Notes on Information and Communication Technology and Computing

वायरलेस संचार की विभिन्न पीढ़ियाँ

वायरलेस टेलीफोन की **शुरुआत 0G (शून्य पीढ़ी) प्रणाली से हुई,** जो द्वितीय विश्व युद्ध के बाद उपलब्ध हुई। मोबाइल टेलीफोन आमतौर पर कारों या ट्रकों में लगाए जाते थे, ब्रीफकेस मॉडल भी बनाए जाते थे। 0G सिस्टम में उपयोग की जाने वाली प्रौद्योगिकियों में MTS (मोबाइल टेलीफोन सिस्टम), बेहतर मोबाइल टेलीफोन सेवा, उन्नत मोबाइल टेलीफोन सिस्टम आदि शामिल हैं।

पीढ़ियाँ	विवरण	लाभ	कमियां
1G	1979 में, दुनिया का पहला सेलुलर सिस्टम जापान के **टोक्यो में निप्पॉन टेलीफोन एंड टेलीग्राफ** (एनटीटी) द्वारा चालू किया गया। पहली पीढ़ी के मोबाइल सिस्टम ने भाषण सेवाओं के लिए एनालॉग ट्रांसमिशन का उपयोग किया। कुछ ही वर्षों में, सेलुलर संचार दुनिया के अन्य हिस्सों में भी फैल गया - 1981 में यूरोप और 1982 में संयुक्त राज्य अमेरिका तक पहुंच गया।	एकाधिक सेल साइटों का उपयोग। कॉल को एक साइट से दूसरी साइट पर स्थानांतरित करने की क्षमता। एक देश में वॉयस कॉल की अनुमति।	आवाज़ में खराबी। ख़राब बैटरी लाइफ। फोन का साइज काफी बड़ा था। कोई सुरक्षा नहीं। क्षमता सीमित थी। ख़राब हैंडऑफ़ विश्वसनीयता।
2G	मोबाइल दूरसंचार की दूसरी पीढ़ी **1991 में फिनलैंड में** शुरू की गई थी। यह GSM (ग्रुप स्पेशल मोबाइल) मानक पर आधारित था। यह टेक्स्ट मैसेजिंग (SMS - लघु संदेश सेवा), फ़ोटो या चित्रों का स्थानांतरण (MMS- मल्टीमीडिया मैसेजिंग सेवा) जैसे डेटा ट्रांसमिशन को सक्षम बनाता है, लेकिन वीडियो को नहीं। इस तकनीक में 2.5G और 2.75G शामिल हैं। 2.5G का मतलब "दूसरी और आधी	टेक्स्ट संदेश, छवि संदेश, SMS और MMS सभी संभव हैं। सिग्नल डिजिटल रूप से एन्कोड किए गए हैं, जिससे भाषण की गुणवत्ता बढ़ जाती है और लाइन का शोर कम हो जाता है। बेहतर स्पेक्ट्रम दक्षता, बेहतर सुरक्षा, बेहतर गुणवत्ता और क्षमता। आवाज और डेटा सेवा। फ़्रेमवर्क कैप बढ़ा दी गई है,	वीडियो जैसे जटिल डेटा को संभालने में असमर्थ। मजबूत डिजिटल सिग्नल की आवश्यकता है।

	पीढ़ी" है। यह एक 2जी-सिस्टम है जिसने **जनरल पैकेट रेडियो सर्विस** (GPRS) लागू किया है। 2.75G को "GSM इवोल्यूशन के लिए उन्नत डेटा दर" भी कहा जाता है। यह डेटा और सूचना के स्पष्ट और तेज़ प्रसारण में मदद करता है।	साथ ही नेटवर्क कवरेज भी।	
3G	तीसरी पीढ़ी पहली बार **2000 के दशक की शुरुआत में** जारी की गई थी। 3G प्रौद्योगिकियां नेटवर्क ऑपरेटरों को उपयोगकर्ताओं को अधिक उन्नत सेवाओं की एक विस्तृत श्रृंखला प्रदान करने में सक्षम बनाती हैं। सेवाओं में मोबाइल परिवेश में विस्तृत क्षेत्र वायरलेस वॉयस टेलीफोनी, वीडियो कॉल और ब्रॉडबैंड वायरलेस डेटा शामिल हैं। इस तकनीक में 3.5G और 3.75G शामिल हैं। **3.5G को हाई-स्पीड डाउनलिंक पैकेट एक्सेस** भी कहा जाता है। यह 3G नेटवर्क के लिए एक सहज विकासवादी मार्ग प्रदान करता है जो उच्च डेटा स्थानांतरण गति की अनुमति देता है। 3.75G को **हाई स्पीड अपलिंक पैकेट एक्सेस** (HSUPA) भी कहा जाता है। यह 3rd G नेटवर्क का उन्नत रूप है जिसमें **हाई स्पीड पैकेट एक्सेस प्लस** (HSPA+) शामिल है।	स्ट्रीमिंग ऑडियो और वीडियो में सुधार किया गया है। कई गुना तेज डेटा ट्रांसमिशन। 3Mbps तक की स्पीड दे सकता है। वीडियो और फोटोग्राफी जैसे मल्टीमीडिया एप्लिकेशन समर्थित हैं। उच्च गति, वेब WAP ब्राउज़िंग और अधिक सुरक्षा। बड़ी क्षमता वाला ब्रॉडबैंड। ग्लोबल पोजिशनिंग सिस्टम, मोबाइल टेलीविजन, फोन कॉल और लाइव वीडियो कॉन्फ्रेंसिंग मूल्य वर्धित सेवाओं के उदाहरण हैं।	महँगा। उच्च बैंडविड्थ की आवश्यकता। महंगे 3G फ़ोन। सेलफोन का आकार बड़ा था।
4G	4G वायरलेस सिस्टम व्यापक क्षेत्र कवरेज और उच्च थ्रूपुट वाला एक पैकेट स्विच्ड वायरलेस सिस्टम है। इसे लागत प्रभावी बनाने और उच्च वर्णक्रमीय दक्षता प्रदान करने के लिए डिज़ाइन किया गया है। 4G वायरलेस ऑर्थोगोनल फ्रीक्वेंसी	उच्च गति, अधिक सुरक्षा, उच्च क्षमता। इंटरनेट, स्ट्रीमिंग मीडिया और वीडियो कॉन्फ्रेंसिंग तक आसानी से पहुंच। असाधारण वर्णक्रमीय दक्षता।	अधिक बैटरी का उपयोग करता है। लागू करना कठिन। महँगे उपकरण की आवश्यकता है।

	डिवीजन मल्टीप्लेक्सिंग (OFDM), अल्ट्रा वाइड रेडियो बैंड (UWB) और मिलीमीटर वायरलेस की तकनीक का उपयोग करता है। 4G का तात्पर्य ऑल-आईपी पैकेट-स्विच्ड नेटवर्क, मोबाइल अल्ट्रा-ब्रॉडबैंड (गीगाबिट स्पीड) एक्सेस और मल्टी-कैरियर ट्रांसमिशन से है। **"मैजिक"** शब्द 4G वायरलेस तकनीक को भी संदर्भित करता है जो मोबाइल मल्टीमीडिया, कहीं भी, वैश्विक गतिशीलता समर्थन, एकीकृत वायरलेस समाधान और अनुकूलित सेवाओं के लिए है।	किसी भी समय और किसी भी स्थान पर उपयोगकर्ताओं को किसी भी प्रकार की सेवा प्रदान करना। सेवा की उच्च गुणवत्ता और प्रति बिट कम लागत।	
5G	5वीं पीढ़ी के वायरलेस सिस्टम में, ग्राहकों को अल्ट्रा-फास्ट इंटरनेट और मल्टीमीडिया अनुभवों से लाभ मिलता है। 5G तकनीक उच्च डेटा दर प्राप्त करने के लिए मिलीमीटर तरंगों और बिना लाइसेंस वाले स्पेक्ट्रम का उपयोग करके डेटा प्रसारित करती है। 5G प्रदर्शन का लक्ष्य उच्च डेटा दर, कम विलंबता, ऊर्जा बचत, लागत में कमी, उच्च सिस्टम क्षमता और बड़े पैमाने पर डिवाइस कनेक्टिविटी है। 5G में मशीन से मशीन संचार संभव हो सकता है। यह स्मार्ट होम और स्मार्ट सिटी, कनेक्टेड कारों आदि के लिए इंटरनेट ऑफ थिंग्स (IoT) का कार्य करता है।	पिछली पीढ़ियों की तुलना में डेटा ट्रांसमिशन तेज़ है। 5G तकनीक द्वारा वैश्विक कनेक्टिविटी और सेवा पोर्टेबिलिटी प्रदान की जाती है। गीगाबिट तक व्यापक प्रसारण बैंडविड्थ, लगभग 75,000 एक साथ कनेक्शन का समर्थन करता है। बड़ी फ़ोन मेमोरी, त्वरित डायलिंग, और ऑडियो/वीडियो स्पष्टता। एक उच्च गति, उच्च क्षमता वाली प्रणाली जो Gbps पर बड़े पैमाने पर डेटा प्रसारण की अनुमति देती है।	रुकावटें कनेक्टिविटी को प्रभावित कर सकती हैं। गैजेट बैटरियों का कमजोर होना। साइबर सुरक्षा। एन्क्रिप्शन का अभाव। अपलोड गति डाउनलोड गति से मेल नहीं खाती।

दृश्य प्रकाश संचार (Visible Light Communication-VLC)

- VLC एक वायरलेस तकनीक है जो **ऑप्टिकल इंटेंसिटी मॉड्यूलेशन पर निर्भर** करती है और संभावित रूप से इंटरनेट-ऑफ-थिंग्स (IoT) कनेक्टिविटी के लिए गेम चेंजर है।
- यह दृश्य प्रकाश के साथ डेटा के उच्च गति संचरण को सक्षम बनाता है। यह डेटा किसी प्रकाश स्रोत द्वारा छोड़े गए प्रकाश की तीव्रता को संशोधित करके प्रसारित किया जाता है।
- इसकी उच्च बैंडविड्थ और विद्युत चुम्बकीय स्रोतों से हस्तक्षेप के प्रति प्रतिरक्षा के कारण यह एक पसंदीदा संचार तकनीक है।
- VLC संचार के लिए 380 nm से 750 nm (यानी 430 THz से 790 THz) के बीच तरंग दैर्ध्य का उपयोग करता है।

VLC सिस्टम

- एक VLC प्रणाली दो भागों से बनी होती है: **ट्रांसमीटर और रिसीवर।**
- तीव्र प्रकाश मॉड्यूलेशन के माध्यम से एक LED लाइट (ट्रांसमीटर) से उत्सर्जित प्रकाश एक प्राप्तकर्ता डिवाइस द्वारा प्राप्त किया जाता है, जिसे बाद में प्रयोग करने योग्य डेटा में अनुवादित किया जाता है।
- फिर इसे तीन परतों में विभाजित किया जा सकता है:
    - **भौतिक परत,** जो मूल रूप से उपकरण और माध्यम के बीच संबंध को निर्धारित करती है,
    - **MAC परत,** जो प्राप्त और संसाधित डेटा को उस दिशा में इंगित करती है जिसमें उन्हें जाने की आवश्यकता होती है, और
    - **अनुप्रयोग परत।**

VLC के अनुप्रयोग

लाई-फाई

- लाई-फाई या **'लाइट फिडेलिटी'** एक **वायरलेस ऑप्टिकल नेटवर्किंग** तकनीक है जो वायरलेस तरीके से उपकरणों के बीच डेटा संचार और संचारित करने के लिए LED लाइट का उपयोग करती है।
- यह Wi-Fi के समान है, जो संचार के लिए रेडियो फ्रीक्वेंसी का उपयोग करता है।
- **LED लाइटें वायरलेस नेटवर्क का आधार** बनती हैं जबकि Li-Fi इन LED लाइटों की तीव्रता को संशोधित करके डेटा के प्रसारण को सक्षम बनाता है।
- एक फोटो सेंसर मॉड्यूलेटेड प्रकाश प्राप्त करता है जिसे बाद में इलेक्ट्रॉनिक रूप में डिमॉड्यूलेट किया जाता है।

वाहन से वाहन संचार

- वाहन रोशनी और मौजूदा ट्रैफिक लाइट बुनियादी ढांचे की उपस्थिति के कारण VLC का उपयोग वाहन संचार के लिए किया जा सकता है।
- वाहन सुरक्षा संचार परियोजना द्वारा संकेतित उच्च प्राथमिकता वाले अनुप्रयोगों में सहकारी फॉरवर्ड टकराव चेतावनी, पूर्व-दुर्घटना संवेदन, आपातकालीन इलेक्ट्रॉनिक ब्रेक लाइट, लेन परिवर्तन चेतावनी, स्टॉप साइन मूवमेंट सहायक, बाएं मोड़ सहायक, यातायात सिग्नल उल्लंघन चेतावनी और वक्र गति चेतावनी शामिल हैं।

पानी के अंदर संचार

- अच्छी कंडक्टिविटी के कारण RF तरंगें समुद्री जल में अच्छी तरह से नहीं चलती हैं। इसलिए, VLC संचार का उपयोग पानी के भीतर संचार नेटवर्क में किया जाना चाहिए।
- अन टेथर्ड रिमोटली ऑपरेटेड व्हीकल (UTROV) पानी के भीतर संचार में VLC का एक और अनुप्रयोग है।
- UTROV का उपयोग करके जो विभिन्न कार्य किए जा सकते हैं उनमें महासागरों का वेधशाला रखरखाव और जहाजों से तैनाती के अवसर शामिल हैं।

सूचना प्रदर्शित करने वाले साइनबोर्ड

- साइनबोर्ड अक्सर LED की एक श्रृंखला से बनाए जाते हैं जो बदले में हवाई अड्डों, बस स्टॉप और अन्य स्थानों पर जानकारी देने के लिए संशोधित होते हैं जहां डेटा का प्रसारण आवश्यक होता है।

स्वास्थ्य सेवा उद्योग

- वाई-फ़ाई का उपयोग चुम्बकीय अनुनाद इमेजिंग जैसे चिकित्सा उपकरणों और यहां तक कि रोगियों के उपचार में भी हस्तक्षेप कर सकता है।
- दूसरी ओर, लाई-फाई एक व्यवहार्य अवसर प्रदान करता है जहां दृश्य प्रकाश संचार ऐसे विद्युतचुंबकीय व्यवधान (EMI-Electromagnetic Interference) संवेदनशील वातावरण में डेटा ट्रांसफर को सक्षम कर सकता है। यह रोबोटिक उपचार और लैप्रोस्कोपी में भी सहायता कर सकता है।

बिजली संयंत्र और अन्य संवेदनशील क्षेत्र

- पावर प्लांट जैसे संवेदनशील क्षेत्रों को ग्रिड-अखंडता और मांग की निगरानी के लिए तेज़ डिजिटल संचार की आवश्यकता है। इसके बजाय, परमाणु ऊर्जा संयंत्रों को मुख्य तापमान की निगरानी करने और इसे शीघ्रता से भेजने की आवश्यकता है।
- वाई-फाई अपने विकिरण के कारण संवेदनशील क्षेत्रों को नकारात्मक रूप से प्रभावित कर सकता है; हालाँकि, ऐसे क्षेत्रों में लाई-फाई का कार्यान्वयन एक सुरक्षित और तेज़ उपाय प्रदान कर सकता है।

शैक्षणिक संस्थान

- कई कारणों से विश्वविद्यालयों और स्कूलों को निर्बाध इंटरनेट पहुंच की आवश्यकता है।
- LED लाइटें स्थापित करके, विश्वविद्यालय और स्कूल न केवल ऊर्जा लागत बचा सकते हैं बल्कि हाई-स्पीड इंटरनेट एक्सेस भी प्रदान कर सकते हैं। शैक्षणिक संस्थानों में लाई-फाई पूरी तरह से वाई-फाई की जगह ले सकता है।

मनोरंजन और विज्ञापन उद्योग

- एक एकल LED लाइट का उपयोग ट्रांसमिशन और रिसेप्शन के साथ-साथ बच्चों के मनोरंजन के लिए दृश्य प्रदान करने के लिए किया जा सकता है।
- VLC का एक अन्य उपयोग विज्ञापन उद्योग में हो सकता है, जहां विज्ञापन के लिए LED से बने बड़े बिलबोर्ड का उपयोग किया जाता है।

VLC संचार के लाभ

- **बड़े बैंडविड्थ का समर्थन करता है:** इसलिए RF संचार की बैंडविड्थ कमियों को दूर करता है।
- **सुरक्षित संचार:** VLC आधारित डेटा संचार को दूसरे कमरे से कोई भी बाधित नहीं कर सकता है। यह RF संचार के विपरीत सुरक्षित संचार प्रदान करता है।

- **ऊर्जा कुशल:** VLC स्रोत का उपयोग रोशनी और संचार दोनों के लिए किया जाता है, इसमें बिजली की खपत कम होती है।
- **EM विकिरण:** प्रकाश आधारित संचार है, इसलिए, RF प्रणालियों से EM विकिरण के कारण प्रभावित नहीं होता है।
- **स्वास्थ्य और स्थापना:** इससे मनुष्यों के स्वास्थ्य को कोई खतरा नहीं है और इसे स्थापित करना आसान है।

VLC संचार के नुकसान

- अन्य परिवेशीय प्रकाश स्रोतों से हस्तक्षेप की समस्याएँ।
- छोटा कवरेज रेंज का समर्थन।
- WiFi प्रणाली के साथ एकीकरण करने की चुनौतियाँ।
- अन्य कमियों में वायुमंडलीय अवशोषण, छायांकन, किरण फैलाव आदि शामिल हैं।

वेब के प्रकार

- **वेब 1.0:** यह डायल-अप इंटरनेट के शुरुआती दिनों को संदर्भित करता है जब वेबसाइटें और वेब पेज स्थिर थे, और उनका प्राथमिक उद्देश्य जानकारी साझा करना था।
- **वेब 2.0:** इसमें सोशल मीडिया प्लेटफ़ॉर्म, ब्लॉग, विकी और इंटरनेट पर वितरित अन्य यूजर-जेनरेटेड कंटेंट प्लेटफ़ॉर्म शामिल हैं।
- **वेब 3.0:** इंटरनेट का एक संस्करण जो बुद्धिमान स्वचालन, संदर्भ-जागरूक अनुप्रयोगों और उन्नत गोपनीयता और सुरक्षा उपायों पर केंद्रित है।
    - यह नया तकनीकी आयाम वर्तमान ऑनलाइन पारिस्थितिकी तंत्र की समस्याओं को हल करने के लिए आर्टिफिशियल इंटेलिजेंस, मशीन लर्निंग और ब्लॉकचेन जैसी नवीनतम तकनीकों की शक्ति का लाभ उठाने में विश्वास करता है।
    - वेब 3.0 के साथ, मोबाइल फोन, डेस्कटॉप, उपकरण, वाहन और सेंसर सहित असमान और तेजी से शक्तिशाली कंप्यूटिंग संसाधनों द्वारा उत्पन्न डेटा, विकेंद्रीकृत डेटा नेटवर्क के माध्यम से उपयोगकर्ताओं द्वारा बेचा जाएगा, यह सुनिश्चित करते हुए कि उपयोगकर्ता स्वामित्व नियंत्रण बनाए रखेंगे।

ऑप्टिकल फाइबर

- ऑप्टिकल फाइबर एक डेटा ट्रांसमिशन विधि है जो एक लंबे फाइबर (जो अक्सर प्लास्टिक या कांच से बना होता है) तक यात्रा करने वाले **लाइट पल्स का उपयोग** करता है।
- फाइबर ऑप्टिक केबल में प्रकाश के पूर्ण आंतरिक परावर्तन का उपयोग किया जाता है।

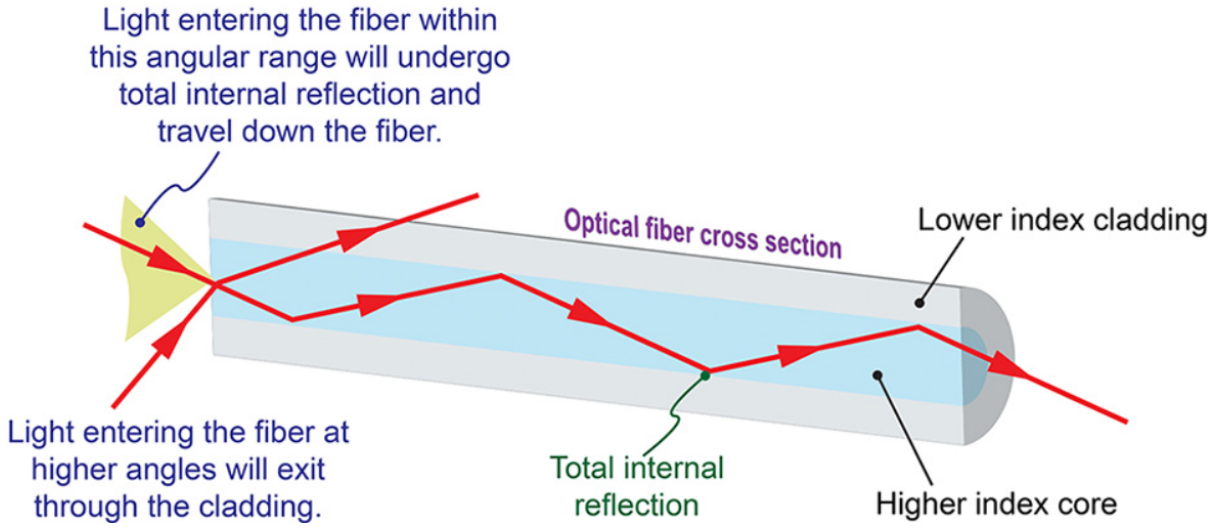

Figure.1. ऑप्टिकल फाइबर का संचालन

ऑप्टिकल फाइबर की संरचना

- कोर, क्लैडिंग और बाहरी कोटिंग सभी ऑप्टिकल फाइबर के घटक हैं। जबकि कांच और प्लास्टिक का उपयोग आमतौर पर किया जाता है, वांछित ट्रांसमिशन स्पेक्ट्रम के आधार पर विभिन्न सामग्रियों का उपयोग किया जा सकता है।
- फाइबर का वह भाग जो प्रकाश संचारित करता है, कोर कहलाता है।
- क्लैडिंग के लिए उपयोग की जाने वाली सामग्री में अक्सर कोर की तुलना में कम अपवर्तक सूचकांक होता है (आमतौर पर लगभग 1 प्रतिशत कम)।
- सूचकांक अंतर के कारण, फाइबर की लंबाई के साथ सूचकांक सीमा पर कुल आंतरिक प्रतिबिंब होता है, जो प्रकाश को साइडवॉल से बाहर निकलने से रोकता है।

ऑप्टिकल फाइबर के अनुप्रयोग

- **चिकित्सा उद्योग:** शरीर के आंतरिक अंगों को खोखले स्थानों में डालकर देखना।
- **संचार:** यह ट्रांसमिशन डेटा की गति और सटीकता को बढ़ाता है। तांबे के तारों की तुलना में, फाइबर ऑप्टिक्स केबल हल्के, अधिक लचीले होते हैं और अधिक डेटा ले जाते हैं।
- **रक्षा:** सैन्य और एयरोस्पेस अनुप्रयोगों के उच्च स्तरीय डेटा सुरक्षा क्षेत्रों में डेटा ट्रांसमिशन के लिए।
- **उद्योग:** दुर्गम स्थानों में इमेजिंग के लिए।
- **प्रसारण:** उच्च-परिभाषा टेलीविजन संकेतों को प्रसारित करने के लिए जिनमें अधिक बैंडविड्थ और गति होती है।
- **प्रकाश और सजावट:** त्योहारों या घरों में।
- **यांत्रिक निरीक्षण:** उन क्षतियों और दोषों का पता लगाने के लिए जो दुर्गम स्थानों पर हैं।

भारतनेट

- नेशनल ऑप्टिकल फाइबर नेटवर्क (NOFN) **अक्टूबर 2011 में लॉन्च** किया गया था और 2015 में इसका नाम बदलकर भारत नेट प्रोजेक्ट कर दिया गया।
- यह परियोजना एक विशेष प्रयोजन वाहन (Special Purpose Vehicle-SPV) अर्थात् भारत ब्रॉडबैंड नेटवर्क लिमिटेड द्वारा क्रियान्वित की जा रही है, जिसे 25 फरवरी, 2012 को **भारतीय कंपनी अधिनियम, 1956 के तहत 1000 करोड़ रुपये की अधिकृत पूंजी** के साथ शामिल किया गया था।
- पूरे प्रोजेक्ट को यूनिवर्सल सर्विस ऑब्लिगेशन फंड (USOF) द्वारा वित्त पोषित किया जा रहा है, जिसे देश के ग्रामीण और दूरदराज के इलाकों में दूरसंचार सेवाओं में सुधार के लिए स्थापित किया गया था।
- यह परियोजना एक **केंद्र-राज्य सहयोगी परियोजना** है, जिसमें राज्य ऑप्टिकल फाइबर नेटवर्क की स्थापना के लिए मुफ्त मार्ग का योगदान दे रहे हैं।
- ग्रामीण क्षेत्रों में विभिन्न सेवाएं शुरू करने के लिए दूरसंचार सेवा प्रदाताओं (Telecom Service Providers-TSPs), केबल टीवी ऑपरेटरों और सामग्री प्रदाताओं जैसे सभी सेवा प्रदाताओं को NOFN तक गैर-भेदभावपूर्ण पहुंच प्रदान की गई है।

भारतनेट का उद्देश्य

- देश की सभी **2,50,000 ग्राम पंचायतों को जोड़ना** और सभी ग्राम पंचायतों को **100 Mbps कनेक्टिविटी प्रदान करना।**
    - इसे प्राप्त करने के लिए, सार्वजनिक क्षेत्र के उपक्रमों (BSNL, रेलटेल और पावर ग्रिड) के मौजूदा अप्रयुक्त फाइबर (डार्क फाइबर) का उपयोग किया गया और जहां भी आवश्यक हो, ग्राम पंचायतों से जुड़ने के लिए वृद्धिशील फाइबर बिछाया गया।
- ग्रामीण भारत में ई-गवर्नेंस, ई-स्वास्थ्य, ई-शिक्षा, ई-बैंकिंग, इंटरनेट और अन्य सेवाओं की डिलीवरी की सुविधा प्रदान करना।

तीन चरण का कार्यान्वयन

- **पहला चरण:** दिसंबर 2017 तक भूमिगत ऑप्टिक फाइबर केबल (OFC) लाइनें बिछाकर एक लाख ग्राम पंचायतों को ब्रॉडबैंड कनेक्टिविटी प्रदान करना।
- **दूसरा चरण:** भूमिगत फाइबर, बिजली लाइनों पर फाइबर, रेडियो और उपग्रह मीडिया के इष्टतम मिश्रण का उपयोग करके देश की सभी ग्राम पंचायतों को कनेक्टिविटी प्रदान करना। इसे मार्च 2019 तक पूरा करना था।
- **तीसरा चरण:** 2019 से 2023 तक, अतिरेक प्रदान करने के लिए रिंग टोपोलॉजी के साथ जिलों और ब्लॉकों के बीच फाइबर सहित एक अत्याधुनिक, फ्यूचर-प्रूफ नेटवर्क बनाया जाएगा।

नया विकास

- अगस्त 2023 में केंद्रीय मंत्रिमंडल ने देश के दूरदराज के क्षेत्रों में 5G नेटवर्क उपलब्ध कराने के लिए भारतनेट के अगले चरण के लिए ₹1,39,579 करोड़ के आवंटन को मंजूरी दे दी है।
- सरकारी सूत्रों के अनुसार, वर्तमान में लगभग 1.94 लाख गाँव जुड़े हुए हैं और बाकी गाँव अगले 2.5 वर्षों में जुड़ने की उम्मीद है।

राष्ट्रीय ब्रॉडबैंड मिशन

- संचार मंत्रालय ने देश भर में, विशेषकर ग्रामीण और दूरदराज के क्षेत्रों में ब्रॉडबैंड सेवाओं तक सार्वभौमिक और न्यायसंगत पहुंच की सुविधा के लिए 17 दिसंबर, 2019 को 'राष्ट्रीय ब्रॉडबैंड मिशन' (National Broadband Mission-NBM) शुरू किया है।
- इसका लक्ष्य **2022 तक सभी गांवों तक ब्रॉडबैंड पहुंच** प्रदान करना है।
- इसमें **2024 तक** ऑप्टिकल फाइबर केबल (OFC) की **30 लाख रूट किमी की वृद्धि** और **प्रति हजार आबादी पर टावर घनत्व को 0.42 से 1 टावर तक बढ़ाना** शामिल है।

राष्ट्रीय ब्रॉडबैंड मिशन का विज़न

- डिजिटल संचार बुनियादी ढांचे के तेजी से विकास को सक्षम करने के लिए, डिजिटल सशक्तिकरण और समावेशन के लिए डिजिटल विभाजन को पाटना, सभी के लिए ब्रॉडबैंड तक सस्ती और सार्वभौमिक पहुंच प्रदान करना।

राष्ट्रीय ब्रॉडबैंड मिशन के उद्देश्य

- डिजिटल बुनियादी ढांचे और सेवाओं के विस्तार और निर्माण में तेजी लाने के लिए आवश्यक नीति और नियामक परिवर्तनों को संबोधित करना।
- पूरे देश में ऑप्टिकल फाइबर केबल और टावरों सहित डिजिटल संचार नेटवर्क और बुनियादी ढांचे का डिजिटल फाइबर मानचित्र बनाना।
- मिशन के लिए निवेश को सक्षम करने के लिए संबंधित मंत्रालयों/विभागों/एजेंसियों और वित्त मंत्रालय सहित सभी हितधारकों के साथ काम करना।
- उपग्रह मीडिया के माध्यम से देश के दूर-दराज के क्षेत्रों तक कनेक्टिविटी बढ़ाने के लिए आवश्यक पर्याप्त संसाधन उपलब्ध कराने के लिए अंतरिक्ष विभाग के साथ काम करना।
- विशेष रूप से घरेलू उद्योग द्वारा ब्रॉडबैंड के प्रसार के लिए नवीन प्रौद्योगिकियों को अपनाने को प्रोत्साहित करना और बढ़ावा देना।
- राइट ऑफ वे (RoW) के लिए नवीन कार्यान्वयन मॉडल विकसित करके संबंधित हितधारकों से सहयोग प्राप्त करना।
- OFC बिछाने के लिए आवश्यक RoW अनुमोदन सहित डिजिटल बुनियादी ढांचे के विस्तार से संबंधित सुसंगत नीतियों के लिए राज्यों/केंद्रशासित प्रदेशों के साथ काम करना।
- किसी राज्य/केंद्र शासित प्रदेश के भीतर डिजिटल संचार बुनियादी ढांचे और अनुकूल नीति पारिस्थितिकी तंत्र की उपलब्धता को मापने के लिए ब्रॉडबैंड रेडीनेस इंडेक्स (BRI) विकसित करना।
- देश भर में डिजिटल संचार बुनियादी ढांचे के विकास और डिजिटल अर्थव्यवस्था के माध्यम से प्रत्यक्ष और अप्रत्यक्ष रोजगार को बढ़ावा देना।

राष्ट्रीय ब्रॉडबैंड मिशन की प्रगति (जून 2022 तक)

- **गांवों तक ब्रॉडबैंड कनेक्टिविटी:** भारतनेट परियोजना के तहत जून 2022 तक 1,77,550 ग्राम पंचायतों को सेवा के लिए तैयार कर दिया गया है।
- **ब्रॉडबैंड स्पीड (Mbps) की उपलब्धता:** भारतीय दूरसंचार नियामक प्राधिकरण ट्राई माई स्पीड ऐप के माध्यम से विभिन्न सेवा प्रदाताओं के लिए डाउनलोड और अपलोड स्पीड के बारे में क्राउड-सोर्स डेटा प्राप्त कर रहा है। 2024-25 तक 50 Mbps तक ब्रॉडबैंड स्पीड हासिल करने की परिकल्पना की गई है।

- **फाइबराइजेशन (लाख किलोमीटर) संचयी:** जून 2022 तक कुल ऑप्टिकल फाइबर केबल लगभग 34.62 लाख किलोमीटर बिछाई गई है। इसे 2024-25 तक 50 लाख किलोमीटर तक बढ़ाने की परिकल्पना की गई है।
- **टावर (लाख में) संचयी:** जून 2022 तक 7.23 लाख टावर स्थापित किए गए हैं। 2024-25 तक इसे 15 लाख टावर तक बढ़ाने की परिकल्पना की गई है।
- **टेलीकॉम टावर्स/बेस ट्रांसीवर स्टेशन (BTS) का फाइबराइजेशन (%) संचयी:** जून 2022 तक लगभग 35.11% टेलीकॉम टावर्स/BTS को फाइबराइज्ड किया गया है। इसे 2024-25 तक 70% तक बढ़ाने की परिकल्पना की गई है।
- **फाइबर संचयी की मैपिंग:** सार्वजनिक क्षेत्र उपक्रम द्वारा बिछाए गए ऑप्टिकल फाइबर केबल के 10 लाख रूट किमी को PM गतिशक्ति NMP पोर्टल पर मैप किया गया है।

नया विकास

- सरकार ने फरवरी 2023 में ब्रॉडबैंड कनेक्टिविटी की परिभाषा को संशोधित किया है।
- केंद्र ने 2 Mbps (मेगाबिट प्रति सेकंड) की उच्चतर न्यूनतम डाउनलोड गति निर्दिष्ट की है। इससे पहले, जुलाई 2013 में दूरसंचार विभाग द्वारा अधिसूचित परिभाषा में इसे न्यूनतम डाउनलोड गति के रूप में 512 kbps (किलोबिट प्रति सेकंड) निर्धारित किया गया था।
- जून, 2023 तक, भारत में लगभग 861.47 मिलियन ब्रॉडबैंड ग्राहक थे।
- जून 2023 के अंत में शीर्ष पांच सेवा प्रदाताओं की कुल ब्रॉडबैंड ग्राहकों में 98.37 प्रतिशत बाजार हिस्सेदारी थी।
- भारत के शीर्ष-5 सेवा प्रदाता हैं- रिलायंस जियो इन्फोकॉम लिमिटेड (447.75 मिलियन), भारती एयरटेल (248.06 मिलियन), वोडाफोन आइडिया (124.90 मिलियन), बीएसएनएल (24.59 मिलियन) और एट्रिया कन्वर्जेंस (2.16 मिलियन)।

क्लाउड कंप्यूटिंग

- क्लाउड कंप्यूटिंग तेज़ नवाचार, लचीले संसाधनों और पैमाने की अर्थव्यवस्थाओं की पेशकश करने के लिए इंटरनेट ("क्लाउड") पर सर्वर, स्टोरेज, डेटाबेस, नेटवर्किंग, सॉफ्टवेयर, एनालिटिक्स और इंटेलिजेंस सहित कंप्यूटिंग सेवाओं की डिलीवरी है।
- फ़ाइलों को हार्ड ड्राइव या स्थानीय स्टोरेज डिवाइस पर रखने के बजाय, क्लाउड-आधारित स्टोरेज उन्हें दूरस्थ डेटाबेस में सहेजना संभव बनाता है।
- जब तक किसी इलेक्ट्रॉनिक उपकरण की वेब तक पहुंच है, तब तक उसे डेटा और उसे चलाने के लिए सॉफ़्टवेयर प्रोग्राम तक पहुंच प्राप्त है।

क्लाउड कंप्यूटिंग का संचालन

क्लाउड कंप्यूटिंग की मुख्य विशेषताएं इस प्रकार हैं:

- **ऑन-डिमांड:** कंप्यूटिंग सेवाएं आम तौर पर मिनट या घंटे के हिसाब से मांग पर बेची जाती हैं।
- **इलास्टिक:** एक उपयोगकर्ता किसी भी समय जितनी चाहे उतनी या कम सेवा प्राप्त कर सकता है।
- **पूरी तरह से प्रदाता द्वारा प्रबंधित:** उपभोक्ता को एक पर्सनल कंप्यूटर और इंटरनेट कनेक्शन के अलावा कुछ भी नहीं चाहिए।
- **डेटा-सघन:** गणना के बजाय डेटा पर ध्यान केंद्रित किया गया है।
- **मापनीयता:** क्लाउड कंप्यूटिंग में उपयोगकर्ता की जरूरतों को पूरा करने के लिए स्केल-अप या स्केल-डाउन करने की क्षमता होती है।

क्लाउड कंप्यूटिंग के प्रकार

सार्वजनिक क्लाउड

- सार्वजनिक क्लाउड का स्वामित्व और संचालन **तृतीय-पक्ष क्लाउड सेवा प्रदाताओं द्वारा** किया जाता है, जो इंटरनेट पर सर्वर और स्टोरेज जैसे कंप्यूटिंग संसाधन वितरित करते हैं। उदाहरणों में एमेजॉन वेब सर्विसेज, माइक्रोसॉफ्ट एज्यूर आदि शामिल हैं।

निजी क्लाउड

- निजी क्लाउड से तात्पर्य **किसी एकल व्यवसाय या संगठन द्वारा** विशेष रूप से उपयोग किए जाने वाले क्लाउड कंप्यूटिंग संसाधनों से है। सेवाओं और बुनियादी ढांचे को एक निजी नेटवर्क पर बनाए रखा जाता है।
- इसे भौतिक रूप से कंपनी के ऑनसाइट डेटासेंटर पर स्थित किया जा सकता है। कुछ कंपनियाँ अपने निजी क्लाउड को होस्ट करने के लिए तृतीय-पक्ष सेवा प्रदाताओं को भी भुगतान करती हैं।

हाइब्रिड क्लाउड

- हाइब्रिड क्लाउड **सार्वजनिक और निजी क्लाउड को जोड़ते हैं,** जो प्रौद्योगिकी द्वारा एक साथ बंधे होते हैं और डेटा और अनुप्रयोगों को उनके बीच साझा करते है।
- डेटा और एप्लिकेशन को निजी और सार्वजनिक क्लाउड के बीच स्थानांतरित करने की अनुमति देकर, हाइब्रिड क्लाउड व्यवसायों को अधिक लचीलापन और अधिक तैनाती विकल्प प्रदान करता है और मौजूदा बुनियादी ढांचे, सुरक्षा और अनुपालन को अनुकूलित करने में मदद करता है।

क्लाउड कंप्यूटिंग सेवाओं के प्रकार

इन्फ्रास्ट्रक्चर एज ए सर्विस (IaaS)

- क्लाउड कंप्यूटिंग सेवाओं की सबसे बुनियादी श्रेणी।
- IaaS के साथ, एक उपयोगकर्ता क्लाउड प्रदाता से IT इंफ्रास्ट्रक्चर-सर्वर और वर्चुअल मशीन, स्टोरेज, नेटवर्क, ऑपरेटिंग सिस्टम को भुगतान के आधार पर किराए पर ले सकता है।

प्लेटफ़ॉर्म एज ए सर्विस (PaaS)

- प्लेटफ़ॉर्म एज ए सर्विस क्लाउड कंप्यूटिंग सेवाओं को संदर्भित करता है जो सॉफ़्टवेयर अनुप्रयोगों के विकास, परीक्षण, वितरण और प्रबंधन के लिए ऑन-डिमांड वातावरण प्रदान करता है।
- PaaS को डेवलपर्स के लिए जल्दी से वेब या मोबाइल ऐप बनाना आसान बनाने के लिए डिज़ाइन किया गया है। PaaS की सहायता से डेवलपर्स को विकास के लिए आवश्यक सर्वर, भंडारण, नेटवर्क और डेटाबेस के अंतर्निहित बुनियादी ढांचे की स्थापना या प्रबंधन करने की चिंता नहीं होती।

सॉफ्टवेयर एज ए सर्विस (SaaS)

- सॉफ्टवेयर एज ए सर्विस इंटरनेट पर, मांग पर और आमतौर पर सदस्यता के आधार पर सॉफ़्टवेयर एप्लिकेशन वितरित करने की एक विधि है।
- SaaS के साथ, क्लाउड प्रदाता सॉफ़्टवेयर एप्लिकेशन और अंतर्निहित बुनियादी ढांचे को होस्ट और प्रबंधित करते हैं, और सॉफ़्टवेयर अपग्रेड और सुरक्षा पैचिंग जैसे किसी भी रखरखाव को संभालते हैं।
- इसमें उपयोगकर्ता इंटरनेट पर एप्लिकेशन से जुड़ते हैं, आमतौर पर अपने फोन, टैबलेट या PC पर वेब ब्राउज़र के साथ।

सर्वर रहित कंप्यूटिंग

- PaaS के साथ ओवरलैप करते हुए, सर्वर रहित कंप्यूटिंग आवश्यक सर्वर और बुनियादी ढांचे को प्रबंधित करने में समय बर्बाद किए बिना ऐप कार्यक्षमता के निर्माण पर ध्यान केंद्रित करता है।
- क्लाउड प्रदाता सेटअप, क्षमता योजना और सर्वर प्रबंधन संभालता है।

क्लाउड कंप्यूटिंग के लाभ

- क्लाउड कंप्यूटिंग सेवाएं IT आवश्यकताओं और भौतिक भंडारण को कम करती हैं, जिससे छोटे व्यवसायों को महत्वपूर्ण व्यावसायिक लागत में कटौती करने में मदद मिलती है।
- अधिकांश क्लाउड सेवाओं का भुगतान सदस्यता के आधार पर किया जाता है, इसलिए पूंजीगत व्यय कम हो जाता है।
- क्लाउड कंप्यूटिंग बहुत तेज़ और तैनात करने में आसान है, इसलिए स्टार्ट-अप लागत कम है।
- व्यावसायिक डेटा को क्लाउड पर ले जाने से आपदा पुनर्प्राप्ति संभव हो सकती है, यानी हार्डवेयर समझौता होने की स्थिति में डेटा पुनर्प्राप्त करना संभव हो सकता है।
- कई व्यवसायों के लिए, क्लाउड पर जाने से कर्मचारियों के बीच सहयोग के अवसर बढ़ते हैं।
- यह टीम के सदस्यों को कहीं से भी काम करने की अनुमति देता है।
- क्लाउड डेटा को केंद्रीकृत करता है, जिसका अर्थ है कि मालिक, कर्मचारी और ग्राहक इंटरनेट एक्सेस के साथ किसी भी स्थान से कंपनी डेटा तक पहुंच सकते हैं।
- क्लाउड कंप्यूटिंग ऊर्जा खपत और कार्बन उत्सर्जन को 30% से अधिक कम करके कंपनी के कार्बन पदचिह्न को कम करता है।
-

कमियां

- क्लाउड-आधारित सेवाओं के लिए, लगातार इंटरनेट कनेक्शन महत्वपूर्ण है।
- जबकि क्लाउड-आधारित सर्वर के लिए अग्रिम या पूंजीगत लागत बहुत कम है, क्लाउड सर्वर को सर्वर और डेटा दोनों को बनाए रखने के लिए हर महीने एक महत्वपूर्ण राशि का भुगतान करने की आवश्यकता होती है।
- अत्यधिक संवेदनशील डेटा वाली कंपनियों को डेटा सुरक्षित रखने के लिए अपने स्वयं के IT विभाग की आवश्यकता हो सकती है क्योंकि जब डेटा क्लाउड में संग्रहीत होता है, तो कंपनी इसे सुरक्षित रखने के लिए किसी तीसरे पक्ष पर भरोसा कर रही होती है।

क्लाउड स्टोरेज

- क्लाउड स्टोरेज एक **क्लाउड कंप्यूटिंग मॉडल** है जो क्लाउड कंप्यूटिंग प्रदाता के माध्यम से इंटरनेट पर डेटा और फ़ाइलों को संग्रहीत करने में सक्षम बनाता है जिसे कोई व्यक्ति सार्वजनिक इंटरनेट या समर्पित निजी नेटवर्क कनेक्शन के माध्यम से एक्सेस कर सकता है।

क्लाउड स्टोरेज का महत्व

लागत प्रभावशीलता

- क्लाउड स्टोरेज के साथ, हार्डवेयर को खरीदने, प्रावधान करने के लिए कोई स्टोरेज, और व्यावसायिक स्पाइक्स के लिए कोई अतिरिक्त पूंजी का उपयोग करने की आवश्यक्ता नहीं है।
- कोई व्यक्ति मांग पर भंडारण क्षमता को जोड़ या हटा सकता है, प्रदर्शन और प्रतिधारण विशेषताओं को तुरंत बदल सकता है, और केवल उस भंडारण के लिए भुगतान कर सकता है जिसका वास्तव में उपयोग किया गया है।

बढ़ी हुई चपलता

- क्लाउड स्टोरेज के साथ, संसाधन केवल एक क्लिक की दूरी पर हैं। इसके परिणामस्वरूप किसी संगठन की चपलता में वृद्धि होती है।

तेज़ तैनाती

- क्लाउड स्टोरेज सेवाएं IT को जब भी और जहां भी जरूरत हो, आवश्यक स्टोरेज की सटीक मात्रा तुरंत वितरित करती है।
- एक डेवलपर स्टोरेज सिस्टम को प्रबंधित करने के बजाय जटिल एप्लिकेशन समस्याओं को हल करने पर ध्यान केंद्रित कर सकता है।

कुशल डेटा प्रबंधन

- क्लाउड स्टोरेज जीवनचक्र प्रबंधन नीतियों का उपयोग करके, उपयोगकर्ता अनुपालन आवश्यकताओं के समर्थन में स्वचालित टियरिंग या डेटा को लॉक करने सहित शक्तिशाली सूचना प्रबंधन कार्य कर सकते हैं।

वस्तुतः असीमित स्केलेबिलिटी

- क्लाउड स्टोरेज वस्तुतः असीमित भंडारण क्षमता प्रदान करता है। इससे ऑन-प्रिमाइसेस भंडारण क्षमता की बाधाएं दूर हो जाती हैं।
- उपयोगकर्ता एनालिटिक्स, डेटा लेक, बैकअप या क्लाउड नेटिव एप्लिकेशन के लिए आवश्यकतानुसार क्लाउड स्टोरेज को कुशलतापूर्वक ऊपर और नीचे कर सकते हैं।

मरम्मत और पुनर्प्राप्ति

- क्लाउड स्टोरेज सेवाओं को किसी भी खोई हुई अतिरेक का तुरंत पता लगाने और मरम्मत करके समवर्ती डिवाइस विफलता को संभालने के लिए डिज़ाइन किया गया है।
- यह अनायास उपयोगकर्ता कार्यों या एप्लिकेशन विफलताओं दोनों से अधिक आसानी से पुनर्प्राप्ति करने के लिए संस्करण और प्रतिकृति टूल का उपयोग करके डेटा की सुरक्षा कर सकता है।

कमियां

इंटरनेट पर निर्भरता

- कोई भी व्यक्ति हमेशा ऑफ़लाइन रहते हुए फ़ाइलों को सहेज सकता है और बाद में उन तक पहुंच सकता है। हालाँकि, अपडेट और सिंक के लिए इंटरनेट कनेक्शन की आवश्यकता होगी।

सुरक्षा और गोपनीयता

- क्लाउड में संग्रहीत करने के लिए गोपनीय डेटा को किसी तीसरे पक्ष के संगठन को दिया जाना चाहिए। इसलिए व्यक्ति को क्लाउड विक्रेता पर पूरा भरोसा होना चाहिए।

लागत

- क्लाउड से फ़ाइलें अपलोड करने और डाउनलोड करने के लिए अतिरिक्त लागतें हैं। यदि कोई उपयोगकर्ता बार-बार बहुत सारी फ़ाइलों तक पहुँचने का प्रयास कर रहा है तो ये लागत तेज़ी से जुड़ सकते हैं।

नियंत्रण पर कमियां

- उपयोगकर्ता द्वारा डेटा को क्लाउड पर ले जाने के बाद, विक्रेता अब इसका प्रभारी है। इसका तात्पर्य यह है कि उपयोगकर्ताओं को अपनी सेवाओं को सुरक्षित, स्थिर, चालू और पूरी तरह कार्यात्मक तरीके से बनाए रखने के लिए विक्रेताओं पर भरोसा करना चाहिए। यह डेटा सुरक्षा पर प्रभाव को सीमित करता है।

भारत में क्लाउड कंप्यूटिंग

क्लाउड कंप्यूटिंग और डेटा सेंटर

- भारत में डिजिटल आबादी का आकार और डिजिटल अर्थव्यवस्था के विकास पथ के लिए डेटा केंद्रों की मजबूत वृद्धि की आवश्यकता है।
- डेटा सेंटर एक केंद्रीकृत स्थान के भीतर एक समर्पित सुरक्षित स्थान है जहां कंप्यूटिंग और नेटवर्किंग उपकरण बड़ी मात्रा में डेटा एकत्र करने, भंडारण, प्रसंस्करण, वितरण या पहुंच की अनुमति देने के उद्देश्य से केंद्रित होते हैं।
- क्लाउड सेवा प्रदाता अंतिम उपयोगकर्ताओं को क्लाउड कंप्यूटिंग सेवाएं प्रदान करने के लिए डेटा केंद्रों में अपने IT बुनियादी ढांचे की मेजबानी करते हैं।
- केंद्रीय बजट 2022-23 में, केंद्रीय वित्त और कॉर्पोरेट मामलों के मंत्री ने प्रस्ताव दिया कि डेटा सेंटर (ऊर्जा भंडारण प्रणालियों के साथ) को बुनियादी ढांचे की सामंजस्यपूर्ण सूची में शामिल किया जाएगा।

डेटा सेंटर की आवश्यकता

- **डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023** के डेटा स्थानीयकरण प्रावधानों और तेजी से जुड़ी दुनिया में देश की डिजिटल संप्रभुता की सुरक्षा के लिए भारत में डेटा सेंटर बुनियादी ढांचे की आवश्यकता आवश्यक है।

- विभिन्न अनुमानों के अनुसार, भारत में डेटा केंद्रों के लिए **लगभग 499 मेगावाट स्थापित बिजली** क्षमता है (दिसंबर 2022 तक)।
- इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय ने 2020 में डेटा सेंटर नीति का एक मसौदा भी प्रस्तावित किया है:
    - भारत को ग्लोबल डेटा सेंटर हब बनाना,
    - क्षेत्र में निवेश को बढ़ावा देना,
    - डिजिटल अर्थव्यवस्था के विकास को बढ़ावा देना,
    - विश्वसनीय होस्टिंग अवसंरचना के प्रावधान को सक्षम करना, और
    - नागरिकों को अत्याधुनिक सेवा वितरण की सुविधा प्रदान करना।

भारत में डेटा सेंटर का विकास

डेटा सेंटर नीति 2020 के मसौदे के अनुसार, देश में डेटा सेंटर क्षेत्र के दीर्घकालिक विकास के लिए, व्यवसायों के लिए अनुकूल, प्रतिस्पर्धी और सतत परिचालन वातावरण बनाना महत्वपूर्ण है। इस दिशा में नीतिगत जोर देने वाले कुछ प्रमुख क्षेत्र शामिल हैं:

- डेटा सेंटरों के लिए निर्बाध, स्वच्छ और लागत प्रभावी बिजली की उपलब्धता डेटा सेंटर क्षेत्र के लिए सबसे महत्वपूर्ण विचारों में से एक बनी हुई है।
- मजबूत और लागत प्रभावी कनेक्टिविटी बैकहॉल की सुविधा के लिए दूरसंचार विभाग (DoT) के साथ काम करने के लिए MeitY।
- डेटा सेंटरों को "आवश्यक सेवा रखरखाव अधिनियम, 1968 (Essential Services Maintenance Act-ESMA)" के तहत एक आवश्यक सेवा घोषित किया जाएगा।
- नेशनल बिल्डिंग कोड के तहत डेटा सेंटरों को एक अलग श्रेणी के रूप में मान्यता देना।
- डेटा सेंटर आर्थिक क्षेत्रों की स्थापना।
- स्वदेशी प्रौद्योगिकी विकास, अनुसंधान और क्षमता निर्माण को बढ़ावा देना।

GI क्लाउड पहल – मेघराज

- क्लाउड कंप्यूटिंग के लाभों का उपयोग और दोहन करने के लिए, भारत सरकार ने फरवरी **2014 में** एक महत्वाकांक्षी पहल - **"GI क्लाउड" शुरू की है जिसे 'मेघराज' नाम दिया गया** है।
- यह पहल **सरकार में क्लाउड के प्रसार को सुनिश्चित करने के लिए** शासन तंत्र सहित विभिन्न घटकों को लागू करने के लिए है।
- इस पहल का फोकस सरकार के ICT खर्च को अनुकूलित करते हुए देश में ई-सेवाओं की डिलीवरी में तेजी लाना है।
- GI क्लाउड की वास्तुशिल्प दृष्टि में भारत सरकार द्वारा जारी किए गए सामान्य प्रोटोकॉल, दिशानिर्देशों और मानकों के एक सेट का पालन करते हुए, मौजूदा या नए (संवर्धित) बुनियादी ढांचे पर निर्मित, कई स्थानों पर फैले अलग-अलग क्लाउड कंप्यूटिंग वातावरण का एक सेट शामिल है।
- **राष्ट्रीय सूचना विज्ञान केंद्र** (National Informatics Centre-NIC) मेघराज पहल के तहत राष्ट्रीय क्लाउड सेवाएं प्रदान कर रहा है। दी जाने वाली सेवाएँ हैं: PaaS, IaaS, SaaS, कंटेनर एज ए सर्विस (NCCaaS), आर्टिफिशियल इंटेलिजेंस एज ए सर्विस, एप्लिकेशन प्रदर्शन प्रबंधन सेवा, संसाधन निगरानी एज ए सर्विस, आदि।

मेघराज के फायदे

- मौजूदा बुनियादी ढांचे का इष्टतम उपयोग।

- भारत में किसी भी सरकारी विभाग द्वारा उपलब्ध कराया गया कोई भी सॉफ्टवेयर बिना किसी अतिरिक्त लागत के अन्य विभागों को भी उपलब्ध कराया जा सकता है।
- यह भारत में सूचना एवं संचार प्रौद्योगिकी (Information and Communication Technology-ICT) बुनियादी ढांचे को बनाए रखने के लिए एक एकल बिंदु प्रदान करता है।
- भारत के नागरिकों की जैसी मांग होगी, सरकार उसके अनुरूप इंफ्रास्ट्रक्चर बढ़ा सकती है।
- कुशल सेवा वितरण।
- संपूर्ण GI क्लाउड के लिए एक सुरक्षा ढांचा कम पर्यावरणीय जटिलता और कम संभावित भेद्यता को जन्म देगा।
- उपयोगकर्ता की गतिशीलता में वृद्धि।
- प्रौद्योगिकी के प्रबंधन में प्रयास का कम होना।
- पहली बार IT समाधान परिनियोजन में आसानी।
- लागत में कमी।
- यह अंतरसंचालनीयता, एकीकरण, सुरक्षा, डेटा सुरक्षा और पोर्टेबिलिटी आदि के मानकों को निर्धारित करता है।

डिजिटल लॉकर

- डिजीलॉकर **डिजिटल इंडिया कार्यक्रम के** हिस्से के रूप में **इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय** (Ministry of Electronics & Information Technology-MeitY) की एक प्रमुख पहल है।
- **2015 में लॉन्च** किए गए इस कार्यक्रम का लक्ष्य सार्वजनिक क्लाउड पर एक सुरक्षित दस्तावेज़ पहुंच मंच प्रदान करते हुए भारत को पेपर रहित बनाना है।
- इसका इरादा नागरिकों को डिजिटल दस्तावेज़ वॉलेट के माध्यम से प्रामाणिक डिजिटल दस्तावेज़ों तक पहुंचने की अनुमति देकर **'डिजिटल सशक्तिकरण'** प्रदान करना है।
- डिजीलॉकर के माध्यम से संग्रहीत दस्तावेजों को साझा और सत्यापित भी किया जा सकता है।

तीन प्रमुख स्तर

- सरकार **'न्यूनतम सरकार और अधिकतम शासन'** के दर्शन के साथ डिजिटल परिवर्तन का लक्ष्य रख रही है, और इसके लिए इसने तीन प्रमुख स्तरों की पहचान की है- i) कैशलेस स्तर, ii) पेपरलेस स्तर और iii) प्रेजेंसलेस स्तर।
- डिजिटल कैशलेस ट्रांसफर के माध्यम से कैशलेस स्तर का ख्याल **भारतीय राष्ट्रीय भुगतान निगम** (National Payments Corporations of India-NPCI) द्वारा रखा जाता है।
- UIDAI द्वारा प्रेजेंसलेस स्तर हासिल की गई है।
- डिजीलॉकर द्वारा eKYC, डिजाइन और सत्यापन प्रक्रिया को संबोधित करते हुए पेपरलेस स्तर को संबोधित किया गया है।

नागरिकों को लाभ

- महत्वपूर्ण दस्तावेज़ कभी भी, कहीं भी।
- प्रामाणिक दस्तावेज़ जो कानूनी रूप से मूल के बराबर हैं।
- डिजिटल दस्तावेज़ों के आदान-प्रदान के लिए नागरिक की सहमति आवश्यक है।
- सरकारी लाभ, रोजगार, वित्तीय समावेशन, शिक्षा और स्वास्थ्य के क्षेत्रों में तेज़ सेवा वितरण।

एजेंसियों को लाभ

- **प्रशासनिक ओवरहेड में कमी:** पेपर रहित शासन का लक्ष्य। यह कागज के उपयोग को कम करके और सत्यापन प्रक्रिया को छोटा करके प्रशासनिक लागत बचाता है।

- डिजिटल परिवर्तन के हिस्से के रूप में विश्वसनीय जारी किए गए दस्तावेज़ प्रदान किए जाते हैं।
- जारी किए गए दस्तावेज़ डिजिलॉकर का उपयोग करके जारी करने वाली एजेंसी से वास्तविक समय में पुनर्प्राप्त किए जाते हैं।

डिजीलॉकर के अंतर्गत विशेष सुविधाएँ एवं उपलब्धियाँ

- नागरिकों को कुल 452 करोड़ रुपये के दस्तावेज़ उपलब्ध कराये गये हैं।
- किसी आपदा की स्थिति में डिजीलॉकर सिस्टम बेहद उपयोगी हो सकता है। केरल बाढ़ के मामले में एक सफल उदाहरण प्रदर्शित किया गया था, जिसमें IT विभाग ने बाढ़ के दौरान केरल के नागरिकों को डिजिटल प्रमाणपत्र जारी किए थे।
- विभिन्न राज्यों में छात्रों के पास स्कूल बोर्डों और उच्च शिक्षा संस्थानों से 40 करोड़ से अधिक शैक्षिक दस्तावेज़ों तक पहुंच है।
- लोगों को डिजिटल DL/RC (ड्राइविंग लाइसेंस/पंजीकरण प्रमाणपत्र) उपलब्ध कराया जाता है।

साइबर सुरक्षा

- साइबर सुरक्षा **सिस्टम, नेटवर्क और प्रोग्राम को डिजिटल हमलों से बचाने** का अभ्यास है।
- ये साइबर हमले आमतौर पर संवेदनशील जानकारी तक पहुंचने, बदलने या नष्ट करने के उद्देश्य से होते हैं; रैंसमवेयर के माध्यम से उपयोगकर्ताओं से पैसे ऐंठना; या सामान्य व्यावसायिक प्रक्रियाओं को बाधित करना भी इसका उद्देश्य हो सकता हैं।

साइबर खतरों की अवधारणा

- साइबर खतरे को कानूनी अधिकार के बिना डेटा, किसी एप्लिकेशन या संघीय प्रणाली तक पहुंच, घुसपैठ, हेरफेर या अखंडता, गोपनीयता, सुरक्षा या उपलब्धता को नुकसान पहुंचाने के लिए निर्देशित किसी भी पहचाने गए प्रयास के रूप में परिभाषित किया गया है।
- साइबर खतरा अनजाने और जानबूझकर, लक्षित या गैर-लक्षित हो सकता है। यह विभिन्न स्रोतों से आ सकता है, जिसमें जासूसी और सूचना युद्ध में लगे विदेशी राष्ट्र, अपराधी, हैकर्स, वायरस प्रोग्राम लेखक और संगठन के भीतर काम करने वाले असंतुष्ट कर्मचारी और ठेकेदार शामिल हो सकते हैं।
- अनजाने खतरे असावधान या अप्रशिक्षित कर्मचारियों, सॉफ़्टवेयर अपग्रेड, रखरखाव प्रक्रियाओं और उपकरण विफलताओं के कारण हो सकते हैं जो अनजाने में कंप्यूटर सिस्टम को बाधित करते हैं या डेटा को दूषित करते हैं।
- जानबूझकर दी गई धमकियों में लक्षित और गैर-लक्षित दोनों तरह के हमले शामिल हो सकते हैं।
    - लक्षित हमला तब होता है जब कोई समूह या व्यक्ति विशेष रूप से एक महत्वपूर्ण बुनियादी ढांचा प्रणाली पर हमला करता है।
    - एक गैर-लक्षित हमला तब होता है जब हमले का इच्छित लक्ष्य अनिश्चित होता है, जैसे कि जब कोई वायरस, वर्म या मैलवेयर बिना किसी विशिष्ट लक्ष्य के इंटरनेट पर जारी किया जाता है।
- बार-बार सबसे चिंताजनक रूप में पहचाने जाने वाला खतरा "अंदरूनी सूत्र" है - जिसमें कोई व्यक्ति वैध रूप से किसी सिस्टम या नेटवर्क तक पहुंच को अधिकृत करता है।

साइबर खतरों के प्रकार

- **डिनायल-ऑफ-सर्विस (DoS) और डिस्ट्रिब्यूटेड डिनायल-ऑफ-सर्विस (DDoS) हमले:** सेवा से इनकार करने वाला (DoS) हमला सिस्टम के संसाधनों पर हावी हो जाता है ताकि वह सेवा अनुरोधों का जवाब न दे सके। DDoS हमला भी एक सिस्टम के संसाधनों पर हमला है, लेकिन यह बड़ी संख्या में अन्य होस्ट मशीनों से लॉन्च किया जाता है जो हमलावर द्वारा नियंत्रित दुर्भाविनापूर्ण सॉफ़्टवेयर से संक्रमित होते हैं।
- **मैन-इन-द-मिडिल (MitM) हमला:** MitM हमला तब होता है जब हैकर क्लाइंट और सर्वर के संचार के बीच खुद को सम्मिलित करता है।
- **फ़िशिंग और स्पीयर फ़िशिंग हमले:** फ़िशिंग हमला एक प्रकार का ईमेल हमला है जिसमें एक हमलावर संबंधित विश्वसनीय संगठन से होने का दिखावा करके इलेक्ट्रॉनिक संचार के माध्यम से उपयोगकर्ताओं की संवेदनशील जानकारी को धोखाधड़ी से ढूंढने का प्रयास करता है। स्पीयर फ़िशिंग विशिष्ट संगठनों या व्यक्तियों को लक्षित करती है, और गोपनीय डेटा तक अनधिकृत पहुंच की तलाश करती है।

- **ड्राइव-बाय आक्रमण:** ड्राइव-बाय डाउनलोड आक्रमण मैलवेयर फैलाने का एक सामान्य तरीका है। हैकर्स असुरक्षित वेबसाइटों की तलाश करते हैं और किसी एक पेज पर HTTP या PHP कोड में एक दुर्भावनापूर्ण (malicious) स्क्रिप्ट डालते हैं। यह स्क्रिप्ट साइट पर आने वाले किसी व्यक्ति के कंप्यूटर पर सीधे मैलवेयर इंस्टॉल कर सकती है, या यह पीड़ित को हैकर्स द्वारा नियंत्रित साइट पर पुन: निर्देशित कर सकती है।
- **पासवर्ड हमला:** ब्रूट-फोर्स पासवर्ड अनुमान लगाने का अर्थ है अलग-अलग पासवर्ड आज़माकर एक यादृच्छिक दृष्टिकोण का उपयोग करना और यह उम्मीद करना कि कोई काम करेगा।
- **SQL इंजेक्शन हमला:** डेटाबेस-संचालित वेबसाइटों के साथ SQL इंजेक्शन एक आम समस्या बन गई है।
- **क्रॉस-साइट स्क्रिप्टिंग (XSS) हमला:** XSS हमले किसी वेबसाइट के डेटाबेस में दुर्भावनापूर्ण जावास्क्रिप्ट को इंजेक्ट करने के लिए तीसरे पक्ष के वेब संसाधनों का उपयोग करते हैं।
- **चोरी छुपे सुनना (eavesdropping) हमला:** यह नेटवर्क ट्रैफ़िक के अवरोधन के माध्यम से होता है। छिपकर, एक हमलावर पासवर्ड, क्रेडिट कार्ड नंबर और अन्य गोपनीय जानकारी प्राप्त कर सकता है जिसे उपयोगकर्ता नेटवर्क पर भेज सकता है।
- **मैलवेयर हमला:** मैलवेयर को अवांछित सॉफ़्टवेयर के रूप में वर्णित किया जा सकता है जो किसी सिस्टम में सहमति के बिना इंस्टॉल किया जाता है। यह खुद को वैध कोड से जोड़ सकता है और इंटरनेट पर खुद को प्रचारित या दोहरा सकता है।
- **रैनसमवेयर:** रैनसमवेयर एक प्रकार का मैलवेयर हमला है जिसमें हमलावर पीड़ित के डेटा को लॉक या एन्क्रिप्ट करता है और फिरौती का भुगतान न करने पर डेटा को प्रकाशित करने या उस तक पहुंच को ब्लॉक करने की धमकी देता है।

साइबर खतरों के स्रोत

- **बॉटनेट ऑपरेटर:** बॉटनेट ऑपरेटर हमलों को समन्वित करने और फ़िशिंग योजनाओं, स्पैम और मैलवेयर हमलों को वितरित करने के लिए समझौता किए गए, दूर से नियंत्रित सिस्टम के एक नेटवर्क या बॉटनेट का उपयोग करते हैं। इन नेटवर्कों की सेवाएँ कभी-कभी भूमिगत बाज़ारों में उपलब्ध कराई जाती हैं।
- **आपराधिक समूह:** आपराधिक समूह मौद्रिक लाभ के लिए सिस्टम पर हमला करना चाहते हैं। विशेष रूप से, संगठित आपराधिक समूह आइडेंटिटी चोरी और ऑनलाइन धोखाधड़ी करने के लिए स्पैम, फ़िशिंग और स्पाइवेयर/मैलवेयर का उपयोग करते हैं। अंतर्राष्ट्रीय कॉर्पोरेट जासूस और आपराधिक संगठन भी औद्योगिक जासूसी और बड़े पैमाने पर मौद्रिक चोरी करने और हैकर प्रतिभा को काम पर रखने या विकसित करने की अपनी क्षमता के माध्यम से खतरा पैदा करते हैं।
- **विदेशी राष्ट्र:** विदेशी ख़ुफ़िया सेवाएँ अपनी सूचना एकत्र करने और जासूसी गतिविधियों के हिस्से के रूप में साइबर उपकरणों का उपयोग करती हैं। साथ ही, कई राष्ट्र सूचना युद्ध सिद्धांत, कार्यक्रम और क्षमताओं को विकसित करने के लिए आक्रामक रूप से काम कर रहे हैं। ऐसी क्षमताएं सैन्य शक्ति का समर्थन करने वाली आपूर्ति, संचार और आर्थिक बुनियादी ढांचे को बाधित करके एक इकाई को महत्वपूर्ण और गंभीर प्रभाव डालने में सक्षम बनाती हैं।
- **हैकर्स:** हैकर्स बदला लेने, दूसरों का पीछा करने और मौद्रिक लाभ के लिए नेटवर्क ब्रेक करते हैं। जबकि अनधिकृत पहुंच प्राप्त करने के लिए पहले उचित मात्रा में कौशल या

कंप्यूटर ज्ञान की आवश्यकता होती थी, हैकर्स अब इंटरनेट से हमले की स्क्रिप्ट और प्रोटोकॉल डाउनलोड कर सकते हैं और उन्हें पीड़ित साइटों के खिलाफ लॉन्च कर सकते हैं।

- **हैक्टिविस्ट:** जो सार्वजनिक रूप से प्रवेश्य वेब पेजों या ई-मेल सर्वर पर राजनीति से प्रेरित हमले करते हैं। ये समूह और व्यक्ति राजनीतिक संदेश भेजने के लिए ई-मेल सर्वर को ओवरलोड करते हैं और वेबसाइटों को हैक करते हैं।
- **अंदरूनी सूत्र:** किसी संगठन के भीतर से काम करने वाला असंतुष्ट अंदरूनी सूत्र, कंप्यूटर अपराधों का एक प्रमुख स्रोत हो सकता है। अंदरूनी सूत्र सिस्टम को नुकसान पहुंचा सकते है या सिस्टम से डेटा चुरा सकते है। अंदरूनी खतरे में ठेकेदार कर्मी भी शामिल हैं।
- **अंतर्राष्ट्रीय कॉर्पोरेट जासूस:** अंतर्राष्ट्रीय कॉर्पोरेट जासूस आर्थिक और औद्योगिक जासूसी और बड़े पैमाने पर मौद्रिक चोरी करने और हैकर प्रतिभा को काम पर रखने या विकसित करने की अपनी क्षमता के माध्यम से खतरा पैदा करते हैं।
- **फ़िशर:** व्यक्ति, या छोटे समूह, मौद्रिक लाभ के लिए पहचान या जानकारी चुराने के प्रयास में फ़िशिंग योजनाओं को अंजाम देते हैं। फ़िशर अपने उद्देश्यों को पूरा करने के लिए स्पैम और स्पाइवेयर/मैलवेयर का भी उपयोग कर सकते हैं।
- **स्पैमर:** व्यक्ति या संगठन उत्पादों को बेचने, फ़िशिंग योजनाओं का संचालन करने, स्पाइवेयर/मैलवेयर वितरित करने, या संगठनों पर हमला करने (यानी, सेवा हमले से इनकार करने) के लिए छिपी या झूठी जानकारी के साथ अनचाहे ई-मेल वितरित करते हैं।
- **स्पाइवेयर/मैलवेयर लेखक:** दुर्भावनापूर्ण इरादे वाले व्यक्ति या संगठन स्पाइवेयर और मैलवेयर का उत्पादन और वितरण करके उपयोगकर्ताओं के खिलाफ हमले करते हैं। मेलिसा वायरस, एक्सप्लोर.ज़िप वर्म, CIH (चेरनोबिल) वायरस, निमडा वर्म, कोड रेड, स्लैमर वर्म और ब्लास्टर वर्म सहित कई विनाशकारी कंप्यूटर वायरस और वर्म फाइलों और हार्ड ड्राइव को नुकसान पहुंचाते है।
- **आतंकवादी:** आतंकवादी राष्ट्रीय सुरक्षा को खतरे में डालने, सैन्य उपकरणों से समझौता करने, अर्थव्यवस्था को बाधित करने और बड़े पैमाने पर हताहत करने के लिए महत्वपूर्ण इन्फ्रास्ट्रक्चर को नष्ट करने, घुसपैठ करने या शोषण करने के लिए साइबर हमले करते हैं।

भारत में साइबर सुरक्षा परिदृश्य

- भारत में, भारतीय व्यवसायों और सरकारी संस्थानों पर साइबर हमलों की बढ़ती संख्या के कारण हाल के वर्षों में साइबर सुरक्षा सर्वोच्च प्राथमिकता बन गई है।
- भारत में हाल के वर्षों में फ़िशिंग हमले बढ़ रहे हैं। एक उल्लेखनीय उदाहरण भारतीय रिज़र्व बैंक पर 2017 का फ़िशिंग हमला है जिसके परिणामस्वरूप $1 मिलियन से अधिक की चोरी हुई।
- भारत में मैलवेयर हमले भी आम हैं। 2016 में, WannaCry रैंसमवेयर हमले ने आंध्र प्रदेश पुलिस बल और भारत संचार निगम लिमिटेड (BSNL) सहित कई भारतीय संगठनों को प्रभावित किया।
- भारत में 2022 में 13.91 लाख साइबर सुरक्षा घटनाएं देखी गईं। संख्याएं अभी भी देश पर साइबर हमलों की पूरी तस्वीर नहीं देती हैं क्योंकि इन आंकड़ों में केवल CERT-In द्वारा रिपोर्ट की गई और ट्रैक की गई जानकारी शामिल है।

- इन चुनौतियों के बावजूद, जब साइबर सुरक्षा की बात आती है तो भारत में सकारात्मक रुझान उभर रहे हैं।
- भारत सरकार ने देश की साइबर सुरक्षा स्थिति में सुधार के लिए कई कदम उठाए हैं, जिसमें राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre-NCIIPC) की स्थापना और राष्ट्रीय साइबर समन्वय केंद्र (National Cyber Coordination Centre-NCCC) बनाना शामिल है।
- इसके अलावा, सरकार ने नागरिकों को साइबर सुरक्षा खतरों के बारे में शिक्षित करने और खुद को सुरक्षित रखने के तरीके के बारे में शिक्षित करने के लिए विभिन्न जागरूकता अभियान शुरू किए हैं।
- भारतीय साइबर स्पेस को सुरक्षित करने के लिए भारत में अनुसंधान एवं विकास, कानूनी ढांचा, सुरक्षा घटनाएं, प्रारंभिक चेतावनी और प्रतिक्रिया, सर्वोत्तम सुरक्षा नीति अनुपालन और आश्वासन, अंतर्राष्ट्रीय सहयोग और सुरक्षा प्रशिक्षण जैसे दृष्टिकोण भी अपनाए जाते हैं।

सूचना प्रौद्योगिकी (IT) अधिनियम, 2000

- 2000 का IT अधिनियम भारत की संसद द्वारा अधिनियमित किया गया था और भारतीय साइबर सुरक्षा कानून का मार्गदर्शन करने, डेटा सुरक्षा नीतियों को स्थापित करने और साइबर अपराध को नियंत्रित करने के लिए **भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम** (Indian Computer Emergency Response Team-CERT-In) **द्वारा प्रशासित** किया गया था।
- यह ई-गवर्नेंस, ई-बैंकिंग, ई-कॉमर्स और निजी क्षेत्र सहित कई अन्य की भी सुरक्षा करता है।
- हालाँकि भारत के पास कोई विशिष्ट, एकात्मक साइबर सुरक्षा कानून नहीं है, यह साइबर सुरक्षा मानकों को बढ़ावा देने के लिए IT अधिनियम और कई अन्य क्षेत्र-विशिष्ट नियमों का उपयोग करता है। यह भारत में महत्वपूर्ण सूचना बुनियादी ढांचे के लिए एक कानूनी ढांचा भी प्रदान करता है।
- इस अधिनियम को **सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के माध्यम से संशोधित** किया गया था। संशोधन लागू किए गए और महत्वपूर्ण अनुभागों के नियम अक्टूबर, 2009 में अधिसूचित किए गए थे जो राष्ट्रीय साइबर सुरक्षा की जरूरतों को संबोधित करते हैं।
- संशोधन में अन्य बातों के साथ-साथ साइबर अपराधों के नए रूपों से निपटने के लिए IT अधिनियम, 2000 में प्रावधान जोड़े गए, जैसे इलेक्ट्रॉनिक रूप में स्पष्ट यौन सामग्री को प्रचारित करना, वीडियो ताक-झांक और गोपनीयता का उल्लंघन और मध्यस्थ और ई-कॉमर्स धोखाधड़ी द्वारा डेटा का रिसाव।
- 2008 का IT अधिनियम किसी भी व्यक्ति, कंपनी या संगठन (मध्यस्थों) पर लागू होता है जो भारत में कंप्यूटर संसाधनों, कंप्यूटर नेटवर्क या अन्य सूचना प्रौद्योगिकी का उपयोग करता है।

राष्ट्रीय साइबर सुरक्षा नीति, 2013

- भारत सरकार ने 1 जुलाई 2013 को साइबर हमलों को रोकने के लिए सूचना की सुरक्षा और क्षमताओं का निर्माण करने के उद्देश्य से राष्ट्रीय साइबर सुरक्षा नीति 2013 लॉन्च की।
- इस नीति का उद्देश्य सरकारी और गैर-सरकारी संस्थाओं सहित सूचना और संचार प्रौद्योगिकी उपयोगकर्ताओं और प्रदाताओं के व्यापक स्पेक्ट्रम को पूरा करना है।
- राष्ट्रीय साइबर सुरक्षा नीति 2013 देश की भौतिक और व्यावसायिक संपत्तियों की सुरक्षा के लिए है।

राष्ट्रीय साइबर सुरक्षा नीति 2013 की मुख्य विशेषताएं

- यह नीति देश के साइबर सुरक्षा मुद्दों से निपटने के लिए व्यापक, सहयोगात्मक और सामूहिक जिम्मेदारी के लिए एक रूपरेखा तैयार करती है।
- नीति में **14 उद्देश्य** बताए गए हैं जिनमें क्षमता निर्माण, कौशल विकास और प्रशिक्षण के माध्यम से अगले पांच वर्षों में 5,00,000 मजबूत पेशेवर, कुशल कार्यबल का निर्माण शामिल है।
- नीति में ICT इन्फ्रास्ट्रक्चर के खतरों के संबंध में रणनीतिक जानकारी प्राप्त करने, प्रभावी, पूर्वानुमानित, निवारक, सक्रिय प्रतिक्रिया और पुनर्प्राप्ति कार्यों के माध्यम से प्रतिक्रिया, समाधान और संकट प्रबंधन के लिए परिदृश्य बनाने के लिए राष्ट्रीय और क्षेत्रीय स्तर पर 24×7 तंत्र बनाने की योजना है।
- यह नीति एक सुरक्षित साइबर इको-सिस्टम बनाने के लिए आठ अलग-अलग रणनीतियों की पहचान करती है, जिसमें विभिन्न उत्पादों या सेवाओं के बीच अंतरसंचालनीयता और डेटा विनिमय की सुविधा के लिए खुले मानकों को प्रोत्साहित करने के अलावा एक आश्वासन ढांचा बनाने की आवश्यकता भी शामिल है।

अन्य लक्ष्य में शामिल हैं

- व्यक्तियों, संगठनों और सरकार के लिए एक लचीला और सुरक्षित साइबरस्पेस बनाना।
- साइबर घटनाओं और साइबर खतरों को कम करने, तेजी से रोकने या प्रतिक्रिया देने के लिए रूपरेखा, क्षमताएं और भेद्यता प्रबंधन रणनीतियां बनाना।
- संगठनों को ऐसी साइबर सुरक्षा नीतियां विकसित करने के लिए प्रोत्साहित करना जो रणनीतिक लक्ष्यों, व्यावसायिक वर्कफ़्लो और सामान्य सर्वोत्तम प्रथाओं के अनुरूप हों।
- साथ ही साइबर अपराध से होने वाले नुकसान को कम करने के लिए संस्थागत संरचनाएं, प्रक्रियाएं, प्रौद्योगिकी और सहयोग बनाना।

सूचना प्रौद्योगिकी नियम

- केंद्र सरकार द्वारा फरवरी 2021 में सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 ('2021 नियम') जारी किए गए थे।
- 2021 नियम **सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 69ए(2), 79(2)(सी) और 87 के तहत** पारित किए गए हैं।
- 2021 के नियम को पहले से अधिनियमित सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश) नियम 2011 के स्थान पर लाया गया।
- 2021 नियम सोशल मीडिया के सामान्य उपयोगकर्ताओं को सशक्त बनाने और एक सुरक्षित और भरोसेमंद ऑनलाइन वातावरण के लिए सोशल मीडिया मध्यस्थों (Social Media Intermediaries-SMIs) और महत्वपूर्ण सोशल मीडिया मध्यस्थों (Significant Social Media Intermediaries-SSMI) पर दायित्व डालने के लिए नियामक ढांचे को अद्यतन करने के लिए पेश किए गए थे।
- यह सोशल मीडिया पर यौन अपराधों से महिलाओं और बच्चों की सुरक्षा पर विशेष जोर देता है।

सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) संशोधन नियम, 2023 ('2023 संशोधन')

- 6 अप्रैल, 2023 को, इलेक्ट्रॉनिक्स और आईटी मंत्रालय (Ministry of Electronics and IT-MeitY) ने आईटी नियम 2021 में संशोधन करने के लिए सूचना प्रौद्योगिकी (मध्यवर्ती

दिशानिर्देश और डिजिटल मीडिया आचार संहिता) संशोधन नियम 2023 को अधिसूचित किया।

- यह संशोधन केंद्र सरकार को केंद्र सरकार के किसी भी व्यवसाय के संबंध में "फर्जी या गलत या भ्रामक" जानकारी की पहचान करने के लिए "तथ्य जांच इकाई" नामित करने के लिए अधिकृत करता है।
- प्रारंभ में, इस संशोधन में केवल ऑनलाइन गेमिंग कंपनियों को विनियमित करने के प्रावधान शामिल थे। लेकिन बाद में MeitY ने एक नया मसौदा प्रकाशित किया जिसमें "तथ्य-जाँच शक्तियाँ" शामिल थीं।
- तथ्य जांच इकाई सरकारी अधिकारियों और मंत्रालयों के बारे में किसी भी ऑनलाइन टिप्पणी, समाचार रिपोर्ट या राय की जांच कर सकती है और फिर इसकी सेंसरशिप के लिए ऑनलाइन मध्यस्थों को सूचित कर सकती है।
- ऐसे मध्यस्थों में न केवल ऑनलाइन सोशल मीडिया कंपनियां शामिल हैं, बल्कि इंटरनेट सेवा प्रदाता और फ़ाइल होस्टिंग कंपनियां जैसे सेवा प्रदाता भी शामिल हैं।
- यदि कोई मध्यस्थ अनुपालन करने में विफल रहता है, तो उन्हें IT अधिनियम, 2000 की **धारा 79 के तहत** अपनी सुरक्षित हार्बर स्थिति खोने का जोखिम होगा।
    - सुरक्षित हार्बर प्रावधान में कहा गया है कि "एक मध्यस्थ उसके द्वारा उपलब्ध या होस्ट की गई किसी भी तीसरे पक्ष की जानकारी, डेटा या संचार लिंक के लिए उत्तरदायी नहीं होगा"।

राष्ट्रीय साइबर सुरक्षा रणनीति 2020

- राष्ट्रीय साइबर सुरक्षा रणनीति 2020 को मार्च 2021 में राष्ट्रीय सुरक्षा परिषद सचिवालय में राष्ट्रीय साइबर सुरक्षा समन्वयक के कार्यालय द्वारा तैयार किया गया था।
- रणनीति का उद्देश्य **साइबर सुरक्षा ऑडिट गुणवत्ता में सुधार करना** है ताकि संगठन अपने साइबर सुरक्षा वास्तुकला और ज्ञान की बेहतर समीक्षा कर सकें।
- योजना का मुख्य लक्ष्य साइबर घटनाओं, साइबर आतंकवाद और साइबरस्पेस में जासूसी को रोकने के लिए हितधारकों, नीति निर्माताओं और कॉर्पोरेट नेताओं के लिए आधिकारिक मार्गदर्शन के रूप में कार्य करना है।
- इसमें साइबर तैयारियों के सूचकांक और प्रदर्शन की निगरानी की भी आवश्यकता है।

भारतीय रिज़र्व बैंक अधिनियम, 2018

- भारतीय रिजर्व बैंक ने 2018 में RBI अधिनियम पेश किया, जिसमें **UCBs** (urban co-operative banks-शहरी सहकारी बैंक) **और भुगतान ऑपरेटरों के लिए साइबर सुरक्षा** दिशानिर्देश और ढांचे का विवरण दिया गया है। 2018 के RBI अधिनियम का लक्ष्य है:
    - ऐसे मानक बनाना जो बैंकों और भुगतान ऑपरेटरों के सुरक्षा ढांचे को नई प्रौद्योगिकियों और डिजिटलीकरण के अनुकूल बनाने के तरीके के अनुसार समान बने।
    - बैंकों को अपनी साइबर संकट प्रबंधन योजनाएँ बनाने और प्रस्तुत करने का आदेश देना।
    - बैंकों को नियमित रूप से खतरा मूल्यांकन ऑडिट शेड्यूल करने के लिए प्रोत्साहित करना।
    - बैंकों को एंटी-फ़िशिंग और एंटी-मैलवेयर तकनीक के साथ अपने स्वयं के ईमेल डोमेन को लागू करने में सहायता करना।

- सभी भारतीय बैंकों को भुगतान प्रसंस्करण साइबर सुरक्षा के लिए ढांचे को मानकीकृत करने और डिजिटल वातावरण में लगातार बढ़ती व्यावसायिक जटिलताओं से निपटने के लिए इन दिशानिर्देशों का पालन करना चाहिए।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In)

- **2004 में** आधिकारिक बनाया गया, CERT-In सूचना प्रौद्योगिकी अधिनियम, 2000 की **धारा 70बी के तहत** स्थापित **राष्ट्रीय नोडल एजेंसी** है, जो कंप्यूटर सुरक्षा संबंधी घटनाओं के घटित होने पर प्रतिक्रिया देती है।
- CERT-In अपनी वेबसाइट पर सूचना के प्रसार के माध्यम से सुरक्षा मुद्दों पर जागरूकता पैदा करता है और 24x7 घटना प्रतिक्रिया सहायता डेस्क संचालित करता है।
- यह घटना निवारण और प्रतिक्रिया सेवाओं के साथ-साथ सुरक्षा गुणवत्ता प्रबंधन सेवा भी प्रदान करता है।
- CERT-In साइबर सुरक्षा के क्षेत्र में निम्नलिखित कार्य करता है:
  - साइबर घटनाओं पर सूचना का संग्रहण, विश्लेषण और प्रसार;
  - साइबर सुरक्षा घटनाओं का पूर्वानुमान और अलर्ट;
  - साइबर सुरक्षा घटनाओं से निपटने के लिए आपातकालीन उपाय;
  - साइबर घटना प्रतिक्रिया गतिविधियों का समन्वय;
  - साइबर घटनाओं की सूचना सुरक्षा, प्रथाओं, प्रक्रियाओं, रोकथाम, प्रतिक्रिया और रिपोर्टिंग से संबंधित दिशानिर्देश, सलाह, भेद्यता नोट और श्वेतपत्र जारी करना; और
  - साइबर सुरक्षा से संबंधित ऐसे अन्य कार्य जो निर्धारित किये जा सकते हैं।

राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Center-NCIIPC)

- NCIIPC की स्थापना **16 जनवरी 2014 को IT अधिनियम, 2000 की धारा 70ए के तहत** भारत सरकार द्वारा की गई थी।
- **नई दिल्ली में स्थित,** NCIIPC को महत्वपूर्ण सूचना अवसंरचना संरक्षण के मामले में राष्ट्रीय नोडल एजेंसी के रूप में नियुक्त किया गया था।
- इसके अतिरिक्त, NCIIPC को **राष्ट्रीय तकनीकी अनुसंधान संगठन** (National Technical Research Organization-NTRO) की एक इकाई माना जाता है और इसलिए यह प्रधान मंत्री कार्यालय के अंतर्गत आता है।
- NCIIPC को महत्वपूर्ण सूचना बुनियादी ढांचे के लिए राष्ट्रीय स्तर के खतरों की निगरानी और रिपोर्ट करना आवश्यक है। महत्वपूर्ण क्षेत्रों में शामिल हैं:
  - शक्ति और ऊर्जा
  - बैंकिंग, वित्तीय सेवाएँ और बीमा
  - दूरसंचार और सूचना
  - परिवहन
  - सरकार
  - सामरिक और सार्वजनिक उद्यम
- NCIIPC ने इन महत्वपूर्ण क्षेत्रों, विशेष रूप से बिजली और ऊर्जा में, संगठनों के लिए नीति मार्गदर्शन, ज्ञान साझाकरण और साइबर सुरक्षा जागरूकता के लिए कई दिशानिर्देशों को सफलतापूर्वक लागू किया है।

डिजिटल व्यक्तिगत डेटा संरक्षण (Digital Personal Data Protection-DPDP) अधिनियम, 2023

- 11 अगस्त, 2023 को डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 (अधिनियम) को भारत के राष्ट्रपति की सहमति प्राप्त हुई और इसे आधिकारिक राजपत्र में प्रकाशित किया गया।
- DPDP अधिनियम **भारत का पहला डेटा संरक्षण अधिनियम** है, और यह **भारत में व्यक्तिगत डेटा के प्रसंस्करण के लिए एक रूपरेखा** स्थापित करता है।
- यह डिजिटल व्यक्तिगत डेटा के प्रसंस्करण के लिए इस तरह से प्रावधान करता है जो व्यक्तियों के अपने व्यक्तिगत डेटा की सुरक्षा के अधिकारों और वैध उद्देश्यों के लिए और उससे जुड़े या प्रासंगिक मामलों के लिए ऐसे व्यक्तिगत डेटा को संसाधित करने की आवश्यकता दोनों को पहचानता है।
- यह अधिनियम संक्षिप्त और सरल है, यानी सरल, सुलभ, तर्कसंगत और कार्रवाई योग्य कानून है, और संसदीय कानून बनाने में महिलाओं को स्वीकार करने के लिए "he" के बजाय "she" शब्द का इस्तेमाल किया गया है।

सात सिद्धांत

यह अधिनियम निम्नलिखित सात सिद्धांतों पर आधारित है:

- व्यक्तिगत डेटा के सहमतिपूर्ण, वैध और पारदर्शी उपयोग का सिद्धांत;
- उद्देश्य सीमा का सिद्धांत (व्यक्तिगत डेटा का उपयोग केवल डेटा प्रिंसिपल की सहमति प्राप्त करने के समय निर्दिष्ट उद्देश्य के लिए);
- डेटा न्यूनीकरण का सिद्धांत (केवल उतना ही व्यक्तिगत डेटा एकत्र करना जितना निर्दिष्ट उद्देश्य को पूरा करने के लिए आवश्यक है);
- डेटा सटीकता का सिद्धांत (सुनिश्चित करना कि डेटा सही और अद्यतन है);
- भंडारण सीमा का सिद्धांत (डेटा को केवल तब तक संग्रहीत करना जब तक कि निर्दिष्ट उद्देश्य के लिए इसकी आवश्यकता हो);
- उचित सुरक्षा उपायों का सिद्धांत; और
- जवाबदेही का सिद्धांत (डेटा उल्लंघनों और विधेयक के प्रावधानों के उल्लंघनों के निर्णय और उल्लंघनों के लिए दंड लगाने के माध्यम से)।

इंटरनेट ऑफ थिंग्स (Internet of Things-IoT)

- इंटरनेट ऑफ थिंग्स शब्द का तात्पर्य जुड़े हुए उपकरणों और प्रौद्योगिकी के सामूहिक नेटवर्क से है जो **उपकरणों और क्लाउड के साथ-साथ स्वयं उपकरणों के बीच संचार की सुविधा** प्रदान करता है।
- मूल रूप से, IoT रोजमर्रा की "चीजों" को इंटरनेट के साथ एकीकृत करता है।

IoT का कार्य

- IoT सिस्टम वास्तविक समय में डेटा के संग्रह और आदान-प्रदान के माध्यम से काम करते हैं। एक IoT प्रणाली में तीन घटक होते हैं: **स्मार्ट डिवाइस, IoT एप्लिकेशन और एक ग्राफिकल यूजर इंटरफ़ेस।**
- स्मार्ट डिवाइस एक उपकरण है, जैसे टेलीविजन, सुरक्षा कैमरा, या व्यायाम उपकरण जिसे कंप्यूटिंग क्षमताएं दी गई हैं। यह अपने वातावरण, उपयोगकर्ता इनपुट या उपयोग पैटर्न से डेटा एकत्र करता है और अपने IoT एप्लिकेशन से इंटरनेट पर डेटा संचार करता है।
- IoT एप्लिकेशन सेवाओं और सॉफ़्टवेयर का एक संग्रह है जो विभिन्न IoT उपकरणों से प्राप्त डेटा को एकीकृत करता है। यह इस डेटा का विश्लेषण करने और सूचित निर्णय लेने के लिए मशीन लर्निंग या कृत्रिम बुद्धिमत्ता (Artificial Intelligence-AI) तकनीक का उपयोग करता है।
- निर्णय वापस IoT डिवाइस को सूचित कर दिए जाते हैं और IoT डिवाइस फिर इनपुट पर समझदारी से प्रतिक्रिया करता है।
- IoT डिवाइस को ग्राफिकल यूजर इंटरफ़ेस के माध्यम से प्रबंधित किया जा सकता है।

IoT उपकरणों के उदाहरण

कनेक्टेड कारें

- ऐसे कई तरीके हैं जिनसे वाहनों, जैसे कारों, को इंटरनेट से जोड़ा जा सकता है। यह स्मार्ट डैशकैम, इंफोटेनमेंट सिस्टम या यहां तक कि वाहन के कनेक्टेड गेटवे के माध्यम से भी हो सकता है।
- वे ड्राइवर के प्रदर्शन और वाहन दोनों की निगरानी के लिए एक्सीलेटर, ब्रेक, स्पीडोमीटर, ओडोमीटर, पहियों और ईंधन टैंक से डेटा एकत्र करते हैं।

कनेक्टेड घर

- स्मार्ट होम डिवाइस मुख्य रूप से घर की दक्षता और सुरक्षा में सुधार के साथ-साथ घरेलू नेटवर्किंग में सुधार पर केंद्रित हैं।
- स्मार्ट आउटलेट जैसे उपकरण बिजली के उपयोग की निगरानी करते हैं और स्मार्ट थर्मोस्टेट बेहतर तापमान नियंत्रण प्रदान करते हैं।
- हाइड्रोपोनिक सिस्टम बगीचे के प्रबंधन के लिए IoT सेंसर का उपयोग कर सकते हैं जबकि IoT स्मोक डिटेक्टर तंबाकू के धुएं का पता लगा सकते हैं।
- दरवाज़े के ताले, सुरक्षा कैमरे और पानी रिसाव डिटेक्टर जैसी घरेलू सुरक्षा प्रणालियाँ खतरों का पता लगा सकती हैं और उन्हें रोक सकती हैं, और घर के मालिकों को अलर्ट भेज सकती हैं।

स्मार्ट शहर

- IoT अनुप्रयोगों ने शहरी नियोजन और इन्फ्रास्ट्रक्चर के रखरखाव को अधिक कुशल बना दिया है।

- IoT अनुप्रयोगों का उपयोग वायु गुणवत्ता और विकिरण के स्तर को मापने, स्मार्ट प्रकाश व्यवस्था के साथ ऊर्जा बिल को कम करने, महत्वपूर्ण इन्फ्रास्ट्रक्चर के लिए रखरखाव की जरूरतों का पता लगाने और कुशल पार्किंग प्रबंधन के माध्यम से मुनाफा बढ़ाने के लिए किया जा सकता है।

उत्पादन

- IoT एप्लिकेशन मशीन की विफलता होने से पहले ही उसका अनुमान लगा सकते हैं, जिससे उत्पादन डाउनटाइम कम हो जाता है।
- श्रमिकों को संभावित खतरों के बारे में चेतावनी देने के लिए हेलमेट और रिस्टबैंड में पहनने योग्य उपकरणों के साथ-साथ कंप्यूटर विज़न कैमरों का उपयोग किया जाता है।

रसद एवं परिवहन

- वाणिज्यिक और औद्योगिक IoT उपकरण इन्वेंट्री प्रबंधन, विक्रेता संबंध, फ्लीट प्रबंधन और निर्धारित रखरखाव सहित आपूर्ति श्रृंखला प्रबंधन में मदद कर सकते हैं।
- शिपिंग कंपनियाँ परिसंपत्तियों पर नज़र रखने और शिपिंग मार्गों पर ईंधन की खपत को अनुकूलित करने के लिए औद्योगिक IoT अनुप्रयोगों का उपयोग करती हैं।

IoT के लाभ

- वास्तविक समय संसाधन दृश्यता।
- लागत में कमी।
- परिचालन दक्षता में सुधार।
- त्वरित निर्णय लेने के लिए डेटा-संचालित अंतर्दृष्टि।
- शुरू से अंत तक, परिसंपत्तियों/संसाधनों की दूरस्थ निगरानी और प्रबंधन।
- वास्तविक समय, पूर्वानुमानित और अनुदेशात्मक अंतर्दृष्टि।
- अंतिम-ग्राहक अनुभव में सुधार।

बिग डेटा

- परिभाषा के अनुसार, बिग डेटा वह डेटा है जिसके पैमाने, विविधता और जटिलता को प्रबंधित करने और इससे मूल्य और छिपे हुए ज्ञान को निकालने के लिए नई वास्तुकला, तकनीकों, एल्गोरिदम और विश्लेषण की आवश्यकता होती है। बिग डेटा की विशेषता 6Vs है:
    - **आयतन (Volume):** असंख्य स्रोतों से प्राप्त डेटा की मात्रा।
    - **विविधता (Variety):** डेटा के प्रकार: संरचित, अर्ध-संरचित, असंरचित।
    - **वेग (Velocity):** वह गति जिस पर बिग डेटा उत्पन्न होता है।
    - **सत्यता (Veracity):** बिग डेटा पर किस हद तक भरोसा किया जा सकता है।
    - **मूल्य (Value):** एकत्र किए गए डेटा का व्यावसायिक मूल्य।
    - **परिवर्तनशीलता (Variability):** वे तरीके जिनसे बड़े डेटा का उपयोग और स्वरूपण किया जा सकता है।

बिग डेटा के अनुप्रयोग

शासन

- साइबर हमलों को रोकने के लिए।
- सुरक्षा प्रणालियाँ बढ़ाना।

- कार्ड से संबंधित धोखाधड़ी के मामलों का पता लगाना।
- आपराधिक गतिविधियों को कम करना।
- शिक्षा की गुणवत्ता में सुधार।
- आपदा प्रबंधन।

खुदरा/उपभोक्ता

- बाज़ार आधारित विश्लेषण।
- आपूर्ति श्रृंखला प्रबंधन और विश्लेषण।
- व्यवहार आधारित लक्ष्यीकरण।
- बाजार और उपभोक्ता विभाजन।

चिकित्सा एवं स्वास्थ्य

- क्लिनिकल परीक्षण डेटा विश्लेषण।
- रोग पैटर्न विश्लेषण।
- अभियान और बिक्री कार्यक्रम अनुकूलन।
- रोगी देखभाल गुणवत्ता और कार्यक्रम विश्लेषण।
- चिकित्सा उपकरण और फार्मेसी आपूर्ति श्रृंखला प्रबंधन।
- दवा की खोज और विकास विश्लेषण।

अर्थव्यवस्था

- वित्तीय डेटा प्रबंधित करने के लिए।
- उत्पादन, मूल्य आँकड़ों को पकड़ने और परिणामी सकल घरेलू उत्पाद की गणना करने के लिए।
- जोखिमों से बचना और वित्तीय फर्मों के घाटे को कम करना।
- कर चोरों को पकड़ना।
- शेल कंपनियों का पंजीकरण रद्द करना।
- मनी लॉन्ड्रिंग को रोकना और आतंकवाद के वित्तपोषण पर अंकुश लगाना।

वित्त और धोखाधड़ी सेवाएँ

- अनुपालन और विनियामक रिपोर्टिंग।
- जोखिम विश्लेषण और प्रबंधन।
- धोखाधड़ी का पता लगाना और सुरक्षा विश्लेषण।
- क्रेडिट जोखिम और स्कोरिंग।
- व्यापार निगरानी।
- हाई स्पीड आर्बिट्राज ट्रेडिंग।

वेब और डिजिटल मीडिया

- बड़े पैमाने पर क्लिकस्ट्रीम विश्लेषण।
- विज्ञापन लक्ष्यीकरण, पूर्वानुमान और अनुकूलन।
- सामाजिक ग्राफ़ विश्लेषण और प्रोफ़ाइल विभाजन।

कृषि एवं भोजन

- बीज चयन।
- कृषि परिसंपत्तियों का ट्रैक रिकॉर्ड रखने के लिए जियो-टैगिंग।
- मौसम की भविष्यवाणी।
- प्रभावी जल प्रबंधन।

- खाद्य प्रसंस्करण।
- फसल रोगों की पहचान।

दूरसंचार

- राजस्व आश्वासन और मूल्य अनुकूलन।
- कॉल डिटेल रिकॉर्ड विश्लेषण।
- नेटवर्क प्रदर्शन।
- मोबाइल उपयोगकर्ता स्थान विश्लेषण।

भारत में सरकारी पहल और हस्तक्षेप

- **राष्ट्रीय डेटा और एनालिटिक्स प्लेटफ़ॉर्म (National Data & Analytics Platform-NDAP):** नीति आयोग ने मई 2022 में राष्ट्रीय डेटा और एनालिटिक्स प्लेटफ़ॉर्म लॉन्च किया। यह प्लेटफ़ॉर्म सरकार भर से विविध डेटासेट को जोड़ने के लिए अत्याधुनिक तरीकों का उपयोग करता है और कई प्रकार के डेटा का उपयोग एक ही बार में करने के लिए सक्षम बनाता है। फरवरी 2023 तक, NDAP **15 क्षेत्रों और 46 मंत्रालयों से 885 डेटासेट** को होस्ट करता है।
- **बिग डेटा प्रबंधन नीति:** इसे राज्यों और केंद्र शासित प्रदेशों में सार्वजनिक क्षेत्र द्वारा उत्पन्न **डेटा के बड़े हिस्से के ऑडिट** के लिए CAG द्वारा तैयार किया गया था।
- **आधिकारिक सांख्यिकी पर राष्ट्रीय डेटा वेयरहाउस:** सांख्यिकी और कार्यक्रम कार्यान्वयन मंत्रालय ने व्यापक-आर्थिक समुच्चय की गुणवत्ता में और सुधार करने के लिए बिग डेटा विश्लेषणात्मक उपकरणों का लाभ उठाने की दृष्टि से आधिकारिक सांख्यिकी पर एक राष्ट्रीय डेटा वेयरहाउस स्थापित करने का प्रस्ताव दिया है।
- महात्मा गांधी राष्ट्रीय ग्रामीण रोजगार गारंटी अधिनियम में प्रत्यक्ष लाभ हस्तांतरण का उपयोग, प्रमाणीकरण और कल्याणकारी योजना का लाभ उठाने के लिए आधार, स्मार्ट सिटी मिशन, डिजिटल इंडिया, BHIM ऐप आदि महत्वपूर्ण सरकारी पहल हैं जो देश में सुशासन प्राप्त करने के लिए बिग डेटा का उपयोग कर रहे हैं।