ऑनलाइन पाठ्य सामग्री

2DCA1

IT TRENDS

UNIT–III

इकाई-3

डॉ. मनीष माहेश्वरी

डॉ. सुनीता द्विवेदी

माखनलाल चतुर्वेदी राष्ट्रीय पत्रकारिता एवं संचार विश्वविद्यालय

बी -38,विकास भवन, एम पी नगर,जोन-1, भोपाल

3. ई-गवर्नेंस

डिजिटलाइजेशन के निरंतर विकास ने दुनिया भर में कई सरकारों को सरकारी प्रक्रियाओं में प्रौद्योगिकी को शामिल करने के लिए प्रेरित किया है। ई-गवर्नेंस या इलेक्ट्रॉनिक गवर्नेंस या इलेक्ट्रॉनिक शासन का अर्थ प्रौद्योगिकी संचालित शासन से है। ई-गवर्नेंस का अर्थ है, सरकार की सभी योजनाएं और सेवाएं नागरिकों तक सूचना एवं संचार प्रौद्योगिकी के माध्यम से उपलब्ध हो जिससे कि इन योजनाओं और सेवाओं का उपयोग शीघ्रता से और पारदर्शिता से किया जा सके।

ई-गवर्नेंस सरकार को अधिक नागरिक-केंद्रित बनाती है। ई-गवर्नेंस केवल सरकारी वेब साइट और ई-मेल, केवल इंटरनेट पर सेवा वितरण के बारे में या सिर्फ सरकारी जानकारी या इलेक्ट्रॉनिक भुगतान तक डिजिटल पहुंच के बारे में नहीं है। यह सभी सुविधाएं ई गवर्नेंस का हिस्सा है। ई-गवर्नेंस नागरिकों को सरकार के साथ संवाद करने, सरकारों की नीति बनाने में सहायता करने और नागरिकों को एक-दूसरे से संवाद करने की सुविधा देता है। सरकार ई-गवर्नेंस को एक उपकरण (tool) के रूप में उपयोग करके नागरिकों की वास्तविक जरूरतों और कल्याण को पता कर सकती है। ई-गवर्नेंस सही मायने में नागरिकों को सरकारी निर्णय लेने की प्रक्रिया में भाग लेने की अनुमति देती है, ई-गवर्नेंस के माध्यम से, सरकारी सेवाओं को नागरिकों को एक उपयुक्त, व्यवस्थित और पारदर्शी मोड में उपलब्ध कराया जाता है।

शासन की अवधारणाओं में भाग लेने वाले तीन मुख्य समूह होते हैं स्वयं सरकार, जनसामान्य और व्यवसायिक समूह। ई-गवर्नेंस का रणनीतिक उद्देश्य सभी दलों, सरकार, नागरिकों और व्यवसायों के लिए शासन का समर्थन और सरलीकरण करना है। सूचना एवं संचार प्रौद्योगिकी का उपयोग तीनों ही समूह की समर्थन प्रक्रियाओं और गतिविधियों को जोड़ सकता है। दूसरे शब्दों में, ई-गवर्नेंस इलेक्ट्रॉनिक साधनों के उपयोग से सुशासन का समर्थन और अनुकरण करता है।

शासन के लिए सूचना एवं संचार प्रौद्योगिकी (आईसीटी) की मुख्य भूमिका निम्नानुसार है:

- वर्तमान में प्रदान किए जा रहे शासन उत्पादों, योजनाओं और सेवाओं की गुणवत्ता में सुधार करना।
- नागरिक-केंद्रित शासन अर्थात जो शासन की सेवाओं में लोगों की भागीदारी बढ़ाएँ।
- शासन क्षेत्र के तहत समाज के वंचित वर्गों (गरीब, अनपढ़, ग्रामीण लोग,
- प्रवासी और विस्थापित लोग) को शामिल किया जा सके।
- एक प्रभावी सरकार जो करदाताओं के पैसे (त्वरित और कुशल सेवाओं) के लिए अधिकतम मूल्य प्रदान करती है।
- आम तौर पर रिकॉर्ड और जानकारी अलग-अलग स्थानों होने के कारण सरकार लोगों के प्रश्नों और समस्याओं का जवाब देने में बहुत समय लेती है। वहीं आईसीटी की मदद से कार्य कम समय में किया जा सकता है।

3.1 ई-गवर्नेंस के प्रकार

- **जी 2 जी (G 2 G) : सरकार से सरकार (Governement to Government)**
  विभिन्न सरकारी विभागों, फर्मों और एजेंसियों के बीच जब सूचना और सेवाओं का आदान-प्रदान होता है। इससे सरकारी प्रक्रियाओं की दक्षता बढ़ जाती है। यह विभिन्न सरकारी संस्थाओं और राष्ट्रीय, राज्य और स्थानीय सरकारी संस्थाओं के बीच और इकाई के विभिन्न स्तरों के बीच कार्य करता है। जी 2 जी में, सरकारी एजेंसियां ऑनलाइन संचार का उपयोग करके समान डेटाबेस साझा कर सकती हैं। जी 2 जी सेवाएँ स्थानीय स्तर पर या अंतर्राष्ट्रीय स्तर पर हो सकती हैं।
  अगर भारत सरकार कोई जानकारी राज्यों को देना चाहती है, तो उस जानकारी से जुड़ी वेबसाइट पर उस जानकारी को डाला जा सकता है। जिसके चलते सरकारों के बीच में कम समय में ज्यादा संपर्क हो जाता है। इसी तरह कई अन्य सरकारी विभाग भी आपस में संपर्क करते हैं और जानकारी को साझा करते हैं।

- **जी 2 सी (G 2 C): सरकार से नागरिक (Government to Citizen)**

  एक आम नागरिक इसकी मदद से अपने सरकारी कामों को आसानी से पूरा कर सकता है। सरकार-से-नागरिक का प्राथमिक उद्देश्य नागरिकों को सुविधाओं की आपूर्ति करना है। यह आम लोगों को लेनदेन करने के लिए समय और लागत को कम करने में भी मदद करता है। एक नागरिक कहीं से भी कभी भी सुविधाएं प्राप्त कर सकता है। नागरिकों को किसी भी समय, कहीं भी सरकारी नीतियों पर अपने विचारों और शिकायतों को साझा करने की स्वतंत्रता है। उदाहरण के लिए मान लीजिए कि अगर किसी व्यक्ति को अपनी किसी बीमा पॉलिसी के बारे में जानकारी लेनी हो, तो वो व्यक्ति बिना बीमा पॉलिसी के दफ्तर जाए अपना ये कार्य कर सकता है। गैस सब्सिडी खाते में आना, परीक्षाओं की जानकारी अथवा रिजल्ट वेबसाइट से मिलना। इसी तरह कोई भी व्यक्ति अपना आयकर, पानी का बिल, रेल का टिकट इनके विभागों में बिना जाए करवा सकता है।

- **जी 2 बी (G 2 B): सरकार से व्यवसाय (Govrnmrnt to Business)** इसमे सरकार और व्यावसायिक फर्मों के बीच सेवाओं का आदान-प्रदान आईसीटी के माध्यम से होता है। यह सरकार और व्यावसायिक कंपनियों दोनों के लिए उत्पादक और लाभदायक है। जी 2 बी व्यवसाय विकास में एक महत्वपूर्ण भूमिका निभाता है। यह सरकारी परियोजनाओं की संचार और पारदर्शिता की दक्षता और गुणवत्ता को उन्नत करता है। इसके माध्यम से व्यापारी घर से ही ऑनलाइन सरकारी कामों को कर सकते है तथा सरकार व्यापारिक क्षेत्रों में संपर्क कर लेन-देन का काम करती है। जैसे ट्रेडिंग लाइसेंस के लिए आवेदन करना, कंपनी या सोसाइटी का रजिस्ट्रेशन, सरकार द्वारा व्यापारों के लिए चलाई गई किसी भी योजना की जानकारी, वैट के लिए पंजीकरण करवाना हो इत्यादि। ऐसा करने से व्यापारियों के समय की बचत होती है।

जी 2 ई (G 2 E): सरकार से कर्मचारी (Government to Employee)

किसी भी देश की सरकार सबसे बड़ी नियोक्ता है और इसलिए वह नियमित आधार पर कर्मचारियों के साथ काम करती है। जी 2 ई का उद्देश्य कर्मचारियों को एक साथ लाना

और ज्ञान साझा करने में सुधार लाना है। यह कर्मचारियों को ऑनलाइन सुविधाएं प्रदान करता है। इसी तरह, छुट्टी के लिए आवेदन करना, वेतन भुगतान रिकॉर्ड की समीक्षा करना और छुट्टी के संतुलन की जांच करना। जी 2 ई क्षेत्र मानव संसाधन प्रशिक्षण और विकास देता है। यह सरकार और कर्मचारियों के बीच कुशलता और तेजी से संपर्क बनाने में मदद करता है, साथ ही उनके लाभों को बढ़ाकर उनके संतुष्टि स्तर तक पहुँचाने में मदद करता है।

3.2 ई-डेमोक्रेसी (E-Democracy)

डेमोक्रेसी (Democracy) शब्द का हिंदी में अर्थ लोकतंत्र, जनतंत्र, या प्रजातंत्र है। इन सभी शब्दों अर्थ होता है 'जनता का शासन'। लोकतंत्र या प्रजातंत्र एक ऐसी शासन व्यवस्था है जिसमें जनता को ये अधिकार दिया गया है कि वह अपनी इच्छा अनुसार अपने शासक का चुनाव करे।

ई-डेमोक्रेसी अर्थात ई-लोकतंत्र, इलेक्ट्रॉनिक और लोकतंत्र शब्द का एक संयोजन है जिसे डिजिटल लोकतंत्र या इंटरनेट लोकतंत्र के रूप में भी जाना जाता है। ई-लोकतंत्र मौजूदा ई-गवर्नेंस मॉडल और प्रथाओं को समृद्ध और परिवर्तित करने के लिए संचार प्रौद्योगिकी का स्मार्ट उपयोग है।

आज का लोकतंत्र प्रतिनिधि लोकतंत्र हैं जिसमें कानूनों, नीतियों और विनियमों के निर्माण और क्रियान्वयन के लिए प्रतिनिधियों का चुनाव होता है। अंतिम निर्णय लेने की शक्ति लोगों द्वारा चुने गए प्रतिनिधियों के पास ही होती है। बड़ा प्रश्न यह है कि चुने गए प्रतिनिधियों लोगों की इच्छा या रुचि का कितना अच्छा प्रतिनिधित्व करते हैं।

लोकतंत्र उतना ही अच्छा माना जाता है जिसमें सरकार लोगों की इच्छा या रुचि का ज्यादा से ज्यादा प्रतिनिधित्व करती है। लोकतंत्र में बदलाव अर्थात ई-लोकतंत्र के आगमन से निर्वाचित प्रतिनिधियों से लेकर व्यक्ति तक राजनीतिक प्रतिनिधित्व बढ़ेगा। ई-लोकतंत्र सूचना एवं प्रौद्योगिकी का उपयोग कर लोकतांत्रिक निर्णय लेने की प्रक्रिया में जनता की भागीदारी को बढ़ाता है।

तकनीक एवं इंटरनेट के प्रयोग ने सूचना को साधारण नागरिक तक आसानी से पहुंचा दिया है। सरकार या राजनेताओं के कार्यों के बारे में जानकारी प्राप्त करना और उसके विषय में अपनी राय प्रकट करना इंटरनेट और आईसीटीने बहुत आसान बना दिया है।

आजकल राजनेताओं द्वारा भी तकनीक एवं इंटरनेट का प्रयोग किया जा रहा है। सोशल मीडिया साइट एवं ऑनलाइन टूल का उपयोग कर राजनेता सीधे आम जनता से जुड़ सकते हैं, सीधे संवाद कर सकते हैं। जनता से प्रतिक्रिया और सलाह प्राप्त कर सकते हैं।

जनता के साथ प्रभावी ढंग से संवाद करने से एक लोकतंत्र अधिक प्रभावी रूप से कार्य करने में सक्षम है। एक प्रभावी लोकतंत्र वह है जो नागरिकों को न केवल सरकार बनाने में योगदान देता है बल्कि समाज को बेहतर बनाने के लिए संवाद करने का मौका देता है। ई-लोकतंत्र पारस्परिक विचार विमर्श एवं सार्वजनिक चर्चा के लिए एक मंच प्रदान करता है और उन्हें सार्वजनिक नीति पर प्रभाव डालने की अनुमति देता है। सरकार को उन प्रमुख मुद्दों पर ध्यान केंद्रित करने में मदद करता है जो समुदाय चाहता है। ई-लोकतंत्र सरकार का एक रूप है जिसमें सभी वयस्क नागरिकों को राजनीतिक प्रक्रियाओं, प्रस्ताव, विकास और कानूनों के निर्माण में समान रूप से भाग लेने के लिए पात्र माना जाता है। ई-लोकतंत्र सामाजिक, आर्थिक और सांस्कृतिक परिस्थितियों को समाहित करता है।

3.3 पब्लिक प्राइवेट पार्टनरशिप

पब्लिक प्राइवेट पार्टनरशिप या सार्वजनिक-निजी साझेदारी को PPP, 3P या P3 आदि नामो से जाना जाता हैं।

सार्वजनिक-निजी साझेदारी एक मॉडल है, जहाँ सरकार बुनियादी परियोजनाओं को पूरा करने के लिए निजी कंपनियों के साथ जुड़ती है। सार्वजनिक-निजी भागीदारी में एक सरकारी एजेंसी और एक निजी क्षेत्र की कंपनी के बीच सहयोग शामिल होता है। दोनों दलों के बीच यह गठबंधन, देश के भीतर अवसंरचनात्मक (Infrastructural) सुविधाओं की वित्त व्यवस्था, डिजाइन, निर्माण और रखरखाव को सुनिश्चित करता है।

सार्वजनिक निजी भागीदारी एक दीर्घकालिक अनुबंध है जो एक सार्वजनिक प्राधिकरण और निजी क्षेत्र द्वारा दीर्घकालिक संपत्ति या सेवा प्रदान करने के लिए बनाई गई है। इसके तहत सरकार निजी कंपनियों के साथ अपनी परियोजनाओं को पूरा करती है। इसके द्वारा किसी जन सेवा या बुनियादी ढांचे के विकास के लिए धन की व्यवस्था की जाती है। इसमें सरकारी और निजी संस्थान मिलकर अपने पहले से निर्धारित लक्ष्य को पूरा करते हैं और उसे हासिल करते हैं। पीपीपी व्यवस्था पब्लिक इंफ्रास्ट्रक्चर प्रोजेक्ट जैसे नए टेलीकम्युनिकेशन सिस्टम, एयरपोर्ट, हाईवे, सार्वजनिक परिवहन नेटवर्क, पार्क, कन्वेंशन सेंटर या पावर प्लांट के लिए मॉडल है जिसमें धन, योजना, निर्माण, संचालन, रखरखाव और विनिवेश शामिल हैं। सार्वजनिक भागीदार का प्रतिनिधित्व सरकार द्वारा स्थानीय, राज्य या राष्ट्रीय स्तर पर किया जाता है।

पीपीपी व्यवस्था बड़ी परियोजनाओं के लिए उपयोगी होती है जिन्हें शुरू करने के लिए अत्यधिक कुशल श्रमिकों और धन की आवश्यकता होती है। पीपीपी व्यवस्था सरकारी क्षेत्र में निजी क्षेत्र की भागीदारी को संदर्भित करती है, जिसका उद्देश्य प्रबंधन विशेषज्ञता और मौद्रिक योगदान के रूप में सार्वजनिक लाभ के उद्देश्य से है। ऐसी परियोजनाएं संबंधित निजी संस्थाओं को सौंपी जाती हैं जो अपने क्षेत्र में विशेषज्ञता और ज्ञान रखती हैं। सार्वजनिक-निजी भागीदारी के माध्यम से किसी परियोजना को वित्तपोषित (finance) करना किसी परियोजना को जल्द पूरा कर सकता है।

- पीपीपी उच्च प्राथमिकता वाली सरकार, नियोजित परियोजनाओं से संबंधित हैं। इसमें दो पक्ष शामिल हैं- सरकार और संबंधित निजी कंपनी।
- पीपीपी दृष्टिकोण दीर्घकालिक सार्वजनिक सेवाओं की सुविधा से संबंधित है जिसमें एक विशिष्ट अवधि के लिए निजी क्षेत्रके डिजाइन, निर्माण, रखरखाव और सहायक सेवाओं के वितरण की आवश्यकता होती है।
- सफल परियोजना के लिए सरकार और फर्म के बीच पूंजी, डिजाइन और अन्य आवश्यक संसाधन, साझा किए जाते हैं।पीपीपी मॉडल से सरकार को उसकी बजटीय समस्या व उधार लेने की सीमाओ से मुक्ति मिलतीहै।

- पीपीपी का मुख्य उद्देश्य सार्वजनिक और निजी दोनों क्षेत्रों के कौशल, विशेषज्ञता और अनुभव को संयोजित करना है ताकि उच्च गुणवत्ता और नई तकनीक वाली सेवाएं प्रदान की जा सकें।
- ये परियोजनाएं आमतौर पर वर्षों के लिए होती हैं, इसलिए सरकारी प्राधिकरण और निजी संस्था एक विस्तारित अवधि के लिए जुड़ी हुई है।
- सरकारी लाभ के उद्देश्य से सरकार की परियोजनाओं में पीपीपी का उपयोग किया जाता है।सरकार सेवाओं की गुणवत्ता और लागत के लिए जवाबदेह होती है।
- पीपीपी, परियोजनाएं के जीवन चक्र को कम करती हैं और तेजी से कार्यान्वयन होती है। कम समय में और अच्छी गुणवत्ता के साथ उपलब्ध कराई जाती है।
- निजी कंपनी को खुली प्रतिस्पर्धी बोली के आधार पर चुना जाता है और प्रदर्शन के आधार पर भुगतान प्राप्त करता है।

3.4 समाधान: मध्य प्रदेश ऑनलाइन पोर्टल

जैसे की आप लोग जानते है कि राज्य के लोगो को अपनी शिकायत का समाधान प्राप्त करने के लिए सरकारी विभागों के चक्कर काटने पड़ते थे, इसके साथ ही आवश्यक यह भी है कि दफ्तर के कार्य करने वाले समय पर ही व्यक्ति समस्याओं के निराकरण के लिए जा सकते हैं अतः स्वयं का रोजगार और काम भी बहुत प्रभावित होता है। अन्य और भी बहुत सी परेशानियों का सामना करना पड़ता था। जिससे लोगो के काफी समय और धन खराब होता था, इन सभी समस्याओ को देखते हुए मध्य प्रदेश सरकार ने लोगों की शिकायतों के लिए एक पोर्टल का निर्माण किया है। इसके माध्यम से आम नागरिक ऑनलाइन एवं डाक पत्र के माध्यम से अपनी शिकायतें दर्ज करा सकतेहैं। इससे लोगो के समय की बचत होगी और आने जाने की परेशानियां कम होंगी। इस प्रणाली के माध्यम से विभिन्न शिकायतों का पारदर्शी तरीके से निराकरण हो सकेगा। इस हेतु सतत निगरानी विभाग द्वारा की जाएगी।

मध्यप्रदेश राज्य के नागरिकों कि शिकायत दर्ज करने के लिए सबसे पहले समाधान पोर्टल samadhan.mp.gov.in पर जाना होगा।इस सेवा के लिए शिकायतकर्ता को कुछ आवश्यक

जानकारी जैसे – मोबाइल नंबर, आधार नंबर, नाम, उपनाम, ईमेल, जिला, ब्लॉक, ग्राम पंचायत, पता आदि आवश्यक जानकारी को भरना होगा। लाभार्थी को एप्लीकेशन फॉर्म में सही "मोबाइल नंबर" एवं "आधार कार्ड नंबर ढालना होगा ताकि एप्लीकेशन फॉर्म अनुमोदित हो सके तथा इसका सन्देश लाभार्थी तक पहुंच जाए। शिकायत पंजीकरण में यदि किसी अन्य डॉक्यूमेंट की भी आवश्यकता होती है तो डॉक्यूमेंट को स्कैन करके अपलोड करना होगा।

आम नागरिक लिखित रूप से अपनी शिकायत दर्ज कर सकें इसकी भी व्यवस्था की गयी है। इसके लिए पत्र के माध्यम से अपनी शिकायतों को जन शिकायत निवारण विभाग को भेज सकते हैं। पत्र प्राप्त होने पर समाधान पोर्टल पर शिकायत दर्ज करने के साथ ही एक यूनिक जनशिकायत नंबर दिया जायेगा। शिकायत कर्त्ता को पत्र में उल्लेखित मोबाईल नंबर पर sms के द्वारा यूनिक जन शिकायत नंबर भेजा जायेगा या नंबर नहीं होने की दशा में जन शिकायत नंबर पत्र के माध्यम से भेजा जायेगा।

प्राप्त शिकायतों को विभाग के द्वारा परीक्षण कर उपयुक्त विभाग, अधिकारी, जिले आदि को प्रेषित कर दिया जाएगा और जल्द ही शिकायत का समाधान संबंधित विभाग द्वारा प्रदान किया जाएगा।

3.5 सी एम हेल्पलाइन

मध्यप्रदेश में सभी सुखी हो, निरोगी हो, सबका कल्याण हो, यही शासन व्यवस्था का ध्येय है। इसी को आधार बनाकर प्रदेश में सी एम हेल्पलाइन १८१ प्रारंभ की गई है। इसका ध्येय है प्रदेश की जनता को सीएम हेल्पलाइन से मिलेगी त्वरित जानकारी और होगा शिकायतों का त्वरित समाधान। सी एम हेल्प लाइन के माध्यम से राज्य शासन से सम्बंधित सभी योजनाओ की जानकारी ले सकतेहैं। इसके साथ ही राज्य शासन द्वारा दी जा रही सभी सुविधाओ से सम्बंधित शिकायते, मांग एवं सुझाव दर्ज करा सकते है। इससे प्रदेश के विभिन्न विभागों के अधिकारी-कर्मचारियों को जोड़ा गया है, जो इस हेल्पलाइन से प्राप्त समस्याओ, शिकायतों का निराकरण करते हैं।

सी एम हेल्पलाइन पर संपर्क करने के लिए टोल फ्री नंबर 181 पर कॉल किया जा सकता है। कॉल करने का समय सुबह 7 बजे से रात्रि 11 बजे तक का है। सी एम हेल्पलाइन के अंतर्गत शिकायतों के निराकरण की समय सीमा 7 से लेकर 30 दिन तक की है।

3.6 एमपी ऑनलाइन सर्विसेज (MP Online Services)

एमपी ऑनलाइन सरकारी सेवाओं को नागरिकों तक प्रभावी रूप से पहुंचाने का एक सरल और सुरक्षित तरीका है। एमपी ऑनलाइन मध्य प्रदेश सरकार की ई गवर्नेंस की एक महत्वपूर्ण पहल है, जिसका उद्देश्य विभिन्न सरकारी विभागों की सेवाओं को सीधे आम नागरिकों को घर बैठे उपलब्ध कराना है। एमपी ऑनलाइन लिमिटेड मध्य प्रदेश सरकार एवं टाटा कंसलटेंसी सर्विसेज (TCS) लिमिटेड का संयुक्त उपक्रम है।

एमपी ऑनलाइन मध्य प्रदेश के सभी 52 जिलों की 350 से भी अधिक तहसीलों में सेवाएं कियोस्क के माध्यम से ऑनलाइन प्रदान कर रहा है। एमपी ऑनलाइन विभिन्न सरकारी सेवाओं जैसे मध्य प्रदेश के विश्वविद्यालयों एवं कॉलेजों के लिए प्रवेश प्रक्रिया, धार्मिक स्थानों के लिए दान, मध्यप्रदेश के राष्ट्रीय पार्कों में भ्रमण हेतु ऑनलाइन टिकट बुकिंग, बिल भुगतान सुविधा, विभिन्न सरकारी विभागों में भर्ती हेतु आवेदन एवं ऑनलाइन परीक्षा प्रक्रिया सहित विभिन्न पाठ्यक्रमों में प्रवेश हेतु ऑनलाइन काउंसलिंग जैसी सेवाएं प्रदान कर रहा है।

एमपी ऑनलाइन एक सिटीजन सर्विस पोर्टल है जो मध्य प्रदेश राज्य में पब्लिक सर्विस मैं सुधार करने के लिए सूचना तथा कम्युनिकेशन तकनीक का उपयोग करता है। पोर्टल का उद्देश्य नागरिकों तथा बिजनेस की आवश्यकताओं को समय पर पूरा करना है। नागरिक केवल एक क्लिक के माध्यम से विभिन्न प्रकार की सेवाओं को एक्सेस कर सकते हैं, एमपी ऑनलाइन पोर्टल पर उपस्थित ऑनलाइन सेवाओं को नागरिकों तक प्रभावी रूप से पहुंचाने का सरल उपाय कियोस्क है। सामान्यतः कियोस्क शहरी क्षेत्र में स्थित दुकान, ऑफिस, इंटरनेट कैफे ही होता है जो एमपी ऑनलाइन लिमिटेड के साथ नागरिकों को ऑनलाइन सेवाएं प्रदान कराने के लिए एक अनुबंध के तहत अधिकृत किया जाता है। कियोस्क आवंटन के लिए इस प्रकार के व्यवसाय से जुड़े व्यवसायी बंधु नियमानुसार ऑनलाइन आवेदन कर सकते हैं। नागरिकों को

ऑनलाइन सेवा प्रदान कराने पर कियोस्क संचालक को प्रत्येक ऑनलाइन सेवा के लिए निर्धारित सेवा शुल्क प्रदान किया जाता है। इस सेवा शुल्क का निर्धारण सचिव, सूचना प्रौद्योगिकी, मध्य प्रदेश शासन की अध्यक्षता में गठित सेवा शुल्क निर्धारण समिति द्वारा किया जाता है।

3.7 भारतीय सरकार का mygov.in

MyGov (मेरी सरकार) भारतीय सरकार द्वारा निर्मित सिटीजन प्लेटफार्म है। जिसका उद्देश्य देश की गवर्नेंस तथा विकास में भारतीय नागरिकों की सक्रिय भागीदारी को बढ़ाना है। MyGov का उद्देश्य ऑनलाइन प्लेटफॉर्म का उपयोग करके आम नागरिक और सरकार को करीब लाना है इसके लिए विशेषज्ञ तथा आम नागरिकों के मध्य विचारों के आदान-प्रदान के लिए इंटरफ़ेस का निर्माण किया गया है। सरकार का उद्देश्य नागरिकों के विचारों, सुझाव तथा छोटे स्तर पर योगदान के द्वारा सुशासन की दिशा में नागरिक भागीदारी को प्रोत्साहित करना है। इस प्लेटफार्म के माध्यम से भारत के विभिन्न क्षेत्रों के विभिन्न नागरिक विभिन्न नीतियों, कार्यक्रमों, योजनाओं आदि से संबंधित क्षेत्रों के बारे में अपने विचार और सुझाव को सरकार के साथ साझा कर सकते हैं। MyGov पर अपने विचार साझा करने के लिए विभिन्न फोकस समूह उपलब्ध है जहां नागरिक विशेष समूह से संबंधित विभिन्न कार्यों, चर्चाओं, चुनाव, वार्ता और ब्लॉक के माध्यम से अपनी रुचि के कार्य को शेयर कर सकते हैं।

3.8 यूआईडीएआई

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई) एक सांविधिक प्राधिकरण है, जिसकी स्थापना भारत सरकार द्वारा आधार (वित्तीय और अन्य सब्सिडी, लाभ और सेवाओं के लक्षित वितरण) अधिनियम, 2016 ("आधार अधिनियम, 2016") के प्रावधानों के अंतर्गत, इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय के तहत् की गई। भारत एक बहुत बड़ा देश है यह 28 राज्यों और 8 केंद्र शासित प्रदेशों में बटा हुआ है। वर्तमान में लगभग 135 करोड़

जनसंख्या वाला देश है। यूआईडीएआई का मुख्य उद्देश्य भारत के प्रत्येक नागरिक को एक राष्ट्रीय पहचान पत्र उपलब्ध ।यह पहचान पत्र भारतीय नागरिकों को आवश्यक मूलभूत सुविधाएं उपलब्ध कराने के लिए उपयोग किया जाता है।

एक सांविधिक प्राधिकरण के रूप में अपनी स्थापनासे पूर्व यूआईडीएआई तत्कालीन योजना आयोग (अब नीति आयोग) राजपत्र अधिसूचना संख्याए-43011/02/2009-एडमिन-1 दिनांक 28 जनवरी, 2009 के तहत् इसके एक संबद्धकार्यालय के रूप में कार्य कर रहा था। बाद में सरकार द्वारा सरकारी कार्य आवंटन नियमों में संशोधन करके 12 सितंबर, 2015 को यूआईडीएआई को तत्कालीन सूचना और प्रौद्योगिकी विभाग (डीईआईटीवाई) के साथ संबद्ध कर दिया गया।

यूआईडीएआई की स्थापना भारत के सभी निवासियों को "आधार" नाम से एक विशिष्ट पहचान संख्या (यूआईडी) प्रदान करने हेतु की गई थी ताकि इसके द्वारा (क) दोहरी और फर्जी पहचान समाप्त की जा सके और प्रत्येक नागरिक की एक वास्तविक पहचान हो, जिसका उपयोग सभी योजनाओं, संस्थाओं और संसाधनों के उपयोग में किया जासके (ख) उसे आसानी से एवं किफायती लागत में सत्यापित और प्रमाणित किया जा सके।

आधार अधिनियम 2016 के तहत्, यूआईडीएआई आधार नामांकन और प्रमाणीकरण, आधार जीवन चक्र के सभी चरणों के प्रबंधन और संचालन सहित, नागरिकों को आधार नंबर जारी करने और प्रमाणीकरण करने के लिए नीति, प्रक्रिया और प्रणाली विकसित करने के लिए और पहचान जानकारी तथा प्रमाणीकरण रिकार्ड की सुरक्षा सुनिश्चित करने के लिए जिम्मेदार है।

3.8.1 यूआईडीएआई के लक्ष्य

- भारत के निवासियों को एक विशिष्ट पहचान उपलब्ध करना जिसे डिजिटल माध्यम से कहीं भी, कभी भी सत्यापित किया जा सके।

3.8.2 यूआईडीएआई के उद्देश्य

- एक अच्छी तरह से परिभाषित समय-सीमा और कड़े गुणवत्ता मेट्रिक्स का पालन करते हुए प्रत्येक निवासी को आधार नंबर प्रदान करना
- अपने सहयोगियों के साथ मिलकर ऐसी संरचना बनाना जो निवासियों को उनकी डिजिटल पहचान को अद्यतन रखने व सत्यापित करने में सुविधाजनक हो
- आधार का लाभ उठाकर निवासियों को उचित, प्रभावी व निष्पक्ष सेवा मिल सके, इस हेतु भागीदारों व सेवा प्रदाताओं के साथ कार्य करना, नवोत्थान को प्रोत्साहित करना, जिसके लिए सरकारी व गैर-सरकारी संस्थाओं द्वारा आधार से जुड़े एप्लीकेशन्स बनवाने हेतु मंच प्रदान करना
- आधार की तकनीकि संरचना की उपलब्धता, विस्तार व परिवर्तनशीलता सुनिश्चित करना
- भा.वि.प. प्राधिकरण (यूआईडीएआई) के लक्ष्यों व आदर्शों को बढ़ावा देने हेतु एक मजबूत व दीर्घ कालिक संगठन बनाना
- विश्व के विभिन्न क्षेत्रों में उपलब्ध सर्वोत्तम निपुणताओं को भागीदारी के आधार पर भा.वि.प. प्राधिकरण (यूआईडीएआई) हेतु उपयोग में लाना
- प्रौद्योगिकी अवसंरचना की उपलब्धता, मापनीयता और परिवर्तनशीलता सुनिश्चित करना

3.9 आधार (Adhar)

आधार यूआईडीएआई प्राधिकरण द्वारा निर्धारित सत्यापन प्रक्रिया को पूरा करने के उपरांत भारत के निवासियों को जारी किया जाता है। आधार संख्या 12 अंकों की एक रैंडम संख्या है। कोई भी व्यक्ति, जो भारत का निवासी है, किसी भी आयु का, बिना किसी लिंग भेद के आधार संख्या प्राप्ति हेतु स्वेच्छा से नामांकन करवा सकता है। नामांकन की प्रक्रिया पूरी तरह से मुफ्त है। व्यक्ति को नामांकन प्रक्रिया के दौरान न्यूनतम जनसांख्यिकीय और बायोमेट्रिक सूचना उपलब्ध करवानी होती है। आधार के लिए किसी भी व्यक्ति को केवल एक बार नामांकन करने की आवश्यकता होती है। बायोमेट्रिक डी-डुप्लीकेशन की प्रक्रिया के माध्यम से विशिष्टता प्राप्त की जाती है और केवल एक आधार ही सृजित किया जाता है।

जनसांख्यिकीय जानकारी: नाम, जन्म तिथि (सत्यापित) या आयु (घोषित), लिंग, पता, मोबाइल नंबर (वैकल्पिक) और ईमेल आईडी (वैकल्पिक), परिचयकर्ता-आधारित नामांकन के मामले में- परिचयकर्ता का नाम और परिचयकर्ता का आधार नंबर, प्रमुख के मामले में परिवार आधारित नामांकन- परिवार के मुखिया का नाम, संबंध और परिवार का आधार नंबर, बच्चे के नामांकन के मामले में माता-पिता किसी एक की नामांकन आईडी या आधार संख्या, प्रूफ़ ऑफ़ रिलेशनशिप (PoR) दस्तावेज़ , बायोमेट्रिक जानकारी: दस उंगलियों के निशान, दो आइरिस स्कैन, और चेहरे की तस्वीर ।

आधार नंबर एक किफायती ऑनलाइन तरीके से सत्यापन योग्य है। यह डुप्लिकेट और नकली पहचान को खत्म करने के लिए मजबूत है। विभिन्न सरकारी कल्याण योजनाओं ओर सेवाओं के प्रभावी वितरण, पारदर्शिता और सुशासन को बढ़ावा देने हेतु एक बुनियादी/प्राथमिक पहचान के रूप में इसे इस्तेमाल किया जा सकता है। यह दुनियाभर में अपनी तरह का एकमात्र कार्यक्रम है, जिसमें लोगों को एक बड़े पैमाने पर मुफ्त में डिजिटल और ऑनलाइन आईडी प्रदान की जा रही है। इसमें सेवा प्रदान करने के तरीके को बदलने की क्षमता है।

आधार संख्या जाति, धर्म, आय, स्वास्थ्य और भूगोल के आधार पर लोगों को नहीं दी जाती है। आधार संख्या पहचान का प्रमाण है, हालांकि, यह आधार नंबर धारक के संबंध में नागरिकता या अधिवास का कोई अधिकार प्रदान नहीं करता है।

आधार के द्वारा पहचान डिजिटल इंडिया के प्रमुख स्तंभों में से एक है। जिसमें देश के प्रत्येक निवासी को एक विशिष्ट पहचान प्रदान की जाती है। आधार कार्यक्रम पहले ही कई मील के पत्थर हासिल कर चुका है और दुनिया में अब तक का सबसे बड़ा बायोमेट्रिक्स आधारित पहचान प्रणाली है।

आधार अपने साथ विशिष्टता, प्रमाणीकरण, वित्तीय पता और ई-केवाईसी की विशेषताओं को अंतर्निहित किया हुआ है।जिसके कारण भारत सरकार केवल किसी निवासी के आधार नंबर का उपयोग करके विभिन्न सब्सिडी, लाभ और सेवाओं के वितरण को सीधे देश के निवासियों तक पहुंचने में सक्षम बनाती है।

3.9.1 आधार की विशेषताएं

I. **विशिष्टता**: इसे जनसांख्यिकीय और बायोमेट्रिक डी-डुप्लीकेशन की प्रक्रिया के माध्यम से प्राप्त किया जाता है। जनसांख्यिकीय और बायोमेट्रिक की जानकारी नामांकन की प्रक्रिया के दौरान एकत्र की जाती है। डी-डुप्लीकेशन प्रक्रिया में यह सत्यापित किया जाता है कि निवासी पहले से ही यूआईडीएआई डेटाबेस में है अथवा नहीं। नामांकन प्रक्रिया के दौरान एकत्र की गई निवासी की जनसांख्यिकीय/ बॉयोमीट्रिक जानकारी को यूआईडीएआई के डेटाबेस के रिकार्ड के साथ तुलना की जाती है। एक व्यक्ति को केवल एक बार आधार के लिए नामांकन करने की आवश्यकता है और डी-डुप्लीकेशन के बाद केवल एक आधार बनाया जाएगा। यदि कोई व्यक्ति एक से अधिक बार नामांकन करवाता है तो उसके बाद के नामांकन खारिज कर दिए जाएंगे।

II. **पोर्टेबिलिटी:** आधार देशव्यापी पोर्टेबिलिटी प्रदान करता है क्योंकि इसे ऑन-लाइन कहीं भी प्रमाणित किया जा सकता है। यह महत्वपूर्ण है क्योंकि लाखों भारतीय एक राज्य से दूसरे राज्य अथवा ग्रामीण क्षेत्र से शहरी केंद्रों आदि में जाते हैं।

III. **रेण्डम (यादृच्छिक) संख्या:** आधार संख्या रेंडमनंबर है जो किसी तार्किक या बुद्धिमत्ता से रहित (जैसे एक ही परिवार के लोगों के आधार नंबर क्रमवार होंगे, आधार में यह संभव नहीं) संख्या है। आधार नामांकन प्रक्रिया में जाति, धर्म, आय, स्वास्थ्य, भूगोल इत्यादि जैसे विवरण को संग्रहित नहीं किया जाता है।

IV. **केंद्रीकृत संग्रहण:** यूआईडी संरचना में नागरिकों के डेटा को केन्द्रीकृत रूप में संग्रहीत किया जाता है। देश में कहीं से भी उसका ऑनलाइन प्रमाणीकरण किया जा सकता है। एक दिन में 10 करोड प्रमाणीकरण करने के लिए आधार प्रमाणीकरण सेवा का गठन किया गया है।

V. **ओपन सोर्स टेक्नोलॉजी :** ओपन सोर्स आर्किटेक्चर विशिष्ट कंप्यूटर हार्डवेयर, विशिष्ट भंडारण, विशिष्ट ओ एस, विशिष्ट डेटाबेस विक्रेता या किसी विशिष्ट विक्रेता की प्रौद्योगिकियों पर निर्भरता को रोकता है। इस प्रकार के एप्लीकेशन खुला स्रोतया खुली प्रौद्योगिकी का उपयोग कर निर्मित करने से एक ही प्रकार के हार्डवेयर पर निर्भरता नहीं रहती है। अलग-अलग हार्डवेयर उपयोग करने से किसी एक विक्रेता को ही फायदा नहीं मिलता है।

3.9.2 आधार नामांकन

आधार नामांकन प्रक्रिया में आईडी युक्त पावती इकट्ठा करने से पूर्व नामांकन फार्म को भरना, जनसांख्यिकीय और बायोमेट्रिक डेटा को कैप्चर करना, पहचान और पते के प्रमाण दस्तावेज़ प्रस्तुत करना शामिल हैं। आधार नामांकन की मुख्य विशेषताएं है:-

- आधार नामांकन निशुल्क है।
- आप अपनी पहचान और पते के प्रमाण व दस्तावेज के साथ भारत में किसी भी प्राधिकृत्त नामांकन केंद्र पर जा सकते हैं।
- यू.आई.डी.ए.आई. पहचान और पते के अनेक प्रमाण दस्तावेजों को स्वीकार करता है जैसे इलैक्शन फोटो आई.डी. कार्ड, राशन कार्ड, पासपोर्ट और ड्राइविंग लाइसेंस पहचान और पते के कॉमन प्रमाण हैं।
- फोटो लगे पेन कार्ड और सरकारी पहचान पत्र पहचान के प्रमाण दस्तावेज के रूप में स्वीकार्य हैं। तीन महीने तक पुराना पानी-बिजली का बिल/टेलीफोन बिल जैसे दस्तावेज पते के प्रमाण के रूप में स्वीकार्य हैं।
- यदि आपके पास उपर्युक्त कॉमन प्रमाण न हो तो राजपत्रित अधिकारी/तहसीलदार द्वारा लैटर-हैड पर जारी प्रमाण-पत्र, पहचान का प्रमाण माना जा सकता है बशर्ते उस पर व्यक्ति का फोटो भी लगा हो। पते के प्रमाण के तौर पर एम.पी./एम.एल.ए./राजपत्रित अधिकारी/तहसीलदार द्वारा लैटर-हैड पर या ग्राम पंचायत मुखिया या उसके समकक्ष प्राधिकारी द्वारा (ग्रामीण क्षेत्र के मामले में) जारी प्रमाण पत्र को पते का प्रमाण दस्तावेज माना जा सकता है बशर्ते उस पर व्यक्ति का फोटो भी लगा हुआ हो।
- यदि, परिवार में किसी सदस्य के पास अपना खुद का कोई मान्य दस्तावेज नहीं है तो वह भी आधार नामांकन करवा सकता है, यदि उसका नाम परिवार के अन्य सदस्य के रूप में मान्य पात्रता/हकदारी दस्तावेज़ में दर्ज है। ऐसे मामले में, परिवार के मुखिया का नामांकन सबसे पहले होना चाहिए जिसके पास अपनी पहचान और पते के प्रमाण के दस्तावेज होने चाहिए। उसके बाद परिवार का मुखिया अपने परिवार के अन्य सदस्यों के लिए नामांकन के समय परिचयदाता बन सकता है जिसके आधार पर उसके परिवार के सदस्यों का नामांकन

हो सकता है। यू.आई.डी.ए.आई, मुखिया के साथ संबंध के रूप में कई दस्तावेजों को मान्यता देता है।

- जहां कहीं निवासी के पास दस्तावेज न हों तो वह नामांकन केंद्र पर उपलब्ध परिचयदाता की मदद ले सकता है। परिचयदाता रजिस्ट्रार द्वारा निर्धारित किए जाते हैं।
- पूरी प्रक्रिया के तहत कृपया नामांकन केंद्र पर नामांकन फार्म में अपना वैयक्तिक विवरण भरें। नामांकन प्रक्रिया में आपका फोटो, फिंगर-प्रिंट और आंखों की पुतलियों के निशान भी लिए जाएंगे। नामांकन प्रक्रिया के दौरान स्वयं द्वारा उपलब्ध करवाई गई जानकारी की समीक्षा कर आप नामांकन के दौरान ही उसमें सुधार भी करवा सकते हैं। नामांकन के दौरान ही कैप्चर की गई जानकारी सहित एक नामांकन नम्बर के साथ पावती पर्ची आपको दे दी जाएगी। नामांकन के 96 घंटों के भीतर, पावती पर्ची सहित नामांकन केंद्र पर जा कर नामांकन डेटा में कोई भी सुधार किया जा सकता है।आधार कार्ड आपके पते पर डाक विभाग द्वारा पहुंचाया जाता है, अथवा यूआईडीएआई की वेबसाइट से इसे डाउनलोड किया जा सकता है।

3.9.3 आधार कार्ड का उपयोग

भारत सरकार समाज के गरीब और कमजोर वर्गों की ओर केंद्रित कई सामाजिक कल्याण योजनाओं को रुपया देती है। आधार के माध्यम से पारदर्शी ढंग से सरकार उनके वितरण तंत्र को सुव्यवस्थित कर सकता है जिस से सही व्यक्ति को फायदा मिले।

यूआईडीएआई जनसांख्यिकीय और बायोमीट्रिक विशेषज्ञताओं की डी-डुप्लीकेटिंग के पश्चात निवासियों के लिए आधार नंबर जारी करता है। डुप्लिकेट को समाप्त करने में सक्षम है और यह सरकार को सही लाभार्थियों का डाटा प्रदान करता है। प्रत्यक्ष लाभ कार्यक्रमों को सक्षम बनाता है, और सरकारी विभागों/ सेवा प्रदाताओं को अपनी योजनाओं के समन्वय और अनुकूलन की अनुमति देता है। आधार लाभार्थियों को सत्यापित करने और लाभ के लक्षित वितरण को सुनिश्चित करने के लिए कार्यान्वयन एजेंसियों को सक्षम करता है।

कल्याणकारी कार्यक्रम जहाँ सेवा वितरण से पहले लाभार्थियों की पुष्टि की जानी आवश्यक है, वहां यह सुनिश्चित करना होगा कि सेवाएं केवल संबंधित लाभार्थियों तक ही पहुंचाई जा सकें। उदाहरणों में सार्वजनिक वितरण प्रणाली (पीडीएस) के लाभार्थियों को रियायती भोजन और केरोसिन वितरण, महात्मा गांधी राष्ट्रीय ग्रामीण रोजगार गारंटी योजना (MGNREGS) के लाभार्थियों की उपस्थिति आदि शामिल हैं।

सेवा वितरण तंत्र के बारे में सटीक और पारदर्शी जानकारी प्रदान करने के साथ, सरकार वितरण प्रणालियों में सुधार कर सकती है। सेवा वितरण नेटवर्क में शामिल मानव संसाधनों का बेहतर उपयोग कर सकती है।

आधार प्रणाली नागरिकों को देश भर में ऑनलाईन पहचान सत्यापन का एकमात्र स्त्रोत प्रदान करती है। नागरिकों का एक बार नामांकन हो जाने पर इलेक्ट्रॉनिक माध्यमों या ऑफ़लाइन सत्यापन के माध्यम से आधार संख्या का उपयोग अपनी पहचान को सत्यापित और प्रमाणित करने के लिए कर सकते हैं। यह सेवाओं, सब्सिडी तथा अन्य सरकारी लाभ देते समय हर बार दस्तावेजों के परीक्षण की जटिल प्रक्रिया को समाप्त करता है।यह व्यक्ति का ऐसा पहचान पत्र है जो ऑनलाईन आधार प्रमाणीकरण के माध्यम से सत्यापित किया जा सकता है। देश में कहीं भी जाने पर उसके साथ उपलब्ध होता है और देश भर में कहीं भी रहते हुए योजनाओं का लाभ लेने में सक्षम बनाता है।

3.10 उमंग (UMANG)

पिछले कुछ वर्षों से भारत सरकार 'डिजिटल इंडिया' आंदोलन को बहुत बढ़ावा दिया है।डिजिटलीकरण के अपने ही लाभ हैं इसमें हर प्रक्रिया तीव्रता के साथ पारदर्शिता के साथ और किसी भी जगह पर रहते हुए की जा सकती है।अतः भारत सरकार आगामी वर्षों में भारत को पूरी तरह से डिजिटल बनाने की दिशा में काम कर रही है। यही कारण है कि भारत सरकार सभी से ऑनलाइन माध्यम से हर कार्य को करने के लिए भी कह रही है। उसी के अनुरूप, उमंग भी सरकार की डिजिटल इंडिया कार्यक्रम को बढ़ावा देने के लिए एक ऐसी पहल है।

ई-गवर्नेंस बनाने के लिए उमंग (UMANG) यूनिफ़ाइड मोबाइल एप्लीकेशन (mobile app) फ़ॉर न्यू एज गवर्नेंस की परिकल्पना की गई है। इसे भारत में मोबाइल गवर्नेंस चलाने के लिए इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय और राष्ट्रीय ई-गवर्नेंस डिवीजन द्वारा विकसित किया गया है। यह एप्प एंड्रॉइड, आईओएस, विंडोज डिवाइस उपयोगकर्ताओं और फीचर फोन उपयोगकर्ताओं के लिए उपलब्ध है। इस ऑल-इन-वन ऐप का उपयोग करके आप केवल माउस क्लिक द्वारा सभी सरकारी संबंधित सेवाओं का प्रदर्शन कर सकते हैं। यूजर्स 12 अलग-अलग भाषाओं में ऐप को एक्सेस कर कर सकते हैं।

उमंग सभी भारतीय नागरिकों को अखिल भारतीय ई-सरकारी सेवाओं जो कि केंद्र से लेकर स्थानीय सरकारी निकायों और अन्य नागरिक केंद्रित सेवाओं तक पहुंचने के लिए एक मंच प्रदान करता है।

उमंग का उद्देश्य केंद्रीय और राज्य सरकारी विभागों, स्थानीय निकायों और निजी संगठनों द्वारा दी जाने वाली प्रमुख सेवाएं प्रदान करना है। यह एक एकीकृत दृष्टिकोण प्रदान करता है जहां नागरिकों को एक से अधिक सरकारी सेवाओं का लाभ उठाने के लिए केवल एक ऐप इनस्टॉल करना होगा।

उमंग सेवा को कई चैनल जैसे मोबाइल ऐप, वेब, आईवीआर और एसएमएस पर उपलब्ध कराया गया है जिसका उपयोग स्मार्टफोन, फीचर फोन, टैबलेट और डेस्कटॉप के माध्यम से किया जा सकता है। आज की जीवन शैली में सुविधा जोड़ने के विचार से उमंग को बनाया गया है। वर्तमान में इंटरनेट और स्मार्ट फोनों का उपयोग बहुत बढ़ा है।इसलिए इंटरनेट माध्यम से जिस तरह एक भारतीय नागरिक आज सरकारी सेवाओं का लाभ उठाते हैं उमंग उसमे क्रन्तिकारी बदलाव लाएगा।

3.10.1 प्रमुख विशेषताऐं

एकाधिक चैनल जैसे कि स्मार्टफोन, डेस्कटॉप और टेबलेट पर उमंग का उपयोग किया जा सकता है। उमंग का मल्टीमीडिया इंटरफ़ेस सशक्त है जो अधिकाधिक उपयोगिता और बेहतर उपयोगकर्ता अनुभव पर केन्द्रित है।

उमंग ऐप सभी पैन इंडिया ई-गवर्नेंस सेवाओं को केंद्रीय से लेकर स्थानीय सरकारी निकायों और अन्य नागरिक-केंद्रित सेवाओं जैसे – आधार और डिजीलॉकर को एक मोबाइल ऐप पर प्रदान करता है। वर्तमान में, उमंग ऐप 12 श्रेणियों में सेवाएं प्रदान करता है जिसमें शामिल हैं – कृषि, शिक्षा, रोजगार और कौशल, ऊर्जा, वित्त, स्वास्थ्य, आवास, पुलिस, लोक शिकायत, राजस्व, परिवहन और उपयोगिता। हालांकि, आगामी दिनों में, ऐप विभिन्न अन्य सेवाओं जैसे कि PayGov और अधिक के साथ एकीकरण प्रदान करेगा।

अब एक मोबाइल ऐप के द्वारा सरकार की विभिन्न सेवाओं उपयोग कर सकते हैं। उमंग एक एकीकृत मंच प्रदान करता है जहाँ से उपयोगकर्ता विभिन्न सरकारी सेवाओं (केंद्रीय, राज्य और क्षेत्रीय) का उपयोग कर सकता है। इसमें वर्तमान में 643 सेवाएं, 117 विभाग और 23 प्रदेश जुड़े हुए हैं।

इस ऐप में, एक 'Service/सेवा' विकल्प है। आप किसी भी सरकार से संबंधित सेवाओं का लाभ उठाने के लिए विकल्प पर क्लिक कर सकते हैं। इसके लिए आपको श्रेणी का चयन करने की आवश्यकता है फिर Service type का चयन करें– जिसका अर्थ है कि क्या आपको केंद्रीय या क्षेत्रीय सेवा की आवश्यकता है, वह नाम लिखें जो आपके पास है, और फिर वर्णानुक्रम के आधार पर परिणाम को क्रमबद्ध करने के लिए विकल्प पर क्लिक कर सकते हैं। जिसके बाद, उमंग आपकी श्रेणी के चयन के आधार पर सर्वश्रेष्ठ परिणाम प्रदर्शित करेगी।

उपयोगकर्ता के सुविधा के लिए उमंग सप्ताह के सभी दिन प्रातः 10 से सांय 6 बजे तकग्राहक सहायता प्रदान करता है।

3.10.2 उमंग ऐप को कैसे इंस्टॉल करें

उमंग वेबसाइट पर डाउनलोड विकल्प उपलब्ध है, जिस पर क्लिक करने पर "क्यू आर QR कोड स्कैन करने के लिए अपने मोबाइल डिवाइस का उपयोग करें और UMANG ऐप डाउनलोड करें" का संदेश आता है।

- उमंग ऐप को दूसरे तरीके से इंस्टॉल करने के लिए एंड्रॉइड फोन पर उमंग ऐप डाउनलोड करने के लिए, Google Play Store पर जाएं और Umang टाइप करें। इसके बाद Install पर क्लिक करें और ऐप डाउनलोड होने की प्रतीक्षा करें। Apple उपयोगकर्ताओं के लिए, ऐप को ऐप्पल ऐप स्टोर से इंस्टॉल किया जा सकता है।
- ऐप को खोलें और उमंग ऐप के साथ एक अकाउंट बनाने के लिए नाम, आयु, लिंग, फोन नंबर और आधार विवरण आदि जानकारी दर्ज करें। आप बाद में जानकारी में सुधार भी कर सकते हैं।
- आप अपने आधार नंबर को ऐप और अन्य सोशल मीडिया अकाउंट से भी लिंक कर सकते हैं|
- उमंग अकाउंट बनाने के बाद, ऐप का उपयोग करने के लिए Service Section पर जाएं और सेवाओं और श्रेणियों के माध्यम से ब्राउज़ करने के लिए Filter सॉर्ट एंड फ़िल्टर अनुभाग पर जा सकते हैं|
- विशेष सेवाओं की तलाश के लिए सर्च विकल्प पर जाएं|

3.11 डिजिटल लॉकर या डिजिलॉकर (Digital Locker)

डिजिटल लॉकर या डिजिलॉकर या ई-लॉकर डिजिटल इंडिया कार्यक्रम के तहत इलेक्ट्रॉनिक्स और आईटी मंत्रालय की एक प्रमुख पहल है। अंग्रेजी भाषा के शब्दों डिजिटल लॉकर का हिंदी में शाब्दिक अर्थ है अंकीय तिजोरी या इलेक्ट्रॉनिक तिजोरी जो दस्तावेजों की छायाप्रति सुरक्षित रखने के काम आती है। डिजीलॉकर का उद्देश्य नागरिकों के पैन कार्ड, पासपोर्ट, मार्कशीट और डिग्री प्रमाणपत्र जैसे अपने महत्वपूर्ण दस्तावेजों को डिजिटल रूप से संग्रहीत करके नागरिक के 'डिजिटल सशक्तिकरण' के लिए है। डिजीलॉकर प्रणाली में जारी दस्तावेजों को मूल भौतिक दस्तावेजों के साथ सूचना प्रौद्योगिकी के नियम 9A (डिजिटल लॉकर सुविधाएं प्रदान करने वाले मध्यस्थों के संरक्षण और प्रतिधारण) के अनुसार माना जाता है। नियम, 2016 8 फरवरी, 2017 को अधिसूचित जी.एस.आर. 711(ई)।

डिजीलॉकर भारत सरकार का एक मोबाइल ऐप और वेबसाइट है जहाँ आप अपने दस्तावेज़ जैसे जन्म प्रमाण पत्र, पैन कार्ड, पासपोर्ट, शैक्षणिक प्रमाण पत्र जैसे अहम दस्तावेजों को ऑनलाइन सुरक्षित रख सकते हैं। आपको अपने सभी दस्तावेज़ों के लिए 1GB स्थान मुफ्त में

दिया जाता है। मूल रूप से यह एक भौतिक लॉकर की तरह है जहां आप अपने आभूषण और दस्तावेजों को संग्रहित करते हैं लेकिन यह लॉकर डिजिटल है और डिजिटल जानकारी संग्रहित करताहै। इसका उपयोग करने से यह सहूलियत है कि आपको अपने दस्तावेज हर समय साथ में लेकर जाने की आवश्यकता नहीं होती।जब भी किसी कार्य हेतु इन दस्तावेजों की आवश्यकता हो आप अपने डीजी लॉकर से इसे ऑनलाइन उपलब्ध करा सकते हैं।

यह सुविधा पाने के लिए बस उपयोगकर्ता के पास भारत सरकार द्वारा प्रद्दत आधार कार्ड होना चाहिए। अपना आधार अंक डाल कर उपयोगकर्ता अपना डिजिलॉकर खाता खोल सकते हैं और अपने जरूरी दस्तावेज़ सुरक्षित रख सकते हैं। आधार अंक की अनिवार्यता होने की वजह से यह तय किया गया है कि इस सरकारी सुविधा का लाभ सिर्फ भारतीय नागरिक ही ले सकें और जिसका भी खाता हो, उसके बारे में सभी जानकारी सरकार के पास हो। कोई भी ठग, झूठा और अप्रमाणित व्यक्ति इसका उपयोग ना कर सके इसके लिये आधार कार्ड होने की अनिवार्यता बेहद आवश्यक है, क्युंकि आधार कार्ड भी भारत सरकार द्वारा पूरी जाँच पड़ताल के बाद ही जारी किया जाता है। इस तरह से इस प्रणाली के दुरुपयोग की संभावना बेहद कम हो जाती है। इस सुविधा की खास बात ये हैं कि एक बार लॉकर में अपने दस्तावेज अपलोड करने के बाद आप कहीं भी अपने प्रमाणपत्र की मूलप्रति के स्थान पर अपने डिज़िलॉकर की वेब कड़ी (यूआरएल) दे सकेंगे। अब बार-बार कागजों का प्रयोग नहीं करना होगा।

डिजीलॉकर के लिए साइन अप करना आसान है – आपको बस अपना मोबाइल नंबर चाहिए। आपका मोबाइल नंबर एक OTP (वन-टाइम पासवर्ड) भेजकर प्रमाणित किया जाएगा, जिसके बाद उपयोगकर्ता नाम और पासवर्ड का चयन करेंगा। इससे आपका डिजीलॉकर अकाउंट बन जाएगा।आपका डिजीलॉकर खाता सफलतापूर्वक बनने के बाद, आप अतिरिक्त सेवाओं का लाभ उठाने के लिए स्वेच्छा से अपना आधार नंबर (UIDAI द्वारा जारी किया गया) प्रदान कर सकते हैं।

3.11.1 डिजीलॉकर के लाभ

I. नागरिकों को लाभ

डिजिटल लॉकर की सबसे बड़ी सुविधा ये हैं कि उपयोगकर्ता कहीं से भी और कभी भी अपने दस्तावेजों को इसके जरिए जमा कर सकते हैं। उन्हें निशुल्क सुरक्षित रख सकते हैं, किसी भी सरकारी काम जहाँ दस्तावेजों की प्रमाणित प्रतियाँ देना अनिवार्य होता है वहाँ मूलप्रति या उसकी छायाप्रति देने की बज़ाय अपने लॉकर का यूआरएल दे सकते हैं। अधिकारी वहाँ से इन प्रमाणपत्रों को देख सकते हैं। इस तरह से भारतीय नागरिकों को हर जगह अपने ज़रूरी दस्तावेज लेकर घूमने की जरूरत नहीं है। यह पूरी तरह से सुरक्षित, सरल और पारदर्शी प्रोसेस है। इसमें नकली दस्तावेजों से बचा जा सकता है।

II. एजेंसियों को लाभ

कम प्रशासनिक ओवरहेड: कागज रहित शासन की अवधारणा पर लक्षित। यह कागज के उपयोग को कम करके और सत्यापन प्रक्रिया को कम करके प्रशासनिक ओवरहेड को कम करता है।

डिजिटल परिवर्तन: विश्वसनीय जारी किए गए दस्तावेज़ प्रदान करता है। डिजीलॉकर के माध्यम से जारी किए गए दस्तावेज़ सीधे जारी करने वाली एजेंसी से प्राप्त किए जाते हैं। उदाहरण के तौर पर आपकी दसवीं कक्षा का सर्टिफिकेट सीधे ही संबंधित बोर्ड से प्राप्त होता है। इसलिए जहां भी इस सर्टिफिकेट की आवश्यकता हो डिजीलॉकर के सर्टिफिकेट को उसके यूआरएल से प्राप्त किया जा सकता है और इसे विश्वसनीय दस्तावेज माना जाता है। सुरक्षित दस्तावेज़ गेटवे: नागरिक की सहमति के साथ विश्वसनीय जारीकर्ता और विश्वसनीय अनुरोधकर्ता सत्यापनकर्ता के बीच भुगतान गेटवे जैसे एक सुरक्षित दस्तावेज़ विनिमय प्लेटफ़ॉर्म के रूप में कार्य करता है।

वास्तविक समय सत्यापन उपयोगकर्ता सहमति प्राप्त करने के बाद जारीकर्ता से सीधे डेटा सत्यापित करने के लिए सरकारी एजेंसियों को सक्षम करने के लिए एक सत्यापन मॉड्यूल प्रदान करता है।

3.12 डिजिटल लाइब्रेरी (Digital Library)

आपको पता ही होगा की हमारा देश बहुत ही तेजी से डिजिटल इंडिया बनता जा रहा हैं। सरकार दिन प्रतिदिन नए नए एप्प, योजनाये, जनता के लिए सुविधाए लेकर आ रही हैं ताकि लोगो की समस्याओं को कम किया सके और समय की बचत भी हो सके। जैसे- डिजिटल लॉकर, डिजिटल भुगतान, डिजिटल हस्ताक्षर, डिजिटल लाइब्रेरी।

पुस्तकालय ज्ञान के भंडार होते हैं क्योंकि पुस्तकें और ज्ञान प्राप्त करने के अन्य संसाधन मुद्रित अर्थात प्रिंटेड रूप में।लाइब्रेरी के उपयोग से व्यक्ति किताबों को खरीदे बिना ही लाइब्रेरी की सदस्यता लेकर उपयोग कर सकते हैं। डिजिटल प्रौद्योगिकी और इंटरनेट कनेक्टिवटी के विकास और प्रचुर उपयोग के साथ पुस्तकालय का परिदृश्य भी तेजी से बदल रहा है। डिजिटल प्रौद्योगिकी, इंटरनेट कनेक्टिवटी और भौतिक रूप में सूचना सामग्री के परिणाम स्वरूप डिजिटल पुस्तकालय तैयार किए जा सकते हैं। पुस्तकें कागज की बजाय डिजिटल संचिका के रूप में होती हैं जिन्हें कम्प्यूटर, मोबाइल एवं अन्य डिजिटल यंत्रों पर पढ़ा जा सकता है। इन्हें इंटरनेट पर भी छापा, बाँटा या पढ़ा जा सकता है। कंटेंट को स्थानीय रूप से स्टोर किया जा सकता है, या दूरस्थ रूप से एक्सेस किया जा सकता है।

एक डिजिटल लाइब्रेरी, प्रिंट या माइक्रोफ़ॉर्म जैसे मीडिया के अन्य रूपों के विपरीत, लाइब्रेरी का एक विशेष रूप है जो डिजिटल संपत्ति का एक संग्रह शामिल करता है। ऐसी डिजिटल वस्तुएं विजुअल मटेरियल, टेक्स्ट, ऑडियो या वीडियो इलेक्ट्रॉनिक मीडिया के रूप में हो सकती हैं जैसा कि यह एक पुस्तकालय है, इसमें मीडिया या फ़ाइलों को व्यवस्थित करने, स्टोर करने और पुनर्प्राप्त करने की विशेषताएं भी हैं जो संग्रह बनाती हैं। दूर से स्टोर होने पर डिजिटल लाइब्रेरी में कंटेंट को स्थानीय रूप से स्टोर या नेटवर्क के माध्यम से एक्सेस किया जा सकता है।

डिजिटल लाइब्रेरी में डिजिटल रिसोर्स का एक संग्रह होता है जो केवल डिजिटल रूप में मौजूद होते हैं, या उन्हें दूसरे रूप से डिजिटल में परिवर्तित किया जाता है। है। ऐसी डिजिटल वस्तुएं विजुअल मटेरियल, टेक्स्ट, ऑडियो या वीडियो इलेक्ट्रॉनिक मीडिया के रूप में हो सकती हैं। इन रिसोर्स को आम तौर पर फोर्मेट्स की एक विस्तृत श्रृंखला में स्टोर किया जाता है और

कंप्यूटर नेटवर्क पर उपयोगकर्ताओं द्वारा एक्सेस किया जा सकता है। इस तरह की लाइब्रेरी को रोज अपडेट किया जा सकता है और उपयोगकर्ताओं द्वारा तुरंत एक्सेस किया जा सकता है।

3.12.1 डिजिटल लाइब्रेरी के फायदे

दौड़ती-भागती इस जिंदगी में लोगों के पास समय की कमी है। ऐसे में ऑनलाइन लाइब्रेरी की उपयोगिता ज्यादा बढ़ जती है। लोगों के पास यह सुविधा होती है कि वह ऑनलाइन किताबें पढ़ सकें। इन ऑनलाइन लाइब्रेरियों में सिर्फ विषय की पुस्तकें ही नहीं होती बल्कि उपन्यास, पत्रिका आदि भी पढ़ने के लिए उपलब्ध होते है।

- डिजिटल लाइब्रेरी एक विशेष स्थान तक ही सीमित नहीं है। इसके लिए उन्हें लाइब्रेरी और विभिन्न जगहों के चक्कर नहीं लगाने पड़ते। उपयोगकर्ता इंटरनेट का उपयोग करके कहीं से भी अपनी जानकारी प्राप्त कर सकता है।
- किसी भी पुस्तकालय का एक निश्चित समय होता है लेकिन डिजिटल लाइब्रेरी को कभी भी दिन के 24 घंटे और साल के 365 दिन उपयोग किया जा सकता है।
- एक ही रिसोर्स का उपयोग एक साथ एक ही समय में कई उपयोगकर्ताओं द्वारा किया जा सकता है।
- डिजिटल लाइब्रेरी एक अधिक संरचित तरीके से बहुत समृद्ध सामग्री तक पहुंच प्रदान करती है यानी हम कैटलॉग से किसी विशेष पुस्तक तक और फिर एक विशेष अध्याय तक पहुंच सकते हैं। साथ ही किसी विषय विशेष के बारे में विस्तृत जानकारी मिल जाती है।
- बाजार में आई नई किताबों के बारे में जानकारी तुरंत मिल जाती है। मनपसंद लेखक की कौन सी नई किताब आई, इसके बारे में तुरंत पता लग जाता है।
- उपयोगकर्ता पूरे संग्रह के शब्द या वाक्यांश के लिए किसी भी खोज शब्द का उपयोग करने में सक्षम है।
- गुणवत्ता में किसी भी गिरावट के बिना मूल की एक सटीक कॉपी किसी भी समय बनाई जा सकती है।

- पारंपरिक लाइब्रेरी स्टोरेज स्पेस द्वारा सीमित हैं। डिजिटल लाइब्रेरी में बहुत अधिक जानकारी स्टोर करने की क्षमता होती है, क्योकि डिजिटल जानकारी के लिए उन्हें रखने के लिए बहुत कम फिजिकल स्थान की आवश्यकता होती है
- कई ऐसी ऑनलाइन लाइब्रेरी हैं जिसमें आप किताबों की समीक्षा लिख सकते हैं। इससे आपको कौन सी किताब खरीदनी है, इसके बारे में अंदाज लग जता है।
- कई ऑनलाइन लाइब्रेरी में आपको किसी विषय के बारे में जानकारी एकत्रित करने के लिए साइटों के रेफरेंस देती हैं। साथ ही इन पर विषय और टॉपिक के अनुसार उस विषय के लेखकों की किताबों के नाम दिए जाते हैं। जिससे आपको विभिन्न लोगों से इस बात की पूछताछ नहीं करनी पड़ती कि अमुक विषय के लिए कौन सी किताब पढ़ी जाए।

3.13 साइबर अपराध/ क्राइम (Cyber Crime)

नेटवर्क और इंटरनेट के उपयोग से पिछले दो दशकों में सभी क्षेत्रों में बहुत बदलाव आया है। व्यक्तिगत, व्यवसायिक हर तरह की गतिविधियों में सूचना प्रौद्योगिकी महत्वपूर्ण होती चली गई है। आपसी संवाद, अध्ययन, सरकारी कामकाज, व्यक्तिगत व्यवसाय इन सभी क्षेत्रों में व्यापक परिवर्तन है। इंटरनेट के उपयोग ने विश्व स्तर का एक नेटवर्क स्थापित किया है, इस नेटवर्क पर प्रौद्योगिकी के उपयोग से सभी गतिविधियां जैसे संचार, अध्ययन, व्यवसाय आदि किए जाते हैं। यह सभी गतिविधियां संभव है क्योंकि सूचनाओं का एक भंडारण और इनका विश्लेषण करने वाली प्रौद्योगिकी उपलब्ध है। यह भंडारण स्थानीय नहीं है बल्कि एक वर्चुअल स्पेस है जो सुरक्षित भंडारण और आवश्यक सूचनाओं को इस भंडार से प्राप्त करने में सहायता करती है,और सभी को इसके उपयोग के समान अवसर प्रदान करता है। इसे ही साइबर स्पेस कहा जा सकता है। वह वर्चुअल स्पेस जिसमें सूचना प्रौद्योगिकी के उपयोग से संचार की क्रियाएं होती हैं को 'साइबर स्पेस' कहा जाता है। साइबरस्पेस कंप्यूटर नेटवर्क का इलेक्ट्रॉनिक माध्यम है, जिसमें ऑनलाइन संचार होता है और जहां व्यक्ति बातचीत कर सकते हैं, विचारों का आदान-प्रदान कर सकते हैं, जानकारी साझा कर सकते हैं। दुनिया के विभिन्न हिस्सों में लोग कई तरह के उपकरणों जैसे सेलफोन, टैबलेट या कंप्यूटर पर वास्तविक समय में संचार कर सकते हैं।

कुछ सेकंड में, एक फोटो, वीडियो, पाठ संदेश, या ईमेल जो किसी एकल व्यक्ति द्वारा साझा किया जाता है, सैकड़ों या हजारों उपयोगकर्ताओं द्वारा देखा जा सकता है और वायरल हो सकता है।

साइबर क्राइम, साइबर स्पेस में इंटरनेट के माध्यम का उपयोग करके आपराधिक इरादे के साथ की गई सभी गतिविधियों को संदर्भित करता है। इंटरनेट पर उपलब्ध कोई भी सामग्री, किसी की व्यक्तिगत जानकारी, फिल्म, ऑडियो, वीडियो ई-बुक्स यह सभी साइबरस्पेस के संग्रहण की सामग्रियां हैं जो उपयोगकर्ताओं के आवश्यकता अनुसार उन्हें उपलब्ध होती हैं। इंटरनेट पर डेटा भेजने की यह क्षमता के फायदे और लाभ के साथ साथ कुछ खतरे भी जुड़े हैं। साइबरस्पेस पर उपलब्ध सामग्री को अपराधिक सोच के साथ उपयोग करने को साइबर क्राइम कहा जा सकता है। यह किसी की व्यक्तिगत जानकारी चुराना, इंटरनेट माध्यम से धन के लेन-देन में गड़बड़ करना, अनावश्यक जानकारी पहुंचाना या प्राप्त करना,किसी की व्यक्तिगत गतिविधि पर नजर रखना या नकल करना जैसी कोई भी गतिविधि हो सकती है। साइबर अपराधों में वे अपराध शामिल हैं जो कंप्यूटरों के लिए विशिष्ट हैं, जैसे हैकिंग, ई-मेल स्पैमिंग, साथ ही चोरी, धोखाधड़ी और जबरन वसूली जैसे कंप्यूटर का उपयोग करके किए गए पारंपरिक अपराध, जो नए माध्यम के विकास के साथ विकसित हुई हैं।

साइबर अपराध कंप्यूटर, नेटवर्क और इंटरनेट के माध्यम से किए जाने वाले किसी भी आपराधिक कार्य को शामिल करता है। यह किसी भी डिजिटल डिवाइस (पीसी, नोटबुक, स्मार्ट टीवी, टैबलेट, स्मार्टफोन, होम इलेक्ट्रॉनिक सिस्टम आदि) को प्रभावित कर सकता है। उदाहरण के लिए, जब कंप्यूटर और इंटरनेट के माध्यम से गैरकानूनी गतिविधियों को अंजाम दिया जाता है तो घृणित अपराध, टेलीमार्केटिंग और इंटरनेट धोखाधड़ी, पहचान की चोरी, और क्रेडिट कार्ड खाता चोरी साइबर अपराध माना जाता है। साइबर अपराध में हैकर्स पेशेवर चोर, अपराधी गिरोह, असंतुष्ट कर्मचारियों, पेशेवर प्रतियोगिता कार्यकर्ता कोई भी हो सकता है।

साइबर अपराध वैश्विक चरित्र हैं। साइबर अपराधों की इस प्रकृति के कारण, कोई भी साइबर अपराधी विश्व स्तर पर किसी भी जगह से अपराध करता है। उसके खिलाफ अपराध करने के लिए पीड़ित स्थान पर जाने की आवश्यकता नहीं है।

3.13.1 साइबर अपराध वर्गीकरण

विभिन्न प्रकार के साइबर अपराध को परिभाषित करने और इंटरनेट और साइबर स्पेस के सुरक्षित उपयोग के लिए हमें चार प्रमुख साइबर अपराध वर्गीकरणों से परिचित होना चाहिए।

- **व्यक्ति के खिलाफ अपराध -** व्यक्ति के खिलाफ अपराध वह है जो किसी भी व्यक्ति या उनके व्यक्तिगत कार्यों को सीधे प्रभावित करता है। यह ऐसे साइबर अपराधों को संदर्भित करता है जो किसी व्यक्ति की इच्छा के खिलाफ किए जाते हैं। इस प्रकार के साइबर अपराध के उदाहरणों में शामिल हैं, (लेकिन यह तक सीमित नहीं हैं) कंप्यूटर सिस्टम पर अनधिकृत नियंत्रण/ पहुंच, फ़िशिंग, ईमेल उत्पीड़न, साइबर बुलिंग, बाल यातना और अवैध वयस्क सामग्री फैलाना। इस तरह के साइबर अपराध व्यक्ति के व्यक्तित्व को प्रभावित करते हैं और गैरकानूनी तरीके से युवा पीढ़ी के मनोविज्ञान को प्रभावित करते हैं।
- **समाज के खिलाफ साइबर अपराध -** वे साइबर अपराध जो बड़े पैमाने पर समाज हित को प्रभावित करते हैं, उन्हें समाज के खिलाफ साइबर अपराधों के रूप में जाना जाता है। ये साइबर स्पेस को माध्यम बनाकर किए जाने वाले गैरकानूनी कार्य हैं जो बड़ी संख्या में लोगों को स्वचालित रूप से प्रभावित करते हैं। इस प्रकार के अपराधों का मुख्य लक्ष्य सरकारी नियमों का उल्लंघन करने वाली व्यवसायिक गतिविधियां है। उदाहरण के लिए सार्वजनिक संगठनों के खिलाफ वित्तीय अपराध, अवैध उत्पाद बेचना, तस्करी, ऑनलाइन जुआ, जालसाजी आदि।
- **कंपनियों / संगठनों के खिलाफ साइबर अपराध -** यह आज साइबर अपराध का आम प्रकार है। जब किसी कंपनी की ऑनलाइन उपस्थिति या उसके किसी भी उत्पाद को हैक कर लिया जाता है, तो यह एक गंभीर समस्या बन जाती है जिसके परिणामस्वरूप कंपनी के साथ-साथ उनके कर्मचारियों, सहयोगियों और ग्राहकों को भी बड़ी संख्या में परिणाम भुगतने पड़ सकते हैं।
- **सरकार के खिलाफ साइबर अपराध -** यह दुनिया के सबसे बुरे प्रकारों में से एक साइबर अपराध है। इसे साइबर आतंकवाद के रूप में भी जाना जाता है, और इसमें सरकारी वेबसाइट पर साइबर हमला, सरकारी सिस्टम और नेटवर्क को तोड़ने, सैन्य वेबसाइटों

को ख़राब करने और बंद करने और प्रचार प्रसार जैसी गतिविधियाँ शामिल हैं। ये अपराध किसी विशेष देश के लोगों में झूठी सूचना प्रसारित करके आतंक फैलाने के उद्देश्य से किए जाते हैं।

3.13.2 साइबर अपराध के विभिन्न प्रकार

साइबर अपराध विभिन्न तरीकों से हमला कर सकता है। यह नेटवर्क के खतरों की पूरी सूची नहीं है, यहां कुछ सबसे सामान्य तरीके हैं जो हर दिन सिस्टम और नेटवर्क पर हमला करते हैं।

I. **मालवेयर (Malware)**

मालवेयर से अर्थ है ऐसे सॉफ्टवेयर जो दुर्भावना से निर्मित किए गए हो। वायरस, रेनसेमवेयर, स्पाइवेयर सामूहिक रूप से मालवेयर की श्रेणी में ही आते हैं । ये अंग्रेज़ी नाम मैलेशियस सॉफ्टवेयर का संक्षिप्त रूप है। मालवेयर, सॉफ्टवेयर का एक फाइल या कोड हो सकता है जो उपकरणों को हानि पहुंचाने, डेटा चोरी करने और आमतौर पर गड़बड़ी पैदा करने के इरादे से बनाए जाते हैं इनका उपयोग कंप्यूटर पर किसी की पहचान चोरी करने या गोपनीय जानकारी में सेंध लगाने के लिए किया जाता है। कई मालवेयर अवांछनीय ईमेल भेजने और कंप्यूटर पर गोपनीय और अश्लील संदेश भेजने और प्राप्त करने का काम करते हैं।

यह ऐसे सॉफ्टवेर है जो कंप्यूटर के उपयोग करते समय व्यक्तिगत या डेटा संबंधी जानकारियों की सुरक्षा के लिए बहुत नुकसानदायक हैं। कंप्यूटर या लैपटॉप की कार्यक्षमता को खराब या धीमा कर सकता है। मालवेयर किसी भी कंप्यूटर में एंटर करके उसे स्लो बना देता है या फिर उसमे और नए मालवेयर बनाकर कर के उसमे स्पेस कम कर देता है। मालवेयर कंप्यूटर में रहते है अपना काम निरंतर करते जाते हैं, लेकिन फाइल के रूप में यह दिखते नहीं। धीरे धीरे कंप्यूटर स्लो होने लगता है और फिर खराब हो जाता है। अगर आपके कंप्यूटर में कैसा भी विंडो एरर (window error) या फिर हार्ड ड्राइव एरर आये तो यह भी मालवेयर की वजह से हो सकता है। मालवेयर विंडो की फाइल को बिगाड़

(corrupt) देता है। जिसके कारण आपको ऐसे एरर दिखाता करता है। इसका प्रयोग कई हैकिंग करने वाले (hackers) अपने हित में करते हैं ताकि वह देख सके की आप अपने कंप्यूटर में क्या-क्या करते हो और उपयोक्ताओं को इसका भान भी नहीं होता।

आमतौर पर मालवेयर बनाने के पीछे निम्न कारण हो सकते हैं

- मालवेयर से संक्रमित कंप्यूटर सिस्टम को रिमोट कंप्यूटर से नियंत्रित करने में सक्षम होना।
- संक्रमित कंप्यूटर सिस्टम से अनचाहे लक्ष्यों को स्पैम भेजना।
- संक्रमित यूजर्स कि व्यक्तिगत और लोकल नेटवर्क की जाँच ।
- व्यक्तिगत या संवेदनशील डेटा चोरी करना।

प्रश्न उठता है कि इस प्रकार के मालवेयर सॉफ्टवेयर सिस्टम में आते कैसे हैं। आज के समय में सबसे सामान्य सोर्स है इंटरनेट, अगर हम इंटरनेट पर किसी मैलेशियस/अनाधिकृत (unauthorized) सी वेबसाइट पर हैं और वहां से कुछ डाउनलोड करते हैं या अगर हम पायरेटेड सॉफ्टवेयर या मूवी को डाउनलोड करते हैं या अगर किसी मैलेशियस वेबसाइट के किसी विज्ञापन पर क्लिक करते हैं। इन सभी सोर्स से कंप्यूटर सिस्टम में वायरस/ मालवेयर आ सकता है। इसके अलावा ऑफलाइन किसी दूसरी जगह से ऐसी पेनड्राइव या किसी सीडी, डीवीडी को अपने कंप्यूटर में लगाते हैं वहां से भी इस प्रकार के मैलेशियस सॉफ्टवेयर हमारे कंप्यूटर में आ सकते हैं।

वायरस, ट्रोजन, स्पायवेयर और रैंसमवेयर मालवेयर के विभिन्न प्रकारों में से हैं।

मालवेयर को कंप्यूटर में आने से कैसे रोके-

- स्पैम ईमेल के साथ जो फाइल अटैच हो कर आई है उसको ना खोलें और ना डाउनलोड करे।
- इन्टरनेट पे सिर्फ विश्वसनीय (trusted) साइट्स पर ही जाएं (visit करे)।
- Pirated फाइल डाउनलोड ना करे।
- अद्यतन एंटीवायरस सॉफ़्टवेयर (Updated antivirus software) का उपयोग अवश्य करें।

- कम्प्यूटर में फायरबॉल (Firwall) को इनस्टॉल कर के रखे।

II. वर्म (Worm)

एक कंप्यूटर वर्म एक स्टैंड अलोन मालवेयर कंप्यूटर प्रोग्राम है जो अन्य कंप्यूटरों में फैलने के लिए खुद को दोहरा सकता है। कंप्यूटर वर्म् किसी अन्य सॉफ्टवेयर में संलग्न नहीं होता बल्कि स्पैम ईमेल या इंसटेंट मैसेज में अटैचमेंट के रूप में आ सकते हैं और उपयोगकर्ता के ज्ञान के बिना मशीन को संक्रमित करता है। यह वास्तव में अपनी ही नकल करता है और खुद को कॉपी करता है इस तरह इसका आकार बढ़ता जाता है और यह और हार्ड डिस्क स्थान को भरता चला जाता है। एक कंप्यूटर में आने के बाद उस कंप्यूटर के नेटवर्क में जुड़े अन्य कंप्यूटर सिस्टम को भी संक्रमित करता चला जाता है, जिससे सिस्टम और नेटवर्क धीमा हो जाता है।

III. वायरस (Virus)

कम्प्युटर वायरस एक प्रकार का इलेक्ट्रॉनिक कोड होता है। इस कोड का उपयोग कंप्यूटर में उपस्थित सूचनाओं को मिटाने या उसे खराब करने का कार्य करता है।

यह एक सूक्ष्म कंप्यूटर प्रोग्राम होता हैं। जो किसी भी कंप्यूटर में प्रवेश कर उस डिवाईस की कार्य-प्रणाली में बाधा उत्पन्न करते हैं। यह टारगेट कंप्यूटर पर अपने आप ही रन हो जाता है (Auto-Execute) जो अपने आपको खुद बढ़ा लेता है।

यह दुर्भावनापूर्ण प्रोग्राम का एक टुकड़ा है जो फ़ाइलों और सिस्टम को नुकसान पहुंचाने की कोशिश करता है। यह एक ऐसा प्रोग्राम है जो खुद को प्रतिकृति बनाता है और संक्रमित फ़ाइलों का उपयोग करके फैलता है। किसी उपयोगकर्ता के ज्ञान के बिना पूरे कंप्यूटर फ़ाइलों में फैल जाता है।

यह कंप्यूटर वायरस अपने कोड को कंप्यूटर में निष्पादित (execute) करने के लिए किसी डॉक्यूमेंट अथवा कंप्यूटर प्रोग्राम के साथ संलग्न (attach) होकर संचालित होता है और

धीरे–धीरे आपके कंप्यूटर में फैलता जाता है। एक कंप्यूटर वायरस में अप्रत्याशित और हानिकारक प्रभाव पैदा करने की क्षमता होती है।

एक बार कंप्यूटर सिस्टम में निष्पादित हो जाने के बाद यह आपके प्रोग्राम और फाइल को नष्ट कर सकते है। इसके अलावा यह कंप्यूटर की कार्य क्षमता को धीमा (slow performance) करते है साथ ही सिस्टम सॉफ्टवेयर को पूरी तरह काम करने से रोकते है। इन कंप्यूटर वायरस को बनाने का उद्देश्य कमजोर सिस्टम को संक्रमित करना, व्यवस्थापक नियंत्रण हासिल करना और सवेंदनशील डेटा चोरी करना होता है।

यह कंप्यूटर वायरस आपके सिस्टम में कई तरह से आ सकता है। सबसे प्रमुख विधि जिसके द्वारा वायरस फैलता है, वह ईमेल के माध्यम से होता है। जैसे ईमेल अटेचमेंट को खोलना, किसी संक्रमित वेबसाइट पर जाना, निष्पादन योग्य फ़ाइलें पर क्लिक करना या संक्रमित वेबसाइट पर विज्ञापन को खोलने से भी यह आपके सिस्टम तक पहुँच सकता है। इसके अलावा वायरस युक्त यू.एस.बी ड्राइव से भी आपके कंप्यूटर में वायरस फैल सकता है।

इसके अलावा ऑफलाइन तरीके की बात करें तो सीडी, फ्लॉपी डिस्क तथा पेनड्राइव आदि की मदद से कंप्यूटर वायरस एक कंप्यूटर से दूसरे डिवाइस में फैल सकता है।

IV. ट्रोजन होर्स (Trojan Horse)

ट्रोजन होर्स एक हानिकारक कंप्यूटर प्रोग्राम होता है जो कि हमारे सिस्टम को नियंत्रण में कर लेता है और असामान्य गतिविधि को अंजाम देता है। ट्रोजन, किसी वायरस की तरह अपनी कॉपी तो नही बना सकते परन्तु ये वायरस को सिस्टम में इंस्टॉल कर सकते है। इसी की मदद से हैकर कंप्यूटर का नियंत्रण सुदूर बैठे दूसरे कंप्यूटर से कर सकता है।

उदाहरण के लिए:- एक दोस्त की फेसबुक आईडी हैक हो जाती है और उसकी आईडी से एक मैसेज आता है कि इस गेम को डाउनलोड करो यह बहुत बढ़िया गेम है, परन्तु वह गेम ना होकर एक ट्रोजन होता है।

- एक ट्रोजन, सिस्टम की फाइलों तथा डेटा को डिलीट कर सकता है।
- महत्पूर्ण जानकारी तथा पासवर्ड को चुरा सकता है।
- सिस्टम को लॉक कर सकता है।
- मालवेयर को डाउनलोड करके इंस्टॉल कर सकता है।
- सिस्टम को दोबारा शुरू कर सकता है।
- सीडी को संक्रमित (infect) कर सकता है।
- सिस्टम की स्क्रीन में मैसेज को प्रदर्शित कर सकता है।
- प्रोग्राम को बन्द कर सकता है।

V. स्पाइवेयर (Spyware)

स्पाइवेयर एक सॉफ्टवेयर होता है जो मालवेयर का एक प्रकार है। यह किसी कंप्यूटर में बिना इजाजत के प्रवेश करता है और उपयोगकर्ताओं की बिना जानकारी के उस कंप्यूटर की सारी निजी जानकारियां मालवेयर भेजने वाले व्यक्ति या समूह को दे देता है। सामान्य शब्दों में कहें तो जिस तरह हमारे दैनिक जीवन मे किसी व्यक्ति द्वारा अपनी सुरक्षा बनाये रखने के लिए सीसीटीवी कैमरा का इस्तेमाल लोगों पर निगरानी रखने के लिए किया जाता है। उसी तरह स्पाइवेयर भी कंप्यूटर में पहुँच कर कंप्यूटर यूज़र द्वारा इंटरनेट पर की जाने वाली सभी गतिविधियों पर नजर रखता है। परन्तु इस बात की जानकारी से उपयोगकर्ता अनजान रहता है।

परन्तु यहाँ ध्यान रखने योग्य बात यह है कि वर्तमान समय में कई कंपनियों तथा कार्यालयों में कर्मचारियों की निगरानी के लिए भी स्पाइवेयर को कंप्यूटर में इनस्टॉल किया जाता हैं। जिससे कंपनी के मैनेजर या सीईओ कर्मचारियों द्वारा कंप्यूटर में की जाने वाली इंटरनेट क्रियाकलापों पर नजर रख सही-सही जानकारी पता लग सके। इस प्रकार स्पाइवेयर विभिन्न प्रकार की निजी जानकारियों को गुप्त रूप से पता लगाता है।

स्पाइवेयर शब्द से पता चलता है कि यह एक सॉफ्टवेयर है जो उपयोगकर्ता के कंप्यूटर पर गुप्त रूप से निगरानी रखता है, जबकि स्पाइवेयर का काम महज निगरानी से भी कहीं

ज्यादा है। स्पाइवेयर विभिन्न प्रकार की व्यक्तिगत जानकारी इकट्ठा करता है, जैसे कि इंटरनेट सर्फिंग की आदतें और जिन साइटों पर जाया जाता है। अतः एक बार किसी कंप्यूटर में स्पाइवेयर के प्रवेश करने पर यूजर का पूरा डाटा चुराया जा सकता है।

यहाँ एक बात हमें ध्यान में रखनी चाहिए कि स्पाइवेयर एक वायरस नहीं है। क्योंकि वायरस की तुलना में स्पाइवेयर कंप्यूटर से अन्य कंप्यूटर्स तक नहीं फैलते। वायरस एक सिस्टम से दूसरे सिस्टम तक पहुँचने की कोशिश करते हैं।

VI. लॉजिक बम (Logic Bomb)

लॉजिक बम एक प्रोग्रामिंग कोड है जो गुप्त रूप से सिस्टम में डाला जाता है और इन्हें विशेष परिस्थितियों, समय दिन या दिनांक में ही एक्टिव होने के लिए तैयार किया जाता है, जैसे कि एक विशिष्ट तिथि तक पहुंचना या एक विशिष्ट कमांड टाइप करने वाला उपयोगकर्ता। प्रोग्राम कोड जिन्हें किसी विशेष समय पर निष्पादित करने के लिए निर्धारित किया जाता है, उन्हें " लॉजिक-बम" के रूप में जाना जाता है। यह एक दुर्भावनापूर्ण कोड है, जो एक विशिष्ट घटना के चालू होने पर एक दुर्भावनापूर्ण कार्य को निष्पादित करता है। यह निर्दिष्ट शर्तों के पूरा होने तक निष्क्रिय रहता है। घटनाओं में एक निश्चित तिथि या समय शामिल हो सकता है, या एक संक्रमित सॉफ़्टवेयर एप्लिकेशन लॉन्च किया जा रहा है या हटाया जा रहा है। जब एक लॉजिक बम एक्टिव होता है तो यह डाटा को डिलीट या करप्ट कर सकता है, फ़ाइल हटाने या हार्ड ड्राइव पूरा डिलीट करना व नेटवर्क को नुकसान पहुंचाने के लिए या अन्य कई प्रकार के अवांछित प्रभाव उत्पन्न कर सकता है। उदाहरण के लिए, कुख्यात "शुक्रवार 13 वां"(Friday the 13th) वायरस जिसने केवल विशिष्ट तिथियों पर मेजबान सिस्टम पर हमला किया; यह हर महीने शुक्रवार को होने वाली "विस्फोट" (खुद को डुप्लिकेट) के रूप में हुआ, इस प्रकार सिस्टम में मंदी का कारण बना।

VII. फ़िशिंग (Phishing)

इलेक्ट्रॉनिक संचार में फ़िशिंग (Phishing) या इलेक्ट्रोनिक जालसाज़ी, एक ऐसा कार्य है जिसमें किसी विश्वसनीय इकाई का मुखौटा धारण कर उपयोगकर्ता नाम (प्रयोक्ता नाम), पासवर्ड (कूटशब्द) और क्रेडिट कार्ड का विवरण (और कभी-कभी, परोक्ष रूप से पैसा) जैसी विभिन्न जानकारियां हासिल करने का प्रयास किया जाता है।

इसमें किसी बैंकिंग, क्रेडिट/ डेबिट कार्ड की डिटेल्स और पासवर्ड जानने के लिए किसी बैंक या आर्गेनाईजेशन के माध्यम से कॉल या मैसेज किया जाता है। यूज़र को लगता है कि मैसेज ज्ञात कॉन्टैक्ट या ऑर्गनाइज़ेशन द्वारा भेजा गया है, लेकिन वह झूठा (Fake) होता है। अपराधी आपको फिशिंग के द्वारा नकली ईमेल या मैसेज करते है जो किसी कम्पनी, बैंक की तरह मिलते जुलते होते है।

फिशिंग पेज बिलकुल Original पेज की तरह ही होता है। उपयोगकर्ताओं को एक नकली वेबसाइट जिसका रूप और अनुभव बिल्कुल असली वेबसाइट (वैध वेबसाइट) के समान होता है पर, अपने विवरण दर्ज करने के लिए निर्देशित किया जाता है। बस इसमें यूआरएल ऐड्रेस में बदलाव होता है जो किसी यूज़र को आसानी से नजर नहीं आता है। फ़िशिंग ईमेल में कॉर्पोरेट लोगो (Logo) और डाटा होता हैं जिससे वह ई-मेल असली लग सके और इसमें मालवेयर से संक्रमित वेबसाइटों की कड़ियां हो सकती हैं। यह लोगों को ईमेल या मैसेज के द्वारा फिशिंग लिंक भेज सकते हैं। कोई भी जब इस लिंक पर क्लिक करता है तो वह फिशिंग पेज पर आ जाता है। यूज़र को लगता है की वह वास्तविक (Original) वेबसाइट है और वह वहां पर अपनी आईडी और पासवर्ड से लॉग इन करते है। जैसे ही वह लॉग इन करते है तो यह आईडी और पासवर्ड हैकर के पास चली जाती है और यूज़र को पता भी नहीं चलता है की वह फिशिंग अटैक के शिकार हो चुके है। फिशिंग से बचने के लिए निम्न बातों का ध्यान रखें:

- किसी अंजान स्रोत से प्राप्त ई-मेल के किसी भी लिंक को क्लिक न करें ना ही किसी अनजानी लिंक में अपनी जानकारी को डाले। उसके साथ हुए अटैचमेंट को

डाउनलोड भी ना करे। इसमें दुर्भावनापूर्ण कोड या ''फिश'' के हमले का प्रयास हो सकता है।

- पॉप-अप विंडो के रूप में आए पेज पर किसी भी प्रकार की कोई जानकारी नही दें।
- कभी भी अपनी व्यक्तिगत जानकारी या अपना पासवर्ड फोन पर या ई-मेल से प्राप्त अनुरोध पर नहीं बताएं।
- हमेशा याद रखें कि जैसे पासवर्ड, पिन (PIN), टिन (TIN) आदि की जानकारी पूरी तरह से गोपनीय है तथा बैंक के कर्मचारी/सेवा कार्मिक भी इसकी माँग नहीं करते हैं। इसलिए ऐसी जानकारियां मांगे जाने पर भी किसी को न दें।
- आप अपने किसी भी अकाउंट में लॉग इन करते समय यूआरएल का ध्यान जरुर रखे। हमेशा एड्रेस बार में सही यूआरएल टाइप कर साईट को लॉग-ऑन करें। आपका यूजर आईडी एवं पासवर्ड केवल अधिकृत लॉग-इन पेज पर ही दें।
- अपना बैंक वगैरह में यूजर आईडी एवं पासवर्ड डालने से पूर्व कृपया सुनिश्चित कर लें कि लॉग-इन पेज का यूआरएल 'https://' से प्रारम्भ हो रहा है 'http:// से नहीं। 'एस' से आशय है सुरक्षित (Secured) तथा यह दर्शाता है कि वेब पेज में एंक्रिप्शन का प्रयोग हो रहा है।
- यदि आप कंप्यूटर का इस्तेमाल करते है। तो अपने कंप्यूटर में एक अच्छे एंटी-वायरस का इस्तेमाल ज़रुर करे जो आपको वेब सिक्यूरिटी देगा।

VIII. हैकिंग (Hacking)

आज के युग में कंप्यूटर और मोबाइल तकनीक का उपयोग तेजी से बढ़ रहा है। इनके आसान उपयोग के कारण आम जनता डिजिटल युग में आ गई है। जितनी तेजी से हम तकनीक में दक्ष हो रहे हैं उतनी ही तेजी से ऑनलाइन गतिविधियां के माध्यम से किया जाने वाला अपराध भी बढ़ रहे। ऑनलाइन माध्यम से किया जाने वाला अपराध अर्थात साइबर क्राइम को हैकिंग कहते हैं। दूसरे शब्दों में कहें एक तकनीकी चालाकी है। जब कोई व्यक्ति गलत उद्देश्य से किसी सिस्टम फंक्शन जैसे कंप्यूटर नेटवर्क, सर्वर आदि में कमजोरी को ढूंढें और उस सिस्टम को अपने अनुसार बदल कर डाटा को चुरा लेता या नष्ट कर देता है क्या उसे बदल देता है, यह प्रक्रिया हैकिंग कहलाती है। जिस व्यक्ति द्वारा यह तकनीकी चालाकी को

अंजाम दिया जाता है उस व्यक्ति को हैकर कहते हैं। हैकर कंप्यूटर या नेटवर्क में विभिन्न प्रकार से सेंध लगाने की कोशिश करता है जैसे

- पासवर्ड पता लगाना।
- सरवर या नेटवर्क में मौजूद कोई तकनीकी खामी के बारे में पता लगाना।
- विभिन्न प्रकार के एक जैसी वेबसाइटों माध्यम से डाटा को एकत्रित करना।
- दोषपूर्ण सॉफ्टवेयर को उपयोगी बताकर कंप्यूटर की जानकारी चुराना और डाटा को नष्ट करना।
- किसी व्यक्ति द्वारा अपने कंप्यूटर में टाइप किए गए शब्दों पर निगरानी रखना।

हैकिंग के विभिन्न प्रकार

- **एथिकल हैकिंग**

  एथिकल हैकिंग वह हैकिंग होती है जो जानकारी को प्राप्त करने जानबूझकर किसी सही उद्देश्य के लिए की जाती है। इस प्रकार की हैकिंग में लोग नेटवर्क, सर्वर, डाटा स्टोरेज और और सूचना प्रणाली मैं संभावित और मौजूद कमियों को ढूंढते हैं जिससे कि उनको दूर किया जा सके। जब हैकरों द्वारा कोई कमी ढूंढ ली जाती है तो उस कमी को बग कहा जाता है। इसमें किसी भी प्रकार का डाटा चुराया नहीं जाता, ना ही नष्ट किया जाता है, और ना ही बदला जाता है। एथिकल हैकिंग पूरी तरह से कानूनी होती है और लोगों को संभावित खतरों से बचाने के लिए की जाती ताकि कोई मौजूद कमी या बग को दूर किया जा सके।

- **मैलेशियस हैकिंग**

  वह हैकिंग जो किसी गलत उद्देश्य से की जाती है और इसका तरीका गैरकानूनी होता है। मैलेशियस हैकिंग कहलाती है। इस प्रकार की हैकिंग में डाटा चुराया जा सकता है, उसे नष्ट किया जा सकता है या उसका गलत इस्तेमाल भी जा सकता। जैसे किसी ईमेल अकाउंट को हैक करना, फेसबुक अकाउंट को हैक करना, बैंक अकाउंट की जानकारी

चुराकर पैसे निकालना, किसी वेबसाइट अकाउंट पर कब्जा करके उसका दुरुपयोग करना आदि काम मैलेशियस हैकिंग में शामिल होते हैं। इस प्रकार की हैकिंग से सरकार और बड़ी कंपनियों को भी नुकसान हो सकता है क्योंकि बहुत से लोगों की जानकारी होती है अथवा गोपनीय जानकारी भी होती है। जैसे सुरक्षा एजेंसियां, पुलिस, शेयर मार्केट, स्टॉक एक्सचेंज, परमाणु केंद्र, अंतरिक्ष शोध केंद्र, आदि वेबसाइट और डाटा को बना बनाया जाता है।

IX. स्पूफिंग (Spoofing)

स्पूफिंग एक दुर्भावनापूर्ण प्रयोग है जो साइबर स्कैमर और हैकर्स द्वारा सिस्टम, व्यक्तियों और संगठनों को धोखा देने के लिए किया जाता है। लोगों को एक प्रामाणिक और सुरक्षित प्रेषक के रूप में प्रस्तुत करते हैं लेकिन ऐसा होता नहीं है। सर्वर को अनाधिकृत उपयोग (unauthorized access) करने की एक तकनीक है जिसमें एक कंप्यूटर, नेटवर्क में मैसेज भेजता है। भेजे जाने वाले पैकेट हैडर के भेजे जाने वाली मशीन (source address) को attacker के द्वारा बदल दिया जाता है। जिसके कारण प्राप्त करने वाली मशीन (destination computer) को यह लगता है कि यह मैसेज किसी विश्वसनीय (trusted) डिवाइस से भेजा गया है। ऐसा इसलिए होता है क्योंकि कि attacker इस डिवाइस के आई पी एड्रेस को बदल देता है। जिसके कारण destination computer इस पैकेट को trusted computer से आने वाला समझता है। मुख्य रूप से स्पूफिंग का उपयोग किया जाता है:

- भेजने वाले (sender) की पहचान (identity) साइबर पुलिस और प्राधिकरण (cyber police and authority) से छुपाने के लिए, क्योंकि इसके द्वारा attacker का पता लगाना मुश्किल होता है।
- Target वाले डिवाइस को alert होने से रोकने के लिए।
- Security script को bypass करने के लिए, security script वो होती है जिसके द्वारा IP address को blacklist करके डिनायल ऑफ सर्विस हमलों को कम करने का प्रयास किया जाता है।

आईपी स्पूफिंग के प्रकार

आईपी स्पूफिंग दो प्रकार के होते हैं।

इस तकनीक का प्रयोग सबसे ज्यादा attackers के द्वारा एक डिवाइस में **डिनायल ऑफ सर्विस अटैक** (DDoS attack) और **मैन इन द मिडिल अटैक** (Man-in-the-Middle attack) करने के लिए किया जाता है।

i. **मैन इन द मिडिल अटैक** जैसा कि नाम से पता चलता है, संदेश के मूल प्रेषक और वांछित प्राप्तकर्ता के बीच संचार बाधित होता है। संदेश की सामग्री को तब किसी भी पक्ष के ज्ञान के बिना संशोधित किया जाता है। हमलावर पैकेट को अपने संदेश के साथ मिलाता है। पीड़ित को यह सोचने में धोखा दिया जाता है कि संदेश की सामग्री प्रामाणिक है।

ii. **डिनायल ऑफ सर्विस अटैक** एक प्रभावशाली हैकिंग तकनीक है जो हैकिंग ग्रुप द्वारा बड़े स्तर पर की जाती। इंटरनेट की दुनिया मैं किसी सर्वर या वेबसाइट पर किया जाने वाला ऐसा अटैक है जिससे किसी भी सर्वर या वेबसाइट को डाउन कर दिया जाता है या बंद कर दिया जाता है या फिर उस वेबसाइट के यूज़र के लिए वेबसाइट को अनुपलब्ध कर दिया जाता। जिससे कोई भी यूजर उस वेबसाइट तक नहीं पहुंच पाता है दुनिया में किसी भी चीज कि काम करने की एक लिमिट होती है इसी तरह से वेबसाइट की एक लिमिट होती है कि 1 मिनट में कितने लोगों को एक्सेस करने की इजाजत देती। उदाहरण के लिए किसी वेबसाइट की लिमिट है कि उस वेबसाइट को 1 मिनट में सिर्फ सौ लोग ही एक्सेस कर सकते हैं। यदि उससे ज्यादा आएंगे तो सर्वर डाउन हो जाएगा जा बंद हो जाएगा। तो यह समझने की बात है की अगर सौ से ज्यादा लोग इस वेबसाइट को 1 मिनट में ओपन करेंगे तो वह बंद या डाउन हो जाएगी। हैकर भी ऐसे ही किसी वेबसाइट पर ओवर ट्रैफिक भेजकर साइट को डाउन कर देते हैं जिससे उसकी यूज़र वेबसाइट तक नहीं पहुंच पाते हैं या उस वेबसाइट को ओपन ही नहीं कर पाते। जिस कारण जिन लोगों का काम वेबसाइट से चल रहा था वह नहीं हो पाएगा। अगर इस प्रकार के अटैक करते हैं और जब वह वेबसाइट नहीं खुल पाती है साइट के मालिक से पैसों की मांग करते हैं। इसी प्रकार दो वेबसाइट समान कार्य के लिए हैं और यदि एक ने

दूसरे की वेबसाइट पर डिनायल ऑफ सर्विस अटैक कर दिया तो यह सामान्य सी बात है, लोग अपनी जरूरतों का सामान खरीदने के लिए उसी वेबसाइट पर जाएंगे जो चल रही है।

X. स्पैम मेल (Spam Mail)

इंटरनेट पर लोगों को संदेश या विज्ञापन बार-बार भेजना जिसका उन्होंने अनुरोध नहीं किया है स्पैम कहलाता है। अर्थात अवांछित ईमेल जो बहुत ज्यादा भेजा जाता है, बिना मांगे या बुलाये आ जाता है, जिसमे प्रायः विज्ञापन भरे होते है।

जब भी कोई भेजने वाला किसी को बहुत बड़ी तादाद में विज्ञापन की मेल भेजता है तो उसे स्पैम मेल कहते हैं। यह ईमेल पाने वाले के बिना अनुमति के आते हैं। यह ईमेल मुख्यतः विज्ञापन से ही भरे होते हैं। अगर कोई ईमेल स्पैम करता है तो यहां स्पैम करने का एक ही फायदा है और वह है अपने उत्पाद का विज्ञापन-पत्र के माध्यम से बढ़ावा करना। जैसे किसी कंपनी या व्यक्ति विशेष ने एक लाख लोगों को स्पैम मेल भेजी। जिसमें उसने अपना उत्पाद का विज्ञापन किया है। अब इन एक लाख लोगों में से यदि दस हजार लोगो ने भी उस ईमेल को खोला तो कंपनी का उत्पाद की जानकारी इन दस हजार लोगों में चली गई। इसके अलावा अगर इन दस हजार लोगों में से एक हजार या पाँच सौ लोगों ने भी उस उत्पाद को खरीद लिया तो इससे कंपनी की बिक्री भी हो गई। और यह सब हुआ बिल्कुल फ्री में जबकि अपने उत्पाद को अन्य तरह से विज्ञापन करने पर पैसे लगता है। जिसको स्पैम के माध्यम से बिल्कुल मुफ्त में कर लिया गया। इसी प्रकार अन्य सोशल साइट्स में भी इस टाइम होता है जैसे कई बार व्हाट्सएप पर कुछ अजीब से मैसेज देखे होंगे। जैसे इस लिंक को अपने 10 दोस्तों के साथ शेयर करें और फिर आप आईफोन जीत सकते हैं। इसके अलावा भी कुछ ऐसे ही मैसेज आते हैं इस लिंक को अपने 10 दोस्तों के साथ शेयर करने पर आपको 100 जीबी डाटा मिलेगा आदि। जो कि बिल्कुल झूठ होता है। याद रखें अगली बार यदि ऐसा कोई मैसेज आता है तो आप इस लिंक पर बिल्कुल भी क्लिक ना करें और उस मैसेज को शेयर भी

ना करें। यदि आपको कोई ऐसा मैसेज भेजता है तो आप उसे बताएं स्पैम है। इस प्रकार के मैसेज भेजने से कोई इनाम नहीं पाएगा, तो आगे से वह ऐसा ना करें।

XI. पहचान चुराना (Identity Theft)

यह क्राइम आज के समय में सबसे ज्यादा देखा गया है। यह ज्यादातर उन लोगों को निशाना बनाते हैं जो की अपने वित्तीय ट्रांजैक्शन और बैंकिंग सर्विसेज के लिए इंटरनेट का उपयोग करते हैं। इस साइबर क्राइम में कोई व्यक्ति गलत उद्देश्य से किसी व्यक्ति का डाटा जैसे कि उसका बैंक अकाउंट नंबर, क्रेडिट या डेबिट कार्ड संबंधित जानकारियां, इंटरनेट बैंकिंग से संबंधित जानकारी, निजी जानकारियां किसी प्रकार से प्राप्त कर लेते हैं। और यही जानकारी का इस्तेमाल कर उस व्यक्ति का पहचान (आईडेंटिटी) लेकर ऑनलाइन चीजें या सामान खरीदते हैं या अन्य वित्तीय लाभ उठाने या अपराध करने की कोशिश की जाती है।

उदाहरण के लिए एक व्यक्ति के पास एक क्रेडिट कार्ड था जिसे ना तो वे इस्तेमाल कर रहे थे और ना ही उसे बंद कराया था। एक दिन उनके पास बैंक से एक फोन आया। उन्हें बताया गया कि उनका क्रेडिट लिमिट खत्म हो चुका है और बिल भरने की उनकी तारीख पास आ रही है। उस व्यक्ति को समझ आया कि उनका वित्तीय रिकॉर्ड चोरी हुआ और उसका दुरूपयोग किया गया है।

किसी अन्य व्यक्ति की पहचान चुराकर कंप्यूटर नेटवर्क पर कार्य करना इस अपराध श्रेणी में आता है।

- कंप्यूटर नेटवर्क पर स्वयं की पहचान बचा कर स्वयं को दूसरे के नाम से प्रस्तुत करना, उसके नाम पर कोई घपला करना, बेवकूफ बनाना आईटी एक्ट के अंतर्गत अपराध है।
- इसके अतिरिक्त किसी अन्य व्यक्ति का पासवर्ड का प्रयोग करना।
- डिजिटल सिग्नेचर की नकल करना भी इस अपराध की श्रेणी में आते हैं।
- किसी अन्य के नाम का प्रयोग कर अवांछित लाभ लेना धोखाधड़ी करना भी इस प्रकार के अपराध में आते हैं।

ध्यान रखिए कि इसलिए कंप्यूटर नेटवर्क पर अपने पासवर्ड व्यक्तिगत जानकारियां सार्वजनिक ना करें। ऐसे अपराधों के लिए आईटी एक्ट 2008 सेक्शन 66 सी के अंतर्गत सजा का प्रावधान है।

3.13.3 साइबर अपराध की रोकथाम:

आइए अपने कंप्यूटर सिस्टम में साइबर अपराध को रोकने के कुछ तरीकों पर नज़र डालें:

- जब भी आपके कंप्यूटर सिस्टम, स्मार्ट फोन, टैबलेट आदि के लिए सिस्टम सॉफ्टवेयर के अपडेट मिलते हैं, उसी समय इसे अपडेट करें क्योंकि कभी-कभी पिछले संस्करण पर आसानी से हमला किया जा सकता है। नवीनतम बग और कमजोरियों को पैच करने के लिए अपने ओएस को नवीनतम रखें।
- कभी भी एक से अधिक वेबसाइट पर एक ही पासवर्ड का उपयोग न करें। प्रत्येक खाते के लिए अलग-अलग पासवर्ड और यूजरनेम बनाए और उन्हें लिख कर रखने से बचें। हमेशा यह सुनिश्चित करें कि पासवर्ड अक्षरों, विशेष वर्णों और संख्याओं को जोड़ कर मजबूत बनाना है। हालांकि छोटा पासवर्ड याद रखना आसान होता है जो आपके जन्मदिन, मध्य नाम या परिवार का नाम पर आधारित हो। परंतु इस प्रकार के पासवर्ड को तोड़ना हैकर के लिए भी आसान होता है। मजबूत पासवर्ड का उपयोग अकाउंट को सुरक्षित रखने में मदद करते है।
- हमेशा मोबाइल और पर्सनल कंप्यूटर में भरोसेमंद और अत्यधिक उन्नत एंटीवायरस सॉफ़्टवेयर का उपयोग करें। यह उपकरणों पर विभिन्न वायरस के हमले की रोकथाम की ओर जाता है। मुफ्त एंटीवायरस/ एंटीमलेवेयर समाधान सहायक हो सकते हैं लेकिन वे अक्सर केवल ट्रायल सॉफ़्टवेयर होते हैं और खतरों से पूर्ण सुरक्षा प्रदान नहीं करते हैं।
- अपनी व्यक्तिगत जानकारी को ऑनलाइन पोस्ट करने से बचे और संवेदनशील जानकारी जैसे – सिक्योरिटी नंबर और क्रेडिट और डेबिट कार्ड नंबर, ओटीपी को शेयर न करे। किसी भी लिंक पर क्लिक करने या किसी भी एप्लीकेशन को डाउनलोड करने के दौरान सतर्क रहें।
- उन वेबसाइट, ईमेल, फोन कॉल्स या डाउनलोड लिंक से बचने की जरूरत है जो आपकी व्यक्तिगत जानकारी के लिए पूछती है। अपना नेट बैंकिंग, डेबिट कार्ड क्रेडिट कार्ड का

पासवर्ड किसी भी स्थिति में किसी भी ट्रांजैक्शन के लिए उपयोग ना करें। यह सिर्फ आपके नेट बैंकिंग के लिए आपकी बैंक की वेबसाइट पर ही उपयोग किया जाना चाहिए।

- जब भी पेमेंट पेज पर हो, तो अपने ब्राउज़र में लॉक सिंबॉल की तलाश करे। ये संकेत करता है कि साइट आपकी जानकारी को सुरक्षित रखने के लिए एन्क्रिप्शन का उपयोग करती है। साइट के एड्रेस बार मे ये भी देखे की क्या URL “https://” के बजाय कहीं “Http://” से तो start नही है। यहां दोनों में S शब्द का अंतर महत्वपूर्ण है।
- जब भी आप ईमेल चेक कर रहे हो या मैसेंजर पर चैटिंग कर रहे हो तो अनचाहे ईमेल या किसी भी अज्ञात व्यक्ति के द्वारा भेजें गए संदिग्ध लिंक या अटैचमेंट पर क्लिक करते वक्त सावधान रहे। यह आपको फ़िशिंग हमलों और अवांछित संक्रमणों से सुरक्षित रखेगा।
- ऑनलाइन शॉपिंग करते वक्त भी सावधान रहने की जरूरत है। मैन इन द मिडल अटैक आपको बीच-बीच में होने वाले हमलों और अपने क्रेडिट कार्ड या ऑनलाइन वॉलेट के अपराधों का शिकार होने से बचाने के लिए, पहले यह सुनिश्चित कर लें कि जिस साइट पर आप खरीदारी कर रहे हैं वह HTTPS के साथ सुरक्षित एन्क्रिप्टेड है। यह भी सुनिश्चित करें कि आप किसी प्रसिद्ध साइट पर खरीदारी कर रहे हैं।
- फ़ायरवॉल का उपयोग करे। ये एक नेटवर्क सुरक्षा प्रणाली है, जो कंप्यूटर/ नेटवर्क और इंटरनेट के बीच ट्रैफिक की निगरानी करता है। जब भी कोई आपके किसी खुले पोर्ट पर खराब पैकेट भेज कर घुसने की कोशिश करता है, तो सिस्टम फ़ायरवॉल डिजिटल अवरोधक के रूप में घुसपैठियों को रोकता है।
- किसी भी ऐसी ऑनलाइन स्कीम जिसमें आपके पैसे जीतने, दुगने करने या घर बैठे लाखों कमाने की बात की गई हो उसमे बिल्कुल भी विश्वास न करे।
- महत्वपूर्ण डाटा की बैकअप कॉपी रखें।
- अपराधी अपराध करने के नए-नए तरीकों की खोज करते हैं अतः हमेशा साइबर अपराध के प्रति सचेत, सजग, सावधान रहे।