचाने की कोशिश की जाती है। इसमें हैकिंग, डिनायल ऑफ सर्विस (DoS) अटैक या डेटा चोरी शामिल हो सकते हैं।
- साइबर आतंकवाद (Cyber Terrorism): साइबर आतंकवाद डिजिटल प्लेटफ़ॉर्म और उपकरणों का उपयोग करके ऐसे हमले करता है, जिनसे समाज में डर पैदा हो, महत्वपूर्ण ढांचे को नुकसान पहुंचे, या पारंपरिक आतंकवाद जैसा असर हो।
- साइबर युद्ध (Cyber Warfare): साइबर युद्ध राज्य-प्रायोजित या बड़े पैमाने पर साइबर हमलों को संदर्भित करता है। इसका उद्देश्य किसी देश के महत्वपूर्ण ढांचे, सैन्य प्रणालियों या अन्य प्रमुख परिसंपत्तियों को नुकसान पहुंचाना, संचालन में बाधा डालना, या संघर्ष के दौरान रणनीतिक लाभ प्राप्त करना है।

साइबर अपराध के उपकरण (Tools of Cyber Crime):

- हैकिंग (Hacking): हैकिंग का मतलब किसी कंप्यूटर सिस्टम, नेटवर्क, या डिजिटल डिवाइस तक बिना अनुमति पहुंच प्राप्त करना है। इसका उपयोग डेटा चुराने, बदलने या नियंत्रित करने के लिए किया जा सकता है।

हैकर्स के प्रकार (Types of Hackers):

- ब्लैक हैट (Black Hat): यह हैकर्स सुरक्षा कमजोरियों का दुरुपयोग करते हैं और डेटा चोरी, मैलवेयर बनाना, या सिस्टम को नुकसान पहुंचाने जैसे कार्य करते हैं।

- व्हाइट हैट (White Hat): इन्हें नैतिक हैकर कहा जाता है। ये सिस्टम की सुरक्षा कमजोरियों की पहचान कर उन्हें ठीक करने के लिए काम करते हैं और संगठनों की मदद करते हैं।
- ग्रे हैट (Grey Hat): ये हैकर्स ब्लैक और व्हाइट हैट के बीच आते हैं। ये बिना अनुमति सिस्टम में घुसपैठ करते हैं, लेकिन आमतौर पर इरादा बुरा नहीं होता है। वे सुरक्षा खामियों की रिपोर्ट कर सकते हैं या निजी लाभ के लिए उनका उपयोग कर सकते हैं।
- स्क्रिप्ट किडी (Script Kiddie): ये अनुभवहीन हैकर्स होते हैं, जो दूसरों द्वारा बनाए गए प्री-लिखित स्क्रिप्ट या टूल्स का उपयोग करते हैं। ये अपनी कोडिंग बनाने में सक्षम नहीं होते।
- हैक्टिविस्ट (Hacktivist): ये राजनीतिक या सामाजिक कारणों को बढ़ावा देने के लिए हैकिंग करते हैं। अक्सर सरकारी वेबसाइट्स या कॉरपोरेशन्स को निशाना बनाते हैं।
- रेड हैट (Red Hat): ये ब्लैक हैट हैकर्स को निशाना बनाते हैं और उनके काम को बाधित करते हैं। आक्रामक रणनीति अपनाते हैं, जैसे कि डिनायल ऑफ सर्विस अटैक।
- ब्लू हैट (Blue Hat): इन्हें संगठनों द्वारा सिस्टम की सुरक्षा जांचने के लिए नियुक्त किया जाता है। इनकी ट्रेनिंग व्हाइट हैट्स जितनी औपचारिक नहीं होती।
- फ्रीकर (Phreaker): ये हैकर्स दूरसंचार प्रणालियों को हैक करने में विशेषज्ञ होते हैं। शुल्क चुकाने से बचने या फोन नेटवर्क तक अनधिकृत पहुंच पाने के लिए तकनीकों का उपयोग करते हैं।

हैकिंग शब्दावली (Hacking Glossary):

- एडवेयर (Adware): ऐसा सॉफ़्टवेयर जो स्क्रीन पर पहले से चुने गए विज्ञापन दिखाने के लिए डिज़ाइन किया गया है।
- अटैक (Attack): सिस्टम पर किया गया वह कार्य जिससे उस पर अनधिकृत रूप से पहुँच प्राप्त कर संवेदनशील डेटा निकाला जा सके।
- बैकडोर (Backdoor): यह एक छिपा हुआ रास्ता है जो कंप्यूटर डिवाइस या सॉफ़्टवेयर में सुरक्षा उपायों को बाईपास कर अनधिकृत प्रवेश की अनुमति देता है।
- बॉट (Bot): यह एक प्रोग्राम है जो किसी क्रिया को बार-बार तेज़ी से और बिना त्रुटि के करता है, जैसे HTTP, FTP अनुरोध भेजना।
- बॉटनेट (Botnet): इसे ज़ॉम्बी आर्मी भी कहा जाता है। यह कंप्यूटरों का एक समूह है जिसका उपयोग मालिक की जानकारी के बिना किया जाता है। इसका उपयोग स्पैम भेजने या डिनायल ऑफ सर्विस (DoS) अटैक के लिए किया जाता है।
- ब्रूट फोर्स अटैक (Brute Force Attack): यह एक स्वचालित प्रक्रिया है जिसमें उपयोगकर्ता नाम और पासवर्ड के विभिन्न संयोजनों को तब तक आज़माया जाता है जब तक सही संयोजन नहीं मिल जाता।
- बफ़र ओवरफ़्लो (Buffer Overflow): यह तब होता है जब मेमोरी ब्लॉक (बफ़र) में आवंटित स्थान से अधिक डेटा लिखने की कोशिश की जाती है।
- क्लोन फ़िशिंग (Clone Phishing): वैध ईमेल का एक ऐसा रूपांतर जिसमें फ़र्जी लिंक जोड़कर उपयोगकर्ता से व्यक्तिगत जानकारी प्राप्त करने का प्रयास किया जाता है।
- डिनायल ऑफ सर्विस अटैक (DoS): यह एक दुर्भावनापूर्ण प्रयास है जिसमें सर्वर या नेटवर्क संसाधनों को अस्थायी रूप से अनुपलब्ध कर दिया जाता है।
- डीडीओएस (DDoS): डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस अटैक।
- फ़ायरवॉल (Firewall): यह एक प्रकार का फ़िल्टर है जो अवांछित घुसपैठियों को आपके सिस्टम या नेटवर्क से बाहर रखता है।
- कीस्ट्रोक लॉगिंग (Keystroke Logging): इसमें उपयोगकर्ता द्वारा दबाए गए कीज़ को ट्रैक किया जाता है। यह लॉगिन आईडी और पासवर्ड रिकॉर्ड करने के लिए उपयोग किया जाता है।
- लॉजिक बम (Logic Bomb): यह एक वायरस है जो सिस्टम में छिपा होता है और विशेष परिस्थितियों के मिलने पर सक्रिय होता है।

- मैलवेयर (Malware): इसमें कंप्यूटर वायरस, वर्म्स, ट्रोजन हॉर्स, रैनसमवेयर, स्पायवेयर, आदि सभी प्रकार के हानिकारक सॉफ़्टवेयर शामिल होते हैं।
- मास्टर प्रोग्राम (Master Program): यह प्रोग्राम ब्लैक हैट हैकर्स द्वारा संक्रमित कंप्यूटरों को सक्रिय करने और स्पैम या DoS अटैक करने के लिए उपयोग किया जाता है।
- फ़िशिंग (Phishing): ईमेल धोखाधड़ी की वह विधि जिसमें वैध दिखने वाले ईमेल भेजे जाते हैं ताकि प्राप्तकर्ताओं की व्यक्तिगत और वित्तीय जानकारी चुराई जा सके।
- फ्रीकर (Phreaker): ये हैकर्स टेलीफोन नेटवर्क को हैक करके मुफ्त लंबी दूरी की कॉल करते हैं या अन्य लोगों की कॉल को टैप करते हैं।
- रूटकिट (Rootkit): यह एक प्रकार का छिपा हुआ सॉफ़्टवेयर है जो सामान्य सुरक्षा सॉफ़्टवेयर द्वारा पहचान में नहीं आता और अपना काम करता रहता है।
- श्रिंक रैप कोड (Shrink Wrap Code): यह एक अटैक है जो अप्रचलित और गलत तरीके से कॉन्फ़िगर किए गए सॉफ़्टवेयर की खामियों का फायदा उठाता है।
- सोशल इंजीनियरिंग (Social Engineering): लोगों को जानबूझकर गुमराह करना ताकि वे अपनी व्यक्तिगत जानकारी, जैसे क्रेडिट कार्ड विवरण, पासवर्ड आदि साझा कर दें।
- स्पैम (Spam): अनचाहा ईमेल, जिसे उपयोगकर्ताओं की सहमति के बिना बड़ी संख्या में भेजा जाता है।
- स्पूफिंग (Spoofing): यह एक तकनीक है जिसमें घुसपैठिया कंप्यूटर को भरोसेमंद होस्ट से संदेश भेजने का धोखा देता है।
- स्पायवेयर (Spyware): ऐसा सॉफ़्टवेयर जो उपयोगकर्ता की जानकारी को गुप्त रूप से एकत्र करता है।
- एसक्यूएल इंजेक्शन (SQL Injection): यह एक तकनीक है जिसमें डेटा-ड्रिवेन एप्लिकेशन पर हमला करने के लिए हानिकारक SQL कोड का उपयोग किया जाता है।
- थ्रेट (Threat): एक संभावित खतरा जो सिस्टम की खामियों का फायदा उठाकर उसे कमजोर बना सकता है।
- ट्रोजन (Trojan): यह एक प्रकार का हानिकारक प्रोग्राम है जो वैध प्रोग्राम जैसा दिखता है लेकिन इसका उद्देश्य डेटा चोरी या नुकसान पहुँचाना होता है।
- वल्नरेबिलिटी (Vulnerability): यह एक कमजोरी है जो सिस्टम या नेटवर्क की सुरक्षा से समझौता करने की अनुमति देती है।
- वर्म (Worm): यह एक आत्म-प्रतिकृति वाला वायरस है जो फ़ाइलों को बदल सकता है और सक्रिय मेमोरी में लगातार खुद को डुप्लिकेट करता रहता है।
- क्रॉस साइट स्क्रिप्टिंग (XSS): यह एक वेब सुरक्षा खामी है जिसमें हमलावर उपयोगकर्ता द्वारा देखे जाने वाले वेब पेज में क्लाइंट-साइड स्क्रिप्ट को इंजेक्ट करते हैं।
- ज़ॉम्बी ड्रोन (Zombie Drone): हाईजैक किए गए कंप्यूटर जो गुमनाम रूप से स्पैम ईमेल भेजने या अन्य दुर्भावनापूर्ण गतिविधियों के लिए उपयोग किए जाते हैं।

कंप्यूटर वायरस

- VIRUS का फुल फॉर्म "Vital Information Resources Under Siege" होता है।
- वायरस छोटे-छोटे प्रोग्राम होते हैं जो कंप्यूटर में प्रवेश कर उसकी कार्य प्रणाली को प्रभावित करते हैं। इन्हें स्वचालित रूप से सक्रिय होने वाले प्रोग्राम कहा जाता है।
- वायरस एक दुर्भावनापूर्ण प्रोग्राम होता है, जिसका उद्देश्य कंप्यूटर की जानकारी को नष्ट करना होता है।
- यह प्रोग्राम जानबूझकर लिखे जाते हैं और कंप्यूटर के बूट सेक्टर से जुड़ जाते हैं। कंप्यूटर जितनी बार बूट होता है, वायरस उतनी ही तेजी से फैलता है।
- वायरस हार्ड डिस्क की स्पीड को धीमा कर देता है और कभी-कभी प्रोग्राम्स को चलने से भी रोक सकता है।
- कई वायरस लंबे समय बाद डेटा और प्रोग्राम को नुकसान पहुंचा सकते हैं।

- वायरस किसी प्रोग्राम के साथ जुड़े रहते हैं और तब तक सक्रिय नहीं होते जब तक वह प्रोग्राम नहीं चलाया जाता।
- एक बार सक्रिय होने पर वायरस कंप्यूटर की मेमोरी से जुड़कर फैलने लगते हैं।
- कंप्यूटर वायरस एक प्रकार का इलेक्ट्रॉनिक कोड है, जिसका उपयोग कंप्यूटर में संग्रहीत जानकारी को नष्ट करने के लिए किया जाता है।
- "वायरस" शब्द का पहली बार उपयोग फ्रेड कोहेन ने कैलिफोर्निया विश्वविद्यालय में अपने शोध पत्र में किया था।
- वायरस टेलीफोन लाइन के माध्यम से कंप्यूटर प्रोग्राम में दुर्भावनापूर्ण तरीके से प्रवेश कर सकता है।
- यह कोड गलत जानकारी प्रदान कर सकता है, संकलित जानकारी को नष्ट कर सकता है और यदि कंप्यूटर नेटवर्क से जुड़ा हो, तो यह पूरे नेटवर्क को प्रभावित कर सकता है।
- वायरस महीनों या वर्षों तक कंप्यूटर में बिना पता चले रह सकते हैं और नुकसान पहुंचा सकते हैं।
- प्रमुख कंप्यूटर वायरस कुछ प्रमुख कंप्यूटर वायरस इस प्रकार हैं:

(i) माइकल एंजेलो वायरस (Michelangelo):

- ✓ इसे "मार्च 6 वायरस" भी कहते हैं क्योंकि यह प्रति वर्ष 6 मार्च (माइकल एंजेलो के जन्मदिन) को डेटा नष्ट करता है।

(ii) डिस्क वॉशर (Disk Washer):

- ✓ यह भारत में 1993 के अंत में पाया गया था। यह हार्ड डिस्क में मौजूद सभी डेटा को नष्ट कर देता था।

(iii) सी-ब्रेन (C-Brain):

- ✓ इसे जनवरी, 1986 में पाकिस्तानी भाइयों अमजद और बासित ने बनाया।
- ✓ इसका उद्देश्य सॉफ्टवेयर की अवैध खरीद को रोकना था। इसे दुनिया का पहला वायरस माना जाता है।

(iv) मैकमैग (McMag):

- ✓ यह वायरस केवल एप्पल मैकिंटोश कंप्यूटर को संक्रमित करता था।
- ✓ यह आपकी स्क्रीन पर "शांति का संदेश" दिखाकर खत्म होता था।
- ✓ इस वायरस का जन्मदाता रिचर्ड ब्रैंडो को माना जाता है।
- ✓ रिचर्ड मैकमैग इस पत्रिका के प्रकाशक थे और इस वायरस का नाम पत्रिका के नाम पर रखा गया था।

(v) यरूशलम (Jerusalem):

- ✓ यह वायरस 1987 में यरूशलम विश्वविद्यालय में खोजा गया।
- ✓ यह केवल शुक्रवार को सक्रिय होता था।

(vi) कोलंबस (Columbus):

- ✓ इसे "डेटा क्राइम" और "13 अक्टूबर" वायरस भी कहा जाता है।
- ✓ यह 13 अक्टूबर, 1989 को दुनियाभर के संक्रमित कंप्यूटरों में सक्रिय हुआ।
- ✓ जेरूसलम की तरह, यह भी निष्पादन योग्य फ़ाइलों को संक्रमित करता है और हार्ड डिस्क पर डेटा को नष्ट कर देता है।
- ✓ भारत में पाया गया पहला कंप्यूटर वायरस सी-ब्रेन (C-Brain) था, जो 1988 में मद्रास (चेन्नई) में पाया गया।

(vii) रैनसमवेयर (Ransomware)

- ✓ रैनसमवेयर एक ऐसा प्रोग्राम है, जो आपकी अनुमति के बिना आपके कंप्यूटर में प्रवेश कर लेता है।
- ✓ मई 2017 में यह सामने आया।
- ✓ यह आपके कंप्यूटर की सभी जानकारी को लॉक कर देता है और फिर आपको एक संदेश दिखाता है कि यदि आप 300 से 600 डॉलर बिटकॉइन में भुगतान करेंगे, तो वह लॉक खोलने की चाबी देगा।
- ✓ यदि आप भुगतान करते हैं, तो वे आपको डेटा तक पहुंच प्रदान करते हैं, लेकिन यदि आप भुगतान नहीं करते हैं, तो आपका डेटा हमेशा के लिए चला जाता है।

साइबर अपराध से बचने के उपाय

- सॉफ़्टवेयर अपडेट रखें: माइक्रोसॉफ्ट विंडोज और अन्य थर्ड-पार्टी सॉफ़्टवेयर को नियमित रूप से अपडेट करें ताकि किसी भी सुरक्षा खामी से बचा जा सके।
- अनचाही ईमेल अटैचमेंट्स न खोलें: अनचाही ईमेल में आए अटैचमेंट्स को न खोलें, क्योंकि इससे मैलवेयर आपके सिस्टम में प्रवेश कर सकता है।
- संदिग्ध लिंक पर क्लिक न करें: कभी भी ऐसे लिंक पर क्लिक न करें जो अनजान ईमेल में हों, चाहे वे किसी जान-पहचान वाले व्यक्ति के नाम से आए हों।
- एंटीवायरस सॉफ़्टवेयर का उपयोग करें: सभी सिस्टम पर एंटीवायरस सॉफ़्टवेयर इंस्टॉल और अपडेट रखें ताकि नए खतरों से सुरक्षा हो सके।
- वेब ब्राउज़र सुरक्षित रखें: वेब ब्राउज़रों की सुरक्षा सुनिश्चित करें और उनके नियंत्रण सेटिंग्स सही रखें ताकि किसी भी प्रकार के साइबर हमले से बचा जा सके।
- फिरौती (रैंसम) न दें: साइबर अपराधियों को कभी भी फिरौती न दें, क्योंकि इसका कोई भरोसा नहीं कि वे आपकी फाइलें वापस देंगे।
- साइबर धोखाधड़ी की रिपोर्ट करें: साइबर धोखाधड़ी की घटनाओं की सूचना CERT-In (कंप्यूटर इमरजेंसी रिस्पांस टीम) और स्थानीय कानून प्रवर्तन एजेंसियों को दें।

साइबर सुरक्षा से जुड़े महत्वपूर्ण शब्द और अवधारणाएं

- हैंडशेकिंग (Handshaking): यह एक प्रक्रिया है जिसमें नेटवर्क पर दो या अधिक कंप्यूटरों के बीच संचार स्थापित करने और नियंत्रित करने के लिए सूचनाओं का आदान-प्रदान किया जाता है। यह डेटा के सुरक्षित और विश्वसनीय स्थानांतरण को सुनिश्चित करता है।
- स्मार्टस्कैन (SmartScan): स्मार्टस्कैन एक सॉफ़्टवेयर है जो कंप्यूटर में वायरस का पता लगाकर उन्हें हटाने का काम करता है।
- पलाडियम (Palladium): यह माइक्रोसॉफ्ट द्वारा विकसित एक प्रणाली है जो कंप्यूटर सुरक्षा को आसान बनाती है और डेटा सुरक्षा तथा बौद्धिक संपदा (Intellectual Property) से जुड़े मुद्दों को संबोधित करती है।
- एन्क्रिप्शन (Encryption): यह डेटा को पढ़ने योग्य रूप से अनपढ़ने योग्य रूप में बदलने की प्रक्रिया है। इसे केवल अधिकृत उपयोगकर्ता ही डिक्रिप्ट कर सकते हैं। यह डेटा को सुरक्षित रखने के लिए बेहद महत्वपूर्ण है, चाहे वह ट्रांसमिशन में हो या स्टोरेज में। ब्लोफिश (Blowfish) और आरएसए (RSA) जैसे प्रमुख एन्क्रिप्शन एल्गोरिदम हैं।
- फायरवॉल (Firewall): फायरवॉल एक नेटवर्क सुरक्षा उपकरण है (सॉफ़्टवेयर या हार्डवेयर के रूप में) जो नेटवर्क ट्रैफिक की निगरानी और फ़िल्टरिंग करता है। यह सुरक्षा नीतियों के आधार पर आने-जाने वाले डेटा को नियंत्रित करता है और अनधिकृत पहुंच से बचाव करता है।
- एंटीवायरस (Antivirus): एंटीवायरस एक सॉफ़्टवेयर है जो वायरस, वर्म्स और ट्रोजन जैसे मैलवेयर का पता लगाकर उन्हें रोकने और हटाने का काम करता है। यह कंप्यूटर की फाइलों को स्कैन करता है और ज्ञात मैलवेयर सिग्नेचर से तुलना करता है। नॉर्टन (Norton), मैक्एफी (McAfee), और अवास्ट (Avast) इसके उदाहरण हैं।
- वर्चुअल कीबोर्ड (Virtual Keyboard): यह एक सॉफ़्टवेयर आधारित कीबोर्ड है जो उपयोगकर्ताओं को बिना फिजिकल कीबोर्ड के अक्षरों को दर्ज करने में मदद करता है। यह विशेष रूप से पासवर्ड और बैंकिंग जानकारी जैसी संवेदनशील जानकारी दर्ज करने में उपयोगी है, क्योंकि यह कीलॉगिंग हमलों (जहां मैलवेयर आपके कीस्ट्रोक्स रिकॉर्ड करता है) से बचाव करता है।

कृत्रिम बुद्धिमत्ता (Artificial Intelligence - AI)

- कृत्रिम बुद्धिमत्ता कंप्यूटर विज्ञान की एक शाखा है, जो ऐसी मशीनें विकसित करने पर केंद्रित है जो सोचने, समझने, सीखने और निर्णय लेने जैसी मानव जैसी बौद्धिक क्षमताओं का अनुकरण कर सकें।

पृष्ठभूमि

- 1950: एलन ट्यूरिंग द्वारा 1950 में प्रस्तावित ट्यूरिंग टेस्ट, मशीन की उस क्षमता का मूल्यांकन करता है जिसमें वह मानवीय व्यवहार जैसा प्रदर्शन कर सके। यदि एक मानव मूल्यांकनकर्ता मशीन और मानव के उत्तरों के बीच अंतर नहीं कर सकता, तो इसे मशीन की बुद्धिमत्ता का प्रमाण माना जाता है।
- 1956: वैज्ञानिक जॉन मैकार्थी ने 'कृत्रिम बुद्धिमत्ता' शब्द की परिभाषा दी। इसलिए, उन्हें कृत्रिम बुद्धिमत्ता का जनक कहा जाता है।
- 1981: जापान ने 1981 में 'फिफ्थ जनरेशन' नामक योजना शुरू की, जो AI के क्षेत्र में एक पहल थी।
  - ✓ ब्रिटेन ने 'एलवी' परियोजना और यूरोपीय संघ के देशों ने 'एस्प्रिट' कार्यक्रम शुरू किया, जो कृत्रिम बुद्धिमत्ता अनुसंधान और विकास को आगे बढ़ाने के लिए थे।
- 1983: कुछ निजी संगठनों ने मिलकर 'माइक्रो-इलेक्ट्रॉनिक्स और कंप्यूटर टेक्नोलॉजी' नामक एक संघ का गठन किया। इसका उद्देश्य कृत्रिम बुद्धिमत्ता के लिए उन्नत तकनीकों जैसे वेरी लार्ज-स्केल इंटीग्रेटेड सर्किट्स (VLSI) का विकास करना था।
- 2011: एप्पल ने AI आधारित वर्चुअल वॉयस असिस्टेंट 'सिरी' लॉन्च किया।
- 2014: अमेज़न ने 'एलेक्सा' नामक वर्चुअल वॉयस असिस्टेंट लॉन्च किया।
- 2014: माइक्रोसॉफ्ट ने 'कोरटाना' नामक वर्चुअल असिस्टेंट लॉन्च किया।
- 2016: गूगल ने AI आधारित 'गूगल असिस्टेंट' लॉन्च किया।
- 2016: हांगकांग की हेंसन रोबोटिक्स कंपनी के डेविड हेंसन ने मानव जैसे रोबोट 'सोफिया' का विकास किया।
- 2017: सैमसंग ने AI आधारित वर्चुअल वॉयस असिस्टेंट 'बिक्सबी' लॉन्च किया।
- 2022: OpenAI ने नवंबर 2022 में 'ChatGPT' लॉन्च किया। यह GPT-3 आर्किटेक्चर पर आधारित एक संवादात्मक AI मॉडल है, जो सवालों के जवाब देने, जानकारी प्रदान करने और विभिन्न विषयों पर चर्चा करने में सक्षम है।

AI के प्रकार

- प्रतिक्रियात्मक मशीनें (Reactive Machines): ये AI सिस्टम केवल वर्तमान स्थिति पर प्रतिक्रिया करते हैं। ये पिछले अनुभवों या यादों का उपयोग नहीं करते। ये केवल पहले से निर्धारित नियमों के आधार पर विशेष कार्य करते हैं।
- सीमित स्मृति (Limited Memory): ये AI सिस्टम ऐतिहासिक डेटा का उपयोग करके निर्णय लेते हैं और समय के साथ बेहतर होते हैं। ये पिछले अनुभवों से सीखते हैं और नई जानकारी के आधार पर अपने कार्यों को समायोजित करते हैं।
- मनोविज्ञान की समझ (Theory of Mind): यह भविष्य की AI अवधारणा है, जिसमें मशीनें मानव की भावनाओं, विश्वासों और इरादों को समझ सकेंगी। इससे इंसानों के साथ बेहतर संवाद और व्यवहार की भविष्यवाणी करना संभव होगा।
- आत्म-जागरूकता (Self-Awareness): यह AI का सबसे उन्नत स्तर है, जहां मशीनें सचेतन और आत्म-जागरूक होंगी। इनमें अपने अस्तित्व और परिवेश के बारे में समझ और भावनाएं होंगी।

आर्टिफिशियल इंटेलिजेंस (AI) के उपक्षेत्र

AI को कई उपक्षेत्रों में विभाजित किया जा सकता है, जैसे:

1. मशीन लर्निंग (Machine Learning)
2. डीप लर्निंग (Deep Learning)
3. नेचुरल लैंग्वेज प्रोसेसिंग (Natural Language Processing)
4. कंप्यूटर विज़न (Computer Vision)

AI के बुनियादी अवधारणाएँ

आर्टिफिशियल इंटेलिजेंस (AI)

- परिभाषा: AI कंप्यूटर विज्ञान का एक क्षेत्र है, जो ऐसी मशीनें बनाने पर केंद्रित है, जो इंसानी बुद्धिमत्ता की नकल कर सकें, जैसे कि सीखना, तर्क करना, समस्या हल करना, निर्णय लेना, और रचनात्मकता।
- कार्य: AI सिस्टम बड़े डेटा सेट से सीखते हैं, पैटर्न पहचानते हैं और समय के साथ अपने प्रदर्शन को बेहतर करते हैं। ये कार्यों को स्वचालित करते हैं और समस्याओं को कुशलता से हल करते हैं।

मशीन लर्निंग (Machine Learning - ML)

- परिभाषा: मशीन लर्निंग AI का एक उपक्षेत्र है, जो मशीनों को डेटा से सीखने में सक्षम बनाता है, बिना विशेष रूप से प्रोग्रामिंग किए।
- कार्य: मशीन लर्निंग एल्गोरिदम का उपयोग करता है, जो डेटा में पैटर्न पहचानते हैं और निर्णय लेने या भविष्यवाणी करने में मदद करते हैं। यह अधिक डेटा के साथ अपनी क्षमताओं को सुधारता है।
- प्रकार:
  - ✓ सुपरवाइज्ड लर्निंग (Supervised Learning): लेबल्ड डेटा का उपयोग कर परिणामों की भविष्यवाणी करता है।
  - ✓ अनसुपरवाइज्ड लर्निंग (Unsupervised Learning): बिना लेबल वाले डेटा का विश्लेषण करता है और छिपे हुए पैटर्न ढूंढता है।
  - ✓ सेमी-सुपरवाइज्ड लर्निंग (Semi-Supervised Learning): थोड़े लेबल वाले और अधिक अनलेबल्ड डेटा का संयोजन करता है।
  - ✓ रिइनफोर्समेंट लर्निंग (Reinforcement Learning): प्रयास और गलती से सीखता है और वांछित व्यवहारों को पुरस्कृत करता है।

डीप लर्निंग (Deep Learning)

- परिभाषा: मशीन लर्निंग का एक उपक्षेत्र है, जो कई परतों वाले न्यूरल नेटवर्क का उपयोग करता है। यह असंरचित डेटा जैसे टेक्स्ट, इमेज और ऑडियो को प्रोसेस करता है।
- कार्य: डीप लर्निंग मॉडल डेटा में महत्वपूर्ण विशेषताओं की पहचान स्वत: करते हैं और अधिक डेटा के साथ सटीकता में सुधार करते हैं।
- उदाहरण: इमेज रिकॉग्निशन सिस्टम, जो कार जैसी वस्तुओं की पहचान करते हैं।

न्यूरल नेटवर्क (Neural Networks)

- परिभाषा: मानव मस्तिष्क से प्रेरित कम्प्यूटेशनल मॉडल, जो जुड़े हुए नोड्स (न्यूरॉन्स) से मिलकर बने होते हैं।
- कार्य: डेटा को इनपुट, हिडन और आउटपुट परतों के माध्यम से प्रोसेस करता है, ताकि भविष्यवाणी या निर्णय लिया जा सके।
- उदाहरण: इमेज और स्पीच रिकॉग्निशन में उपयोग।

AI मॉडल्स

- परिभाषा: ये ऐसे प्रोग्राम होते हैं, जो डेटा पैटर्न का विश्लेषण कर AI कार्य करते हैं।
- कार्य: एल्गोरिदम का उपयोग कर इनपुट डेटा को आउटपुट में बदलते हैं, बिना विशेष प्रोग्रामिंग के।
- उदाहरण:
  - ✓ GPT-4 (टेक्स्ट जनरेशन)
  - ✓ स्टेबल डिफ्यूजन (इमेज जनरेशन)

नेचुरल लैंग्वेज प्रोसेसिंग (NLP)

- परिभाषा: NLP मशीनों को मानव भाषा को समझने और उत्पन्न करने में सक्षम बनाता है।
- कार्य: टेक्स्ट और स्पीच का विश्लेषण करता है, पैटर्न की पहचान करता है और प्राकृतिक भाषा में उत्तर उत्पन्न करता है।
- उदाहरण: वॉयस असिस्टेंट जैसे Amazon Alexa और Google Assistant

जेनरेटिव AI (Generative AI)

- परिभाषा: बड़े डेटा सेट से पैटर्न सीखकर नई सामग्री बनाता है।
- कार्य: टेक्स्ट, इमेज, ऑडियो, और कोड उत्पन्न करता है।
- उदाहरण:
  - ✓ टेक्स्ट जेनरेटर: मानव जैसे लिखित सामग्री उत्पन्न करता है।
  - ✓ इमेज जेनरेटर: नई दृश्य सामग्री बनाता है।
  - ✓ वीडियो जेनरेटर: वीडियो क्लिप तैयार करता है।
  - ✓ ऑडियो जेनरेटर: म्यूजिक तैयार करता है या आवाज उत्पन्न करता है।
  - ✓ कोड जेनरेटर: कोड लिखता और डिबग करता है।

लार्ज लैंग्वेज मॉडल्स (LLMs)

- परिभाषा: AI मॉडल्स, जो बड़े टेक्स्ट डेटा पर प्रशिक्षित होते हैं, लिखित भाषा को समझने और उत्पन्न करने के लिए।
- कार्य: टेक्स्ट जनरेशन, अनुवाद और सारांश जैसी गतिविधियाँ गहन अध्ययन (Deep Learning) के माध्यम से करते हैं।
- उदाहरण: वह मॉडल जिनमें अरबों पैरामीटर होते हैं और जो शब्दों के बीच संबंध और संदर्भ समझते हैं।

जेनरेटिव एडवर्सेरियल नेटवर्क्स (GANs)

- परिभाषा: GANs AI मॉडल होते हैं, जो दो न्यूरल नेटवर्क (जनरेटर और डिस्क्रिमिनेटर) का उपयोग करके वास्तविक दिखने वाला डेटा उत्पन्न करते हैं।
- कार्य:
  - ✓ जनरेटर: डेटा बनाता है।
  - ✓ डिस्क्रिमिनेटर: डेटा की गुणवत्ता की जाँच करता है और इसे बेहतर बनाने में मदद करता है।
- उदाहरण: वास्तविक इमेज और डीपफेक वीडियो बनाने में उपयोग।

मल्टीमॉडल AI

- परिभाषा: ऐसा AI, जो एक साथ विभिन्न प्रकार के डेटा (जैसे टेक्स्ट, इमेज और ऑडियो) को प्रोसेस करता है।
- कार्य: विभिन्न डेटा प्रकारों को एकीकृत करके बेहतर संदर्भ और समझ प्रदान करता है।
- उदाहरण: ऐसी प्रणाली, जो दृश्य और टेक्स्ट जानकारी को मिलाकर बेहतर परिणाम देती है।

AI के वास्तविक जीवन में उपयोग

1. स्वास्थ्य क्षेत्र (Healthcare)
   - मेडिकल डायग्नोसिस: IBM Watson जैसे AI सिस्टम मेडिकल डेटा का विश्लेषण करके बीमारियों का निदान करते हैं।
   - व्यक्तिगत उपचार: AI एल्गोरिदम मरीजों के डेटा का अध्ययन करके उनके लिए व्यक्तिगत उपचार योजना तैयार करते हैं। (उदाहरण: Tempus)
   - ड्रग डिस्कवरी: AI दवाओं के निर्माण की प्रक्रिया को तेज करता है और यौगिकों की प्रभावशीलता का पूर्वानुमान लगाता है। (उदाहरण: Atomwise)
2. वित्त (Finance)
   - धोखाधड़ी पहचान: AI लेनदेन की निगरानी करके धोखाधड़ी की गतिविधियों को पकड़ता है। (उदाहरण: Mastercard's Decision Intelligence)
   - एल्गोरिदमिक ट्रेडिंग: AI बाजार विश्लेषण के आधार पर सही समय पर ट्रेड करता है। (उदाहरण: Renaissance Technologies)
   - ग्राहक सेवा: AI चैटबॉट्स ग्राहकों की पूछताछ का उत्तर देते हैं। (उदाहरण: Bank of America की Erica)
3. खुदरा क्षेत्र (Retail)
   - व्यक्तिगत सिफारिशें: AI उपयोगकर्ता के व्यवहार के आधार पर उत्पादों की सिफारिश करता है। (उदाहरण: Amazon की सिफारिश प्रणाली)
   - इन्वेंटरी प्रबंधन: AI मांग का पूर्वानुमान लगाकर स्टॉक को प्रबंधित करता है। (उदाहरण: Walmart)
   - ग्राहक डेटा विश्लेषण: AI ग्राहक डेटा का विश्लेषण करके लक्षित मार्केटिंग करता है। (उदाहरण: H&M)

4. परिवहन (Transportation)

- स्वायत्त वाहन: AI कारों और ट्रकों को चलाता है, जिससे सुरक्षा और दक्षता बढ़ती है। (उदाहरण: Tesla Autopilot)
- रूट ऑप्टिमाइज़ेशन: AI डिलीवरी और राइड-शेयरिंग के लिए कुशल मार्ग सुझाता है। (उदाहरण: Uber की नेविगेशन प्रणाली)
- पूर्वानुमानित रखरखाव: AI वाहनों की निगरानी करके रखरखाव की ज़रूरतों का पूर्वानुमान लगाता है। (उदाहरण: Rolls-Royce के एयरक्राफ्ट इंजन मॉनिटरिंग)

5. निर्माण (Manufacturing)

- पूर्वानुमानित रखरखाव: AI उपकरणों की निगरानी करता है और उनकी विफलता की संभावना का पूर्वानुमान लगाता है। (उदाहरण: Siemens)
- गुणवत्ता नियंत्रण: AI उत्पादों में दोष की जाँच करता है। (उदाहरण: FANUC के AI-समर्थित रोबोट्स)
- सप्लाई चेन ऑप्टिमाइजेशन: AI लॉजिस्टिक्स और सप्लाई चेन संचालन को कुशल बनाता है। (उदाहरण: DHL)

6. ग्राहक सेवा (Customer Service)

- चैटबॉट्स: AI चैटबॉट्स 24/7 ग्राहक सहायता प्रदान करते हैं। (उदाहरण: Zendesk का Answer Bot)
- भावना विश्लेषण (Sentiment Analysis): AI ग्राहक की प्रतिक्रिया का विश्लेषण करके सेवाओं में सुधार करता है। (उदाहरण: Sprinklr)
- वर्चुअल असिस्टेंट: AI असिस्टेंट नियुक्तियों की बुकिंग जैसी गतिविधियों में मदद करते हैं। (उदाहरण: Apple का Siri)

7. ऊर्जा क्षेत्र (Energy)

- स्मार्ट ग्रिड: AI ऊर्जा वितरण और खपत को अनुकूलित करता है। (उदाहरण: GE का Predix)
- नवीकरणीय ऊर्जा प्रबंधन: AI मौसम का पूर्वानुमान लगाकर सौर और पवन ऊर्जा का प्रबंधन करता है। (उदाहरण: Google का DeepMind)
- ऊर्जा दक्षता: AI इमारतों में ऊर्जा उपयोग को कुशल बनाता है। (उदाहरण: Siemens का बिल्डिंग ऑटोमेशन सिस्टम)

8. मनोरंजन (Entertainment)

- सामग्री निर्माण: AI संगीत, कला और लेखन उत्पन्न करता है। (उदाहरण: OpenAI का MuseNet)
- सिफारिश प्रणाली: AI उपयोगकर्ताओं की देखने की आदतों के आधार पर फ़िल्में और शो सुझाता है। (उदाहरण: Netflix)
- इंटरैक्टिव गेम्स: AI गेमिंग अनुभव को उत्तरदायी और अनुकूल बनाता है। (उदाहरण: EA का FIFA गेम्स)

9. शिक्षा (Education)

- व्यक्तिगत शिक्षण: AI छात्रों के लिए शैक्षिक सामग्री को उनकी आवश्यकता के अनुसार तैयार करता है। (उदाहरण: Knewton)
- ग्रेडिंग और मूल्यांकन: AI ग्रेडिंग को स्वचालित करता है और फीडबैक प्रदान करता है। (उदाहरण: Gradescope)
- वर्चुअल ट्यूटर: AI ऑन-डिमांड ट्यूटरिंग और सहायता प्रदान करता है। (उदाहरण: Carnegie Learning का MATHia)

10. कृषि (Agriculture)

- सटीक खेती (Precision Farming): AI डेटा का विश्लेषण करके फसल उत्पादन को बेहतर बनाता है। (उदाहरण: John Deere)
- स्वचालित फसल कटाई: AI-संचालित रोबोट्स फसलों की कुशलतापूर्वक कटाई करते हैं। (उदाहरण: Harvest CROO Robotics)
- कीट नियंत्रण: AI खेतों की निगरानी करके कीटों का पता लगाता है और उनका प्रबंधन करता है। (उदाहरण: PEAT का Plantix ऐप)

AI से जुड़ी चुनौतियाँ

AI में पक्षपात (Bias in AI)

- डेटा पक्षपात (Data Bias): AI सिस्टम अपने प्रशिक्षण डेटा में मौजूद पक्षपात को दोहरा सकते हैं, जिससे अनुचित परिणाम मिलते हैं। उदाहरण: फेशियल रिकग्निशन सिस्टम गहरे रंग की त्वचा वाले व्यक्तियों पर सही तरीके से काम नहीं करते, क्योंकि उनका प्रशिक्षण डेटा पक्षपाती हो सकता है।
- एल्गोरिदम पक्षपात (Algorithm Bias): एल्गोरिदम कुछ विशेषताओं को प्राथमिकता दे सकते हैं, जिससे परिणाम असंतुलित हो जाते हैं। उदाहरण: प्रेडिक्टिव पुलिसिंग एल्गोरिदम अल्पसंख्यक समुदायों को अधिक निशाना बना सकते हैं।
- मानव पक्षपात (Human Bias): डिजाइनर और उपयोगकर्ता अपने व्यक्तिगत पक्षपात AI सिस्टम में शामिल कर सकते हैं, जिससे निष्पक्षता और सटीकता प्रभावित होती है।

गोपनीयता की चिंताएँ (Privacy Concerns)

- AI सिस्टम को बड़ी मात्रा में डेटा की आवश्यकता होती है, जिससे गोपनीयता संबंधी समस्याएँ उत्पन्न होती हैं। उदाहरण: वर्चुअल असिस्टेंट जैसे Alexa और Google Home व्यक्तिगत डेटा एकत्र करते हैं, जो डेटा चोरी और दुरुपयोग के खतरे में आ सकता है।

सुरक्षा जोखिम (Security Risks)

- AI साइबर हमलों का शिकार हो सकता है या इसका उपयोग साइबर अपराधों के लिए किया जा सकता है।
- स्वायत्त सिस्टम (Autonomous Systems) जैसे सेल्फ-ड्राइविंग कारें हैकिंग के प्रति संवेदनशील हैं।
- AI-जनित सामग्री, जैसे डीपफेक, का उपयोग गलत सूचना फैलाने के लिए किया जा सकता है।

पारदर्शिता की कमी (Lack of Transparency)

- कई AI सिस्टम, विशेषकर डीप लर्निंग आधारित मॉडल, "ब्लैक बॉक्स" जैसे होते हैं, जिनकी निर्णय प्रक्रिया स्पष्ट नहीं होती।
- यह विश्वास की कमी और त्रुटियों या पक्षपात का पता लगाने में कठिनाई उत्पन्न करता है।

रोजगार का संकट (Job Displacement)

- AI और ऑटोमेशन दोहराए जाने वाले कार्यों वाले रोजगार को प्रभावित कर सकते हैं।
- हालांकि AI नए रोजगार के अवसर पैदा कर सकता है, लेकिन कई श्रमिकों के लिए नई तकनीकों के अनुसार खुद को ढालना मुश्किल हो सकता है, जिससे आर्थिक और सामाजिक समस्याएँ उत्पन्न होती हैं।

नैतिक दुविधाएँ (Ethical Dilemmas)

- AI कई नैतिक समस्याएँ खड़ी करता है, जैसे:
  - ✓ स्वायत्त हथियार (Autonomous Weapons) जीवन और मृत्यु से जुड़े फैसले ले सकते हैं।
  - ✓ निगरानी AI (Surveillance AI) गोपनीयता का उल्लंघन कर सकता है।
- AI के लाभों और नैतिक पहलुओं के बीच संतुलन बनाना जरूरी है।

विनियमन और कानूनी मुद्दे (Regulation and Legal Issues)

- AI का विकास नियमों और कानूनी ढाँचे से तेज हो रहा है, जिससे जिम्मेदारी और बौद्धिक संपदा (Intellectual Property) जैसे मुद्दों पर अनिश्चितता है। उदाहरण: यदि स्वायत्त वाहन दुर्घटना करता है, तो यह स्पष्ट नहीं है कि जिम्मेदार कौन होगा।

विस्तार और सामान्यीकरण (Scalability and Generalization)

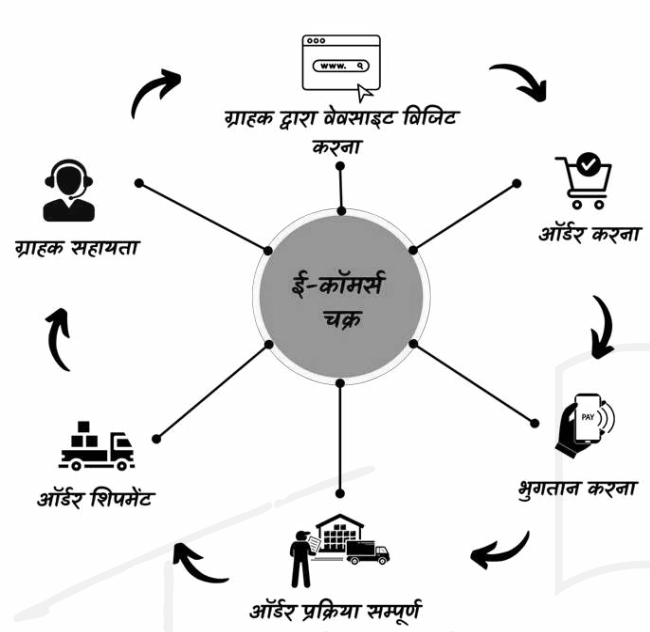
- AI सिस्टम अक्सर एक कार्य से दूसरे कार्य में सामान्यीकरण करने में असमर्थ होते हैं। उदाहरण: एक शतरंज के लिए प्रशिक्षित AI आसानी से अन्य खेलों में उपयोग नहीं किया जा सकता, जब तक उसे फिर से प्रशिक्षित न किया जाए।

ऊर्जा खपत (Energy Consumption)

- बड़े AI मॉडल्स को प्रशिक्षण देने और चलाने के लिए भारी कंप्यूटिंग संसाधनों की आवश्यकता होती है, जिससे ऊर्जा की खपत बढ़ती है।
- इसका पर्यावरण पर नकारात्मक प्रभाव पड़ता है।

मानव और AI के बीच संवाद (Human-AI Interaction)

- AI सिस्टम और मनुष्यों के बीच प्रभावी और सहज संवाद सुनिश्चित करना जरूरी है।
- खराब डिज़ाइन वाले इंटरफेस गलतफहमी और त्रुटियों का कारण बन सकते हैं, खासकर स्वास्थ्य जैसे महत्वपूर्ण क्षेत्रों में।



ई-कॉमर्स

व्यापार में खरीद और बिक्री के साथ-साथ परिवहन, बीमा, बैंकिंग, संचार जैसी संबंधित सेवाएं शामिल होती हैं। जब इन सभी गतिविधियों में सूचना और संचार तकनीक का उपयोग किया जाता है, तो इसे इलेक्ट्रॉनिक कॉमर्स या ई-कॉमर्स कहा जाता है।

ई-कॉमर्स मॉडल

1. B2B (व्यवसाय से व्यवसाय):
   - इसमें लेन-देन उत्पादक और आपूर्तिकर्ता के बीच या उत्पादक और थोक व्यापारी या थोक व्यापारी और खुदरा व्यापारी के बीच होता है। दोनों पक्ष व्यवसायिक इकाइयाँ होती हैं।
   - उदाहरण: अमेज़न, अलीबाबा, फ्लिपकार्ट आदि।
2. B2C (व्यवसाय से उपभोक्ता):
   - जैसा कि नाम से पता चलता है, इसमें एक तरफ व्यवसाय (उत्पादक या खुदरा विक्रेता) और दूसरी तरफ उपभोक्ता होते हैं। इसमें प्रचार, ऑर्डर प्राप्त करना, सप्लाई की जानकारी देना आदि जैसी विपणन गतिविधियाँ शामिल होती हैं।
   - उदाहरण: उपभोक्ता फ्लिपकार्ट, अमेज़न से सीधे सामान खरीदते हैं।
3. C2C (उपभोक्ता से उपभोक्ता):
   - इसमें उन वस्तुओं का लेन-देन होता है जिनका मौजूदा बाजार नहीं होता, जैसे पुराने/इस्तेमाल किए गए सामान (पुरानी किताबें, घरेलू उपकरण)।
   - उदाहरण: OLX
4. C2B (उपभोक्ता से व्यवसाय):
   - इसमें लेन-देन उपभोक्ता और व्यवसायी के बीच होता है।
   - उपभोक्ता अपना प्रोजेक्ट/कार्य तय बजट के साथ ऑनलाइन भेजता है और कुछ ही घंटों में कंपनियाँ उसकी आवश्यकताओं को देखकर अपनी बोलियां (bids /प्रस्ताव) भेजती हैं।
   - उदाहरण: Google AdSense, Shutterstock आदि।
5. B2A (व्यवसाय से प्रशासन):
   - इसमें कंपनी और सार्वजनिक प्रशासन/सरकार के बीच ऑनलाइन माध्यम से लेन-देन होता है।
   - उदाहरण: सॉफ़्टवेयर विक्रेता और सरकारी विभाग।
6. C2A (उपभोक्ता से प्रशासन):
   - इसमें उपभोक्ता और सरकार के बीच किए गए सभी इलेक्ट्रॉनिक लेन-देन शामिल होते हैं, जैसे करों का भुगतान, स्वास्थ्य सेवाओं का भुगतान, दूरस्थ शिक्षा प्राप्त करना आदि।
7. M- कॉमर्स (मोबाइल कॉमर्स):
   - इसमें स्मार्टफोन की मदद से उत्पाद और सेवाएँ खरीदी और बेची जाती हैं।