

खंड 2 डेटा हैंडलिंग



Pignou
THE PEOPLE'S
UNIVERSITY

खंड 2 डेटा हैंडलिंग

यह पाठ्यक्रम “व्यापार में कंप्यूटर का अनुप्रयोग” का दूसरा खंड है। यह खंड उपलब्ध डेटा को संभालने के लिए कंप्यूटर की उपयोगिता पर केंद्रित है जो संगठनों के लिए अधिक उपयोगी है। यह खंड शिक्षार्थियों को विभिन्न डेटा सौंपने की तकनीकों, सेवाओं और सुरक्षा उपायों और व्यवसाय में उनके अनुप्रयोगों से परिचित करेगा। यह व्यापार में इंटरनेट की प्रयोज्यता पर भी ध्यान केंद्रित करता है, ताकि इसे बेहतर इंटरनेट सेवाएं प्रदान करने के माध्यम से व्यवसाय संचालन को अधिक सुचारु रूप से संचालित किया जा सके। “डेटा हैंडलिंग” विषय पर खंड में चार इकाइयाँ शामिल हैं, जिनका विवरण नीचे दिया गया है:

इकाई 5 इस खंड की पहली इकाई डेटा और सूचना के साथ पाठकों को पेश करती है और व्यावसायिक सूचना प्रणाली, डेटा बेस मैनेजमेंट सिस्टम (डी.बी.एम. एस.), एंटरप्राइज रिसोर्स प्लानिंग (ई.आर.पी.), निर्णय समर्थन प्रणाली (डी.एस.एस.), प्रबंधन सूचना प्रणाली (एम.आई.एस.), जनरल डेटा प्रोटेक्शन रेगुलेशन (जी.डी.पी.आर.) इत्यादि की आवश्यकता और निहितार्थ पर प्रकाश डालती है।

इकाई 6 यह इकाई पाठकों को साइबर सुरक्षा और व्यवसाय के लिए उसके विभिन्न सिद्धांतों से अवगत कराती है। इसके अलावा यह इकाई उन कदमों पर चर्चा करती है, जिन्हें व्यापारिक संगठनों की परिसंपत्तियों को सुरक्षित रखने के लिए उठाए जाने की आवश्यकता होती है। यह इकाई उन्नत सुरक्षा उपायों जैसे ओ.टी.पी., कैप्चा कोड (Capcha code) आदि पर भी जानकारी देती है।

इकाई 7 यह विशेष इकाई इंटरनेट, इसके लाभ, कार्यों और विभिन्न सेवाओं जैसे ईमेल, एस.एम.टी.पी., आई.एम.ए.पी., पी.ओ.पी., वेब ब्राउजर आदि के साथ शिक्षार्थियों को परिचित करती है और विभिन्न अनुप्रयोगों ने उन्हें अपने काम को आसान बनाने में मदद करने के लिए पेशकश की है। यह इकाई इसके अलावा बेब डोमेन के महत्व का वर्णन करती है।

इकाई 8 यह इकाई चर्चा करती है कि प्लास्टिक मुद्रा अस्तित्व में कैसे आई और वर्तमान समय में इसका उपयोग कैसे हुआ। यह इकाई वर्तमान समय में वाणिज्यिक गतिविधियों, उनके विकास, महत्व और उपयोग में किए जाने वाले डिजिटल भुगतानों के विभिन्न मॉडलों की पहचान करती है। यह इकाई भारत में डिजिटल भुगतान प्रणाली पर विमुद्रीकरण नीतियों के प्रभावों के बारे में भी बताती है।

इकाई 5 व्यापार सूचना प्रणाली

इकाई की रूपरेखा

- 5.0 उद्देश्य
- 5.1 प्रस्तावना
- 5.2 डेटा और सूचना
- 5.3 बी आई. एस. (व्यापार सूचना प्रणाली) का परिचय
- 5.4 डेटा बेस मैनेजमेंट सिस्टम (DBMS)
 - 5.4.1 रिलेशनल डेटा बेस मैनेजमेंट सिस्टम (RDBMS)
 - 5.4.2 डेटा एब्स्ट्रैक्शन
 - 5.4.3 डेटा बेस एडमिनिस्ट्रेटर
 - 5.4.4 डेटा की पुनर्प्राप्ति
- 5.5 डिसीजन सपोर्ट सिस्टम (DSS)
- 5.6 एंटरप्राइज रिसोर्स प्लानिंग (ERP)
- 5.7 प्रबंधन सूचना प्रणाली (MIS)
- 5.8 जनरल डेटा प्रोटेक्शन रेगुलेशन (GDPR)
- 5.9 सारांश
- 5.10 शब्दावली
- 5.11 स्वपरख प्रश्न

5.0 उद्देश्य

इस इकाई को पढ़ने के बाद आप इस योग्य हो सकेंगे कि:

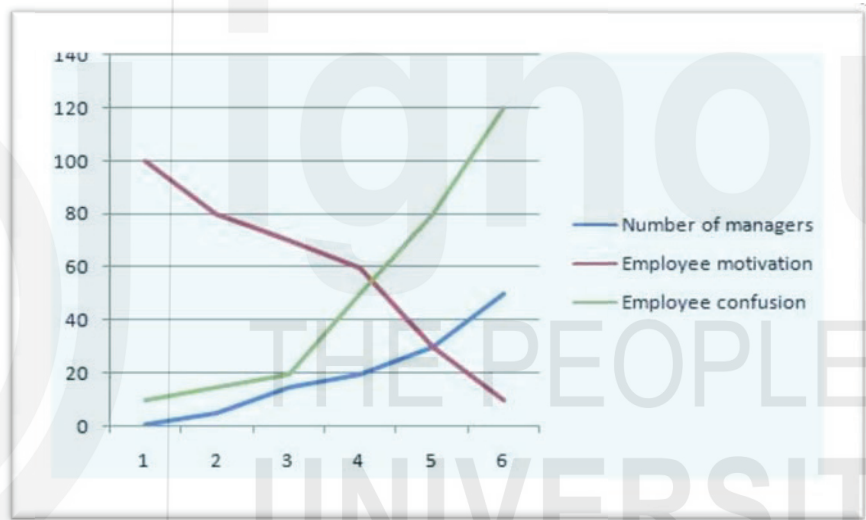
- डेटा और सूचना को समझ सकें।
- संगठन में उपलब्ध जानकारी के आधार पर प्रभावी निर्णय प्रणाली पर प्रकाश डाल सकें।
- व्यापार सूचना प्रणाली की आवश्यकता और निहितार्थ पर समझ सकें।

5.1 प्रस्तावना

किसी देश की अर्थव्यवस्था के काम करने के लिए व्यापार बहुत आवश्यक है। यह अर्थव्यवस्था को चलाने के लिए सहायक है। किसी देश में व्यापार के बुनियादी ढांचे की अनुपस्थिति को चलाने के लिए एक ऐसी अर्थव्यवस्था की ओर ले जाती है, जो देश के समग्र विकास में आदिम या अप्रभावी है। किसी देश में व्यापार की नींव जितनी मजबूत होती है, अर्थव्यवस्था उतनी ही मजबूत होती है। अर्थव्यवस्था और व्यापार के बीच के संबंध को समझने के लिए आइए एक उदाहरण पर विचार करें मान लीजिए कि कोई आदमी एक कंपनी बनाता है, तो उसे चलाने के लिए, वह लोगों को नियुक्ति विभिन्न काम करने के लिए करता है, जैसे लिपिक, लेखा-जोखा,

चपरासी, सफाई कर्मचारी तथा प्रशासनिक कार्य हेतु। यह कई लोगों को उनकी जीविका के लिए नौकरी के अवसर प्रदान करेगा। किसी देश की स्थिर जीविका उसके विकास के लिए बहुत आवश्यक है। यह वृद्धि मौलिक स्तर पर व्यापार की मूल बातों को समझने से संबंधित है जो अंततः डेटा और सूचना के गठन की ओर ले जाती है, जिसका विश्लेषण किया जाना आवश्यक है। जैसे ही कोई व्यवसाय शुरू होता है, यह डेटा उत्पन्न करता है। इस डेटा को सूचना, ज्ञान और बुद्धिमत्ता में परिवर्तित किया जा सकता है। एक संगठन में प्रभावी निर्णय लेने के लिए यह सब आवश्यक है। यह किसी विशेष संगठन / संस्थान को चलाने में शामिल संभावित जोखिमों को समझने में भी मदद करता है। व्यवसाय स्थापित करने से पहले कुछ विचार हैं, जो बाद में अर्थव्यवस्था को प्रभावित करेंगे। ये विचार हैं:

- व्यवसाय के सूत्र कैसे व्यवहार करते हैं?
- अर्थव्यवस्था से क्या संबंध है?
- व्यवसाय के विशिष्ट खंड क्या हैं?



चित्र 5.1: एक व्यवसाय के लिए विकास चार्ट नमूना

*स्रोत : Officevibe

व्यवसाय हमेशा एक सामान्य चलने वाला वक्र नहीं होती है। किसी व्यवसाय की वृद्धि हमेशा एक समान नहीं होती है, यह बढ़ सकती है और फिर गिर सकती है या पठार के समान है और फिर से बढ़ सकती है और इसी तरह आगे हो सकता है (चित्र 5.1) यह कर्मचारियों की प्रेरणा पर आधारित होता है। ऐसा सामान्य आर्थिक उतार-चढ़ाव जैसे स्टाफ की जरूरत, इन्वेंट्री, मशीनरी रखरखाव, संसाधन स्तर के कारण होता है।

आज के समय में, आधुनिक संगठन खुली व्यवस्था है। यहां पर बदलावों के अनूकूल इन खुली प्रणालियों के बीच सूचना का अदान-प्रदान होता है, जो कि लगातार बदलती हुई प्रौद्योगिकी और बाजार द्वारा लगाए जाते हैं, समय की आवश्यकता है कि सही समय पर सही जानकारी हो। इसे प्राप्त करने के लिए, जानकारी को निर्णय लेने के लिए प्रभावी रूप में एकत्रित, संगठित, संसाधित और मूल्यांकन किया जाना चाहिए। सूचना प्रणाली ने सूचना प्रसंस्करण की विभिन्न शाखाओं को बढ़ावा दिया है, जहां डेटा प्रसंस्करण प्रभावी जटिल परिस्थितियों में निर्णय लेना और अनुभवी कार्यकर्ताओं की अभूतपूर्व वृद्धि की आवश्यकता बढ़ गई है। किसी भी बुनियादी सूचना प्रणाली में

कंप्यूटर हार्डवेयर और सॉफ्टवेयर, पूर्व-निर्धारित प्रक्रियाएं, विश्लेषणात्मक मॉडल, विभिन्न निर्णय लेने की स्थितियों का नियोजन और नियंत्रण शामिल है।

सूचना प्रणाली का उदय व्यावसायिक वातावरण में बदलाव के कारण हुआ है, जिसने प्रभावी रूप से वैश्वीकरण को जन्म दिया है। वैश्विक बाजार में दुनिया के बाजारों, कार्य समूहों और वितरण प्रणालियों का उचित प्रबंधन और नियंत्रण शामिल है। यह इस बदलते परिवेश के कारण है कि वैश्विक अर्थव्यवस्थाओं ने अपनी संरचना को ज्ञान और सूचना आधारित दृष्टि में बदल दिया है। इस संरचना में नए उत्पादों और सेवाओं, की पीढ़ी उत्पादकता, समय आधारित प्रतियोगिताओं, छोटे (कम) उत्पाद जीवन, निर्माण नेतृत्व और जल्दबाजी में अशांत वातावरण शामिल है। बदलते पर्यावरण के मद्देनजर उद्यम का रूपांतरण भी है, जिसमें कई विशेषताएं हैं जैसे – विकेंद्रीकरण, स्थान स्वतंत्रता, लचीलापन, कम लेन-देन और समन्वय लागत, सशक्तिकरण और सहयोगी टीम का काम (चित्र : 5.2)। कई कारक हैं जो एक व्यापार सूचना प्रणाली के डिजाइन का नेतृत्व करते हैं। जैसे कि :

- संगठन का वातावरण
- संगठन की संरचना
- संगठन की कार्यक्षमता
- संगठन की नीतियां
- निर्णय लेने की क्षमताओं का प्रभावी प्रबंधन
- प्रबंधन की भूमिका

यह समझना भी महत्वपूर्ण है कि एक बार जब सूचना प्रणाली के डिजाइन की कल्पना की जाती है, तो ऑपरेटिंग तत्व होते हैं जिन पर विचार किया जाना चाहिए। ये लेन-देन प्रसंस्करण, मास्टर फाइलों का रखरखाव, प्रक्रिया पूछताछ, रिपोर्ट और इंटरएक्टिव समर्थन हैं। उपयोगकर्ताओं को लेन-देन, अग्रिम रिपोर्ट, तदर्थ (ad hoc) पूछताछ, उपयोगकर्ता मशीन के दस्तावेज होने से सूचना प्रणाली के डिजाइन और परिचालन संरचना से लाभ होता है। इस सूचना प्रणाली और इससे संबंधित अवधारणाओं को समझने के लिए, यह अध्याय किसी भी व्यापार सूचना प्रणाली के सभी महत्वपूर्ण आयामों को एक व्यापक दृष्टिकोण प्रदान करता है।

5.2 डेटा और सूचना

शब्द डेटा की उत्पत्ति 1640 के दशक में हुई थी, जहां इसे पहली बार अंग्रेजी शब्द के रूप में इस्तेमाल किया गया था। इस शब्द का अर्थ 1946 में उपयोग की जाने वाली कंप्यूटर की जानकारी है। शब्द डेटा प्रोसेसिंग की उत्पत्ति और उपयोग पहली बार 1954 में किया गया था। आजकल, इसका दैनिक जीवन में अधिक सारगर्भित उपयोग होता है, जहाँ यह लागू होता है। डेटा के रूप में अवलोकन और तथ्यों को शामिल करता है। कभी-कभी यह माना जाता है कि डेटा और सूचना का अर्थ समान है और विनिमेय करने योग्य हैं। हालांकि, लैटिन शब्द डेटा (डेटम का बहुवचन) और जानकारी अलग-अलग परिप्रेक्ष्य में है। एक डेटा, शाब्दिक अर्थ में, किसी भी वर्ण, शब्द, संख्या का मतलब होगा। यदि इस डेटा को प्रासंगिक संदर्भ में नहीं रखा गया

डेटा हैंडलिंग

है, तो इसका मतलब हमारे लिए कुछ भी नहीं है या कम है। दूसरी ओर, सूचना को संसाधित डेटा के रूप में जाना जाता है, जिसका उपयोग प्रभावी निर्णय लेने के लिए किया जा सकता है।

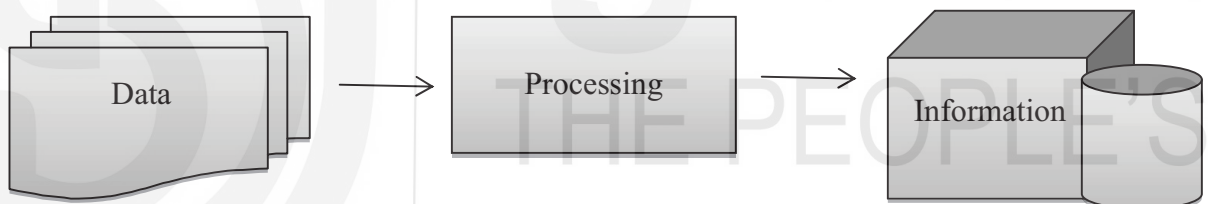
Jaspreet, 7464566835, Mandawali, New Delhi

चित्र 5.2 : डेटा का प्रतिनिधित्व

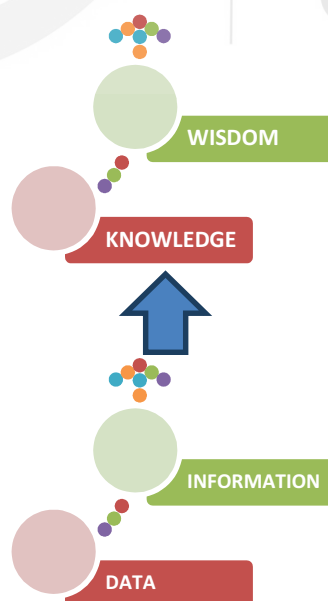
Jaspreet
7464566835
Mandawali
New Delhi

चित्र 5.3 : सूचना का प्रतिनिधित्व

जब डेटा को प्रसंस्करण के माध्यम से रूपांतरित किया जाता है तो उसे सूचना कहा जाता है। चित्र 5.4, डेटा से सूचना तक इस परिवर्तन को दर्शाता है। एक बार संसाधित की गई यह जानकारी ज्ञान और बुद्धिमत्ता देती है जिसका उपयोग प्रभावी निर्णय लेने के लिए किया जा सकता है। सूचना के लिए यह परिवर्तन केवल निर्णय लेने के लिए आवश्यक नींव नहीं है। आगे के चरणों में, इस जानकारी का उपयोग ज्ञान और बुद्धिमत्ता बनाने के लिए किया जाता है। चित्र 5.5, ज्ञान के लिए डेटा के स्तर के बुद्धिमत्ता परिवर्तन को दर्शाता है।



चित्र 5.4 : डेटा का सूचना में परिवर्तन



चित्र 5.5: डेटा का परिवर्तन

किसी भी सूचना प्रणाली के लिए डेटा बहुत महत्वपूर्ण है। यह डेटा कई व्यावसायिक सूचना प्रणालियों के पीछे चलने वाला बल है। प्रभावी ज्ञान के लिए डेटा / सूचना के प्रकार, संदर्भ, अवधारणा, शब्दार्थ की समझ आवश्यक है। बाद के खंडों में, व्यापार सूचना प्रणाली, डेटाबेस प्रबंधन प्रणाली, निर्णय समर्थन प्रणाली की आवश्यकता पर चर्चा की गई है, जो डेटा विश्लेषण की आवश्यकता को और बढ़ाएगी।

5.3 बी.आई.एस. (व्यापार सूचना प्रणाली) का परिचय

औपचारिक रूप से, व्यवसाय एक व्यक्ति की व्यावसायिक गतिविधि है, जिसके पास नियमित व्यवसाय, व्यापार या किसी भी प्रकार का काम है। अर्थव्यवस्था अनिवार्य रूप से विभिन्न क्षेत्रों में चल रहे व्यवसायों पर निर्भर है। यह पैसों के लिए एक दूसरे के रुझान या सेवाओं के आदान प्रदान से भी परिभाषित होता है। वस्तु की कीमत का निर्धारण, मांग में बदलाव, उपभोक्ता पसंद / नापसंद, लागत में परिवर्तन का प्रभाव कुछ ऐसे विचार हैं जो व्यापार को अर्थशास्त्र से जोड़ते हैं। अर्थव्यवस्था के कुशल संचालन के लिए व्यवसाय महत्वपूर्ण है। यह आर्थिक प्रणाली में एक अनिवार्य कारक है। भारत में भी, आर्थिक प्रणाली के प्रभावी विकास के लिए, विभिन्न ऋण और योजनाएं प्रदान की जाती हैं। क्रेडिट उपलब्धता की प्रक्रिया को आसान बनाने के लिए भारत ने छोटे पैमाने के व्यवसायों / युवा / महिला / एससी / एसटी उद्यमियों के लिए विभिन्न वित्तीय निकायों के साथ भागीदारी की है। कुछ लोकप्रिय ऋण योजनाएं, क्रेडिट गारंटी फंड योजना (Credit Guarantee Fund Scheme) (CGFS), मुद्रा (Micro Units Development & Refinance Agency Ltd.) (MUDRA) ऋण योजना और स्टैंड अप इंडिया योजना, भारतीय उद्योग परिसंघ (CII) और फेडरेशन ऑफ इंडियन चेबर्स ऑफ कॉमर्स एंड इंडस्ट्री (FICCI) दो प्रमुख उद्योग चेबर्स हैं, जिन्हें सरकार और उद्योग के बीच की खाई को भरने के लिए बनाया गया है। वे उद्योग के नियमों, नीतियों और संगठन की देखरेख करते हैं।

एक व्यवसाय को विभिन्न वर्गों में वर्गीकृत किया जा सकता है। ये वर्ग संचालन, प्रोटोकॉल, निवेश विकल्प, कानूनी निहितार्थ, आर्थिक निर्भरता और स्वतंत्रताओं को परिभाषित करती हैं। किसी व्यवसाय का स्वामित्व उसके वर्ग को परिभाषित करता है।

जैसे कि यह पैसों के लिए एक दूसरे के सामान या सेवाओं के आदान-प्रदान से भी परिभाषित होता है।

- निजी स्वामित्व
- लाभरहित
- राज्य के स्वामित्व में

जैसा कि पहले कहा गया था, इन वर्गों के अलग-अलग परिचालन परिदृश्य हैं। व्यवसाय का अन्य वर्गीकरण इस प्रकार है:

- साझेदारी
- सीमित भागीदारी
- सीमित देयता कंपनी (LLC)

- सहकारिता (Co-operative)

इन वर्गों में से, एकल स्वामित्व दुनिया में प्रचलित सबसे पुरानी योजनाओं में से एक है। इसमें एक अकेला व्यक्ति गतिविधियों के प्रबंधन और नियंत्रण के लिए जिम्मेदार होता है। जबकि, साझेदारी में, दो या अधिक व्यक्ति एक व्यवसाय में लाभ और हानि (कुछ पूर्व निर्धारित प्रोटोकॉल के तहत) साझा करने के लिए सहमत होते हैं। एकल स्वामित्व और साझेदारी में कुछ बुनियादी अंतर तालिका 5.1 में सूचीबद्ध हैं।

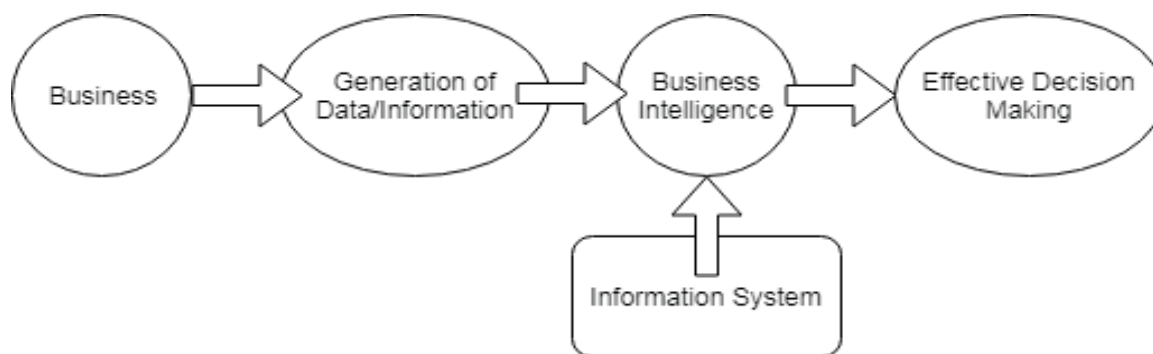
तालिका 5.1: एकल स्वामित्व और साझेदारी के बीच अंतर

क्र.सं.	एकल स्वामित्व	साझेदारी
1.	यह स्थापित करने के लिए सरल है।	इसके लिए दो या दो से अधिक भागीदारों के बीच समझौते की आवश्यकता होती है।
2.	यह एकमात्र व्यक्ति द्वारा नियंत्रित और प्रबंधित किया जाता है।	यह दो या अधिक भागीदारों द्वारा प्रबंधित और नियंत्रित किया जाता है।
3.	निर्णय लेना त्वरित है क्योंकि इसमें कोई भागीदार नहीं है।	निर्णय लेने के लिए सभी भागीदारों की आपसी सहमति की आवश्यकता होती है।
4.	देनदारियों / लाभ / हानि सभी मालिक द्वारा वहन किया जाता है।	साझेदारों द्वारा देनदारियों / लाभ / हानि को साझा किया जाता है।
5.	वित्त केवल एक सीमा तक ही उठाया जा सकता है।	वित्त जुटाने की गुंजाइश अधिक है।

हम व्यापार को सूचना प्रणाली से कैसे संबंधित कर सकते हैं?

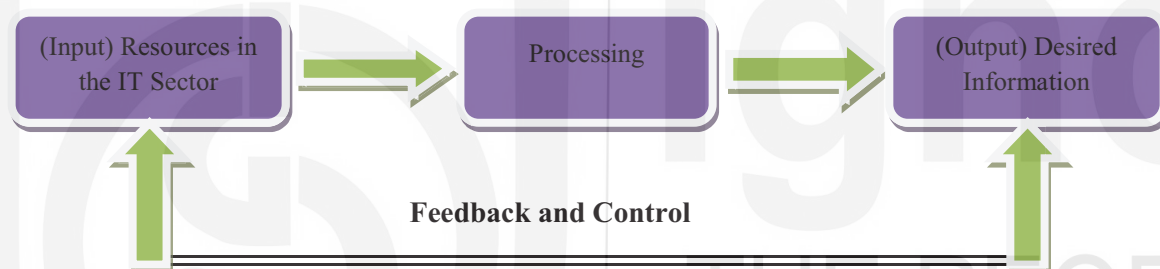
सूचना प्रणाली के भीतर व्यवसाय को कवर करने वाले विभिन्न पहलुओं को चित्र 5.6 में दर्शाया गया है। यह कई शर्तों के सम्मेलन को दर्शाता है जो व्यवसाय संचालन के संदर्भ में हैं। अब हमें एक व्यापार और एक सूचना सिस्टम के बीच के संबंध को समझने की आवश्यकता है। आजकल लोग डेटा एनालिटिक्स (analytics) और आंकड़ों के बारे में बात करते हैं। ये सभी उपयुक्त डेटा के बिना कुछ भी नहीं हैं। यह डेटा व्यापारिक संगठनों द्वारा उत्पन्न किया जाता है, जो आगे ज्ञान की खोज और अन्य संभावित अनुप्रयोगों के लिए उपयोग किया जा सकता है। प्रभावी निर्णय लेने के लिए उत्पन्न आंकड़ों का विश्लेषण किया जाता है। यह विशेष सॉफ्टवेयर की मदद से किया जाता है जिसे सूचना प्रणाली कहा जाता है।

निर्णय लेने के साथ व्यापारिक सूचना की निर्भरता को इन सूचना प्रणालियों के बिना पूरा नहीं किया जा सकता है। ये परिष्कृत सॉफ्टवेयर हैं जो सबसे सुरुचिपूर्ण तरीके से शक्तिशाली जानकारी का प्रबंधन, रखरखाव और भंडारण करते हैं। चित्र 5.6 इस निर्भरता को दर्शाता है, जो व्यापारिक सूचना के सभी प्रमुख घटकों से संबंधित है।



चित्र 5.6: सूचना प्रणाली के साथ व्यापार का संबंध

अब चूंकि, हमने सूचना प्रणाली को औपचारिक रूप दे दिया है, इसलिए एक व्यावसायिक सूचना प्रणाली की वास्तुकला को समझने की आवश्यकता है जिसमें एक संगठन के कुशल कामकाज के लिए अन्य महत्वपूर्ण घटक शामिल हैं। चित्र 5.8, एक व्यापार सूचना प्रणाली के वास्तुशिल्प घटकों की व्याख्या करता है।



चित्र 5.7: व्यवसाय सूचना प्रणाली की वास्तुकला

व्यापक परिप्रेक्ष्य में एक व्यावसायिक सूचना प्रणाली चार बुनियादी कार्यात्मक प्रणालियों की बिक्री कर सकती है – बिक्री और विपणनय औद्योगिक उत्पादन; वित्तीय लेखांकन मानव संसाधन। ये सभी कार्यात्मक प्रणालियां उनके प्रोटोकॉल, उपयोग, रखरखाव और समर्थन में भिन्न हैं। इन कार्यात्मक प्रणाली के हिस्से का एकमात्र सामान्य लक्ष्य प्रभावी समग्र व्यावसायिक विकास है। इन प्रणालियों के अलावा, एक व्यापार सूचना प्रणाली को निर्वाचन क्षेत्र के दृष्टिकोण से वर्गीकृत किया जा सकता है। ये सिस्टम इस प्रकार हैं:

- लेनदेन प्रसंस्करण प्रणाली (टी.पी.एस.)
- प्रबंधन सूचना प्रणाली (एम.आई.एस.)
- निर्णय समर्थन प्रणाली (डी.एस.एस.)
- कार्यकारी सहायता प्रणाली (ई.आई.एस.)

इन बुनियादी प्रणालियों में से, MIS DSS को सहायता प्रदान करता है। इसके बाद, MIS और DSS, EIS को सहायता प्रदान करते हैं और TPS, MIS और DSS को सहायता प्रदान करते हैं। इन प्रणालियों की कार्यक्षमता अगले वर्गों में बताई गई है।

बोध प्रश्न क

1) एक DBMS फाइल प्रोसेसिंग सिस्टम से कैसे भिन्न होता है?

.....

.....

.....

.....

2) स्कीमा और इंस्टेंस के बीच अंतर पर चर्चा करें।

.....

.....

.....

.....

3) सूचना प्रसंस्करण से आप क्या समझते हैं?

.....

.....

.....

.....

.....

4) एकल-स्वामित्व क्या है? साझेदारी पर इसके फायदे क्या हैं?

.....

.....

.....

.....

.....

5.4 डेटा बेस मैनेजमेंट सिस्टम (DBMS)

डेटा बेस मैनेजमेंट सिस्टम (जिसे लोकप्रिय रूप से डी.बी.एम.एस. के रूप में जाना जाता है) में तार्किक रूप से संबंधित डेटा का एक संग्रह होता है और इस डेटा को एक्सेस करने के लिए आवश्यक संचालन का एक सेट होता है। एक डेटाबेस प्रणाली के अंत में शामिल हैं:

- डेटाबेस
- डेटाबेस प्रबंधन प्रणाली

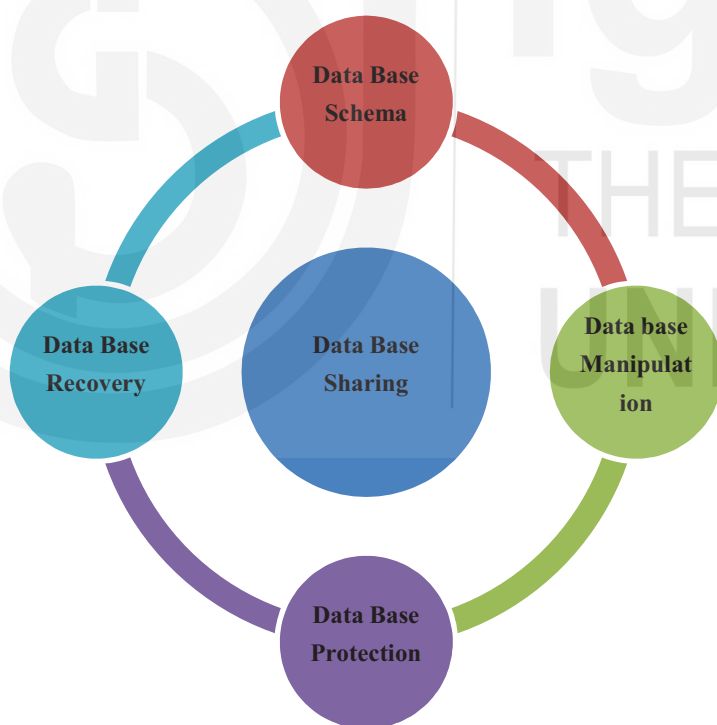
किसी व्यवसाय में चल रही विभिन्न परिचालन इकाइयों से एकत्रित जानकारी / डेटा को भंडार में संग्रहित किया जाता है। इस रिपॉजिटरी (कोष) को डेटा बेस कहा जाता है। एक बार डेटा एकत्र हो जाने के बाद, अब जरूरत है कि डेटा का प्रभावी ढंग से

विश्लेषण किया जाए। इसे प्रभावी ढंग से विश्लेषण करने के लिए किसी को इसे ठीक से संग्रहीत करने की आवश्यकता है ताकि डेटा सुरक्षित हो, सुसंगत हो और अपनी अखंडता बनाए रखे। इस डेटा को कुशलता से प्रबंधित करना भी महत्वपूर्ण है। डेटा का यह कुशल प्रबंधन डेटा बेस मैनेजमेंट सिस्टम (DBMS) के माध्यम से किया जाता है।

एक डी.बी.एम.एस. के निहित गुण निम्नानुसार हैं:

- कुछ पूर्वनिर्धारित पहलू की पहचान की जानी चाहिए, उदाहरण के लिए, एक कंपनी, संस्थान, कॉलेज आदि।
- इसमें तार्किक रूप से सुसंगत डेटा होना चाहिए।
- डेटा के अर्थ विज्ञान को पहले से अच्छी तरह से समझा जाना चाहिए।
- इसे सूचना के संबंधित स्रोत, संबंधित घटनाओं और इच्छित उपयोगकर्ताओं के साथ एक विशिष्ट उद्देश्य के लिए डिजाइन और कार्यान्वित किया जाना चाहिए।

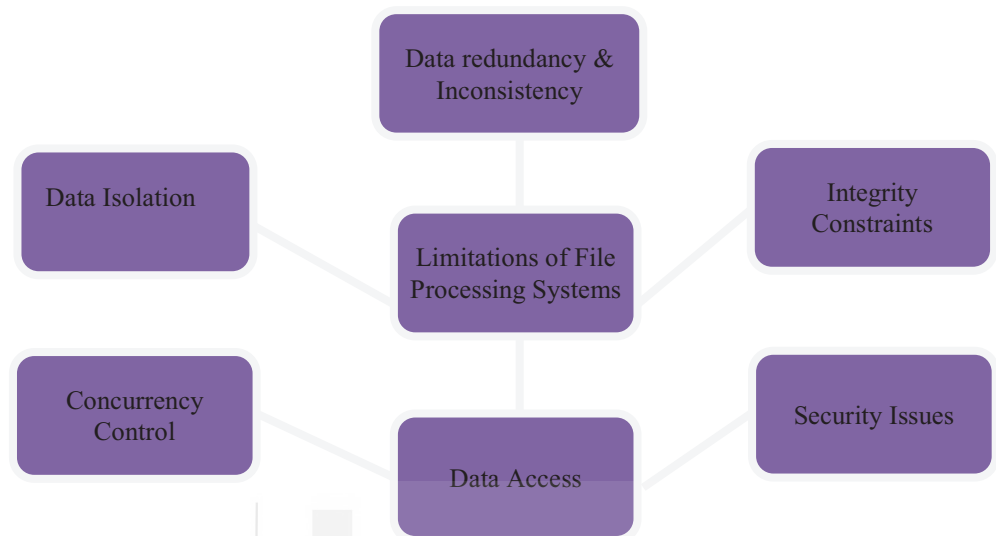
DBMS के प्रमुख कार्य डेटाबेस संरचना को परिभाषित करना, डेटा प्रकार परिभाषा, अद्यतन (updates) करना, हटाना, संग्रहीत जानकारी पर संचालन पढ़ना, संगति को संरक्षित करना, अनधिकृत पहुंच को रोकना और डेटाबेस पुनर्प्राप्ति (चित्र 5.9) को सुविधाजनक बनाना है।



चित्र 5.8 : डेटा बेस प्रबंधन प्रणाली की प्रमुख कार्यशीलता

परंपरागत रूप से, फाइल प्रोसेसिंग सिस्टम (FPS) का उपयोग संस्थानों / संगठनों की रिपॉजिटरी को संभालने के लिए किया जाता था। एफ.पी.एस. में, जिन फाइलों का उपयोग किया गया था उनकी संरचना को आवेदन में हार्ड-कोडित किया जाना था। यद्यपि एफपीएस के साथ हैंडलिंग आसान थी, लेकिन कई प्रमुख अनुप्रयोगों में इसका

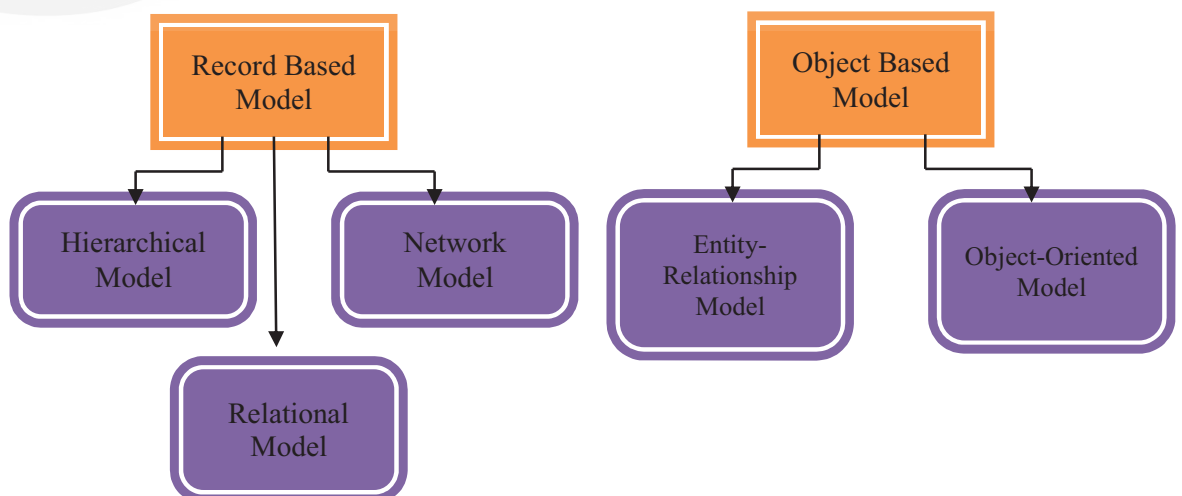
अभाव था। डीबीएमएस के आगमन के साथ, एफपीएस की सीमाओं को आसानी से समझा जा सकता है। चित्र 5.9 में विभिन्न क्षेत्रों में एफपीएस की सीमाएं दी गई हैं।



चित्र 5.9 : डेटा बेस मैनेजमेंट सिस्टम पर फाइल प्रोसेसिंग सिस्टम की सीमाएँ

एक डेटाबेस सिस्टम में कई विशेषताएँ हैं, जो एक एफ.पी.एस. की सीमाओं को पार करती हैं। इसमें डेटा डिक्शनरी शामिल है, इसमें स्टोरेज मैनेजमेंट, ट्रांजैक्शन मैनेजमेंट, कंसीडर कंट्रोल, डेटाबेस रिकवरी और लैंग्वेज इंटरफेस है। इन विशेषताओं को लागू करने के लिए डेटा का वर्णन करने, डेटा संबंधों, डेटा शब्दार्थ और डेटा अखंडता बाधाओं को संभालने के लिए डेटा मॉडल का उपयोग किया जाता है। डेटा मॉडल दो प्रकार के होते हैं:

- वस्तु आधारित मॉडल
- रिकॉर्ड आधारित मॉडल



चित्र 5.10: डेटा मॉडल के प्रकार

ऑब्जेक्ट आधारित मॉडल को एंटीटी रिलेशनशिप (ई-आर) मॉडल और ऑब्जेक्ट ओरिएंटेड मॉडल के रूप में वर्गीकृत किया जाता है जबकि रिकॉर्ड आधारित मॉडल को आमतौर पर श्रेणीबद्ध, नेटवर्क और संबंधपरक मॉडल (चित्र 5.11) के रूप में वर्गीकृत किया जाता है। विभिन्न प्रकार के इन वर्गों में से, संबंधपरक मॉडल सबसे आम और व्यापक रूप से उपयोग किया जाने वाला मॉडल है। यह इसलिए है क्योंकि रिलेशनल मॉडल समझने में आसान है, लागू करना आसान है, डेटा को बनाए रखने के लिए एक मजबूत गणितीय आधार और मजबूत मानक है। अगली उपधारा में संबंधपरक मॉडल को समझाया गया है।

5.4.1 रिलेनेशनल डेटा बेस मैनेजमेंट सिस्टम (RDBMS)

रिलेशनल डेटा बेस मैनेजमेंट सिस्टम (RDBMS) रिलेशनल मॉडल पर आधारित है। यह सबसे अधिक इस्तेमाल किया जाने वाला रिकॉर्ड आधारित मॉडल है। इसमें डेटा को स्टोर करने के लिए तालिकाओं का उपयोग किया जाता है, जिन्हें संबंध भी कहा जाता है। डेटा और तालिकाओं के बीच संबंध को भी तालिका में ही दर्शाया गया है। तालिका 5.2, आर.डी.बी.एम.एस. की व्यापक रूप से प्रयुक्त शब्दावली का वर्णन करती है।

तालिका 5.2: RDBMS की शब्दावली

S.No.	शब्दावली	विवरण
1.	रिश्ता	तालिका (एक अद्वितीय नाम के साथ) को संबंध कहा जाता है।
2.	टुपल	तालिका की प्रत्येक पंक्ति को टुपल कहा जाता है।
3.	गुण	तालिका का प्रत्येक स्तंभ संबंध का एक गुण है।
4.	योजना	डेटाबेस की समग्र संरचना (ब्लूप्रिंट)
5.	उदाहरण	डेटा का वास्तविक संग्रह (डेटा का स्नैपशॉट)
6.	डी.बी.ए.	नियंत्रण के लिए डेटाबेस एडमिनिस्ट्रेटर जिम्मेदार है

5.4.2 डेटा एब्स्ट्रक्शन

डेटा एब्स्ट्रक्शन RDBMS का एक बहुत अभिन्न अंग है। यह आसान दृश्य और डेटाबेस स्कीम को लागू करने में मदद करता है, ताकि निर्भर सुविधाओं में बहुत अधिक परिवर्तन न हो। चित्र इस डेटा को वास्तुशिल्प तरीके से अमूर्त करने के लिए संदर्भित करता है। इसमें तीन प्रमुख स्तर होते हैं: भौतिक स्तर, तार्किक स्तर और बाहरी स्तर।

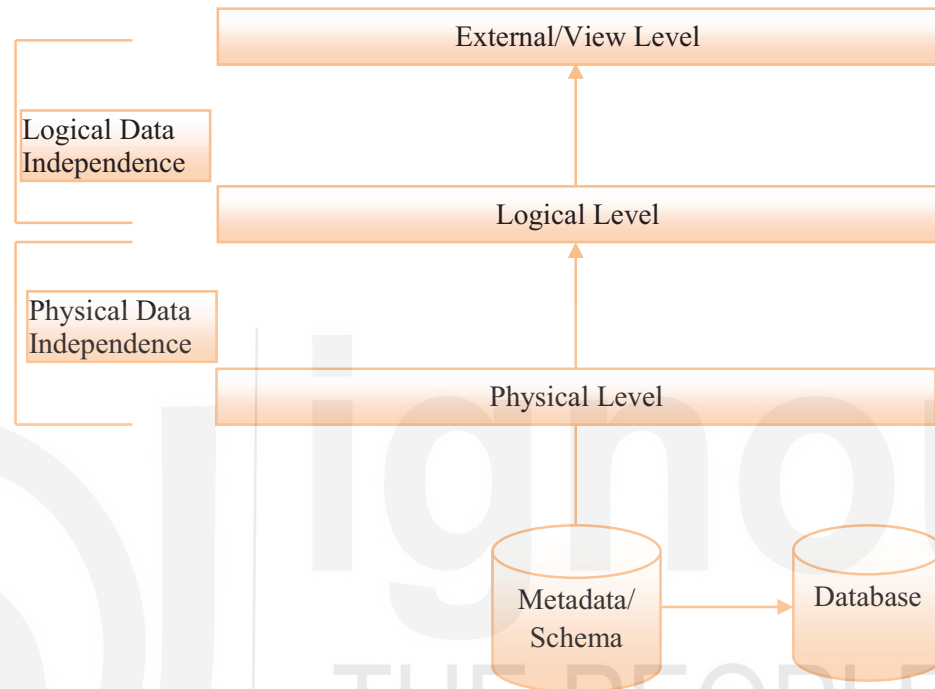
सबसे निचले स्तर पर स्कीमा / डेटाबेस है जो मॉडल के भौतिक दृश्य से जुड़ा है। तार्किक स्तर में बाहरी दृष्टि से आवश्यक सभी वैचारिक जटिलताओं और निर्भरताएं होती हैं। ऊपरी परत बाहरी/दृश्य स्तर है जो उपयोगकर्ता / उपयोगकर्ता अनुप्रयोग से जुड़ा है।

इन स्तरों की निर्भरता का समर्थन करने के लिए, दो डेटा स्वतंत्रता तंत्र परिभाषित किए गए हैं:

डेटा हैंडलिंग

- भौतिक डेटा स्वतंत्रता
- तार्किक डेटा स्वतंत्रता

भौतिक डेटा स्वतंत्रता में, भौतिक स्तर में परिवर्तन तार्किक स्तर के कामकाज और कार्य को प्रभावित करते हैं। तार्किक डेटा स्वतंत्रता में, यदि तार्किक स्तर पर कोई परिवर्तन होता है, तो यह बाह्य स्तर पर स्वयं को प्रतिबिंबित नहीं करेगा। इस प्रकार, इन तंत्रों के साथ डेटा एब्सट्रक्शन में डेटा की स्वतंत्रता बहाल हो जाती है।



चित्र 5.11: अमूर्त डेटा

5.4.3 डेटा बेस एडमिनिस्ट्रेटर

डेटा बेस एडमिनिस्ट्रेटर (DBA) डेटाबेस जिम्मेदारियों के सर्वोच्च नियंत्रक के रूप में कार्य करता है। उनके नियंत्रण में डी.बी.ए. के कार्य इस प्रकार हैं:

- वैचारिक योजना की डिजाइनिंग और इसे किसी भी परिवर्तित आवश्यकताओं के तहत अपडेट करें
- भंडारण संरचना और इसके उपयोग के तरीकों की कुशल कार्यप्रणाली
- यह सुनिश्चित करना कि उपयोगकर्ताओं को वांछित जानकारी मिले
- सिस्टम सुरक्षा सुनिश्चित करें, क्योंकि प्रत्येक उपयोगकर्ता की एक भूमिका होती है और उसके अधिकारों का प्रबंधन करना होता है
- किसी भी दुर्भावनापूर्ण गतिविधि/हमले के खिलाफ डेटाबेस सुनिश्चित करें
- समय-समय पर बैकअप और उचित अभिलेखीय डेटा सुनिश्चित करना
- अचानक व्यवधान / विफलता के मामले में वसूली की प्रक्रिया

- सिस्टम प्रदर्शन, प्रक्रियाओं और आवश्यकताओं के समुचित कार्य को सुनिश्चित करना
- आवश्यक उपकरणों और सॉफ्टवेयर अप-ग्रेडेशन के लिए तकनीकी सहायता प्रदान करना

डी.बी.एम.एस. एक आत्म-वर्णन प्रणाली है, जो डेटा एब्स्ट्रक्शन, मल्टीपल व्यू सपोर्ट, मल्टी-यूजर सपोर्ट, कंसीडर कंट्रोल, कुशल रिकवरी, प्रभावी एक्सेस राइट्स, अनधिकृत एक्सेस को प्रतिबंधित करने, अतिरेक को नियंत्रित करने का काम करती है। डेटा अखंडता की बाधा, समवर्ती पहुंच समर्थन, नियमित बैकअप और पुनर्प्राप्ति तंत्र, आसान अनुकूलनशीलता सुनिश्चित करना और रखरखाव के सफल मानकों को सुनिश्चित करना भी महत्वपूर्ण है।

अब तक, पाठक एक डी.बी.एम.एस., आर.डी.बी.एम.एस. और डी.बी.ए. की भूमिकाओं और जिम्मेदारियों की अवधारणाओं से परिचित हैं। आर.डी.बी.एम.एस. को देखने, प्रबंधित करने और बनाए रखने के लिए, एक संरचित प्रश्न भाषा (SQL) का उपयोग किया जाता है। SQL का उपयोग आर.डी.बी.एम.एस. के साथ बातचीत को प्रबंधित करने के लिए किया जाता है। यह एक गैर-प्रक्रियात्मक भाषा है, जो डेटाबेस से डेटा को कुशलतापूर्वक अपडेट, डालने और हटाने के लिए उपयोग की जाती है। इस में 'गेम-लाइक' सिंटेक्स है और यह लचीला है। आउटपुट को प्रभावित किए बिना एक प्रश्न को कई अलग-अलग तरीकों से लिखा जा सकता है।

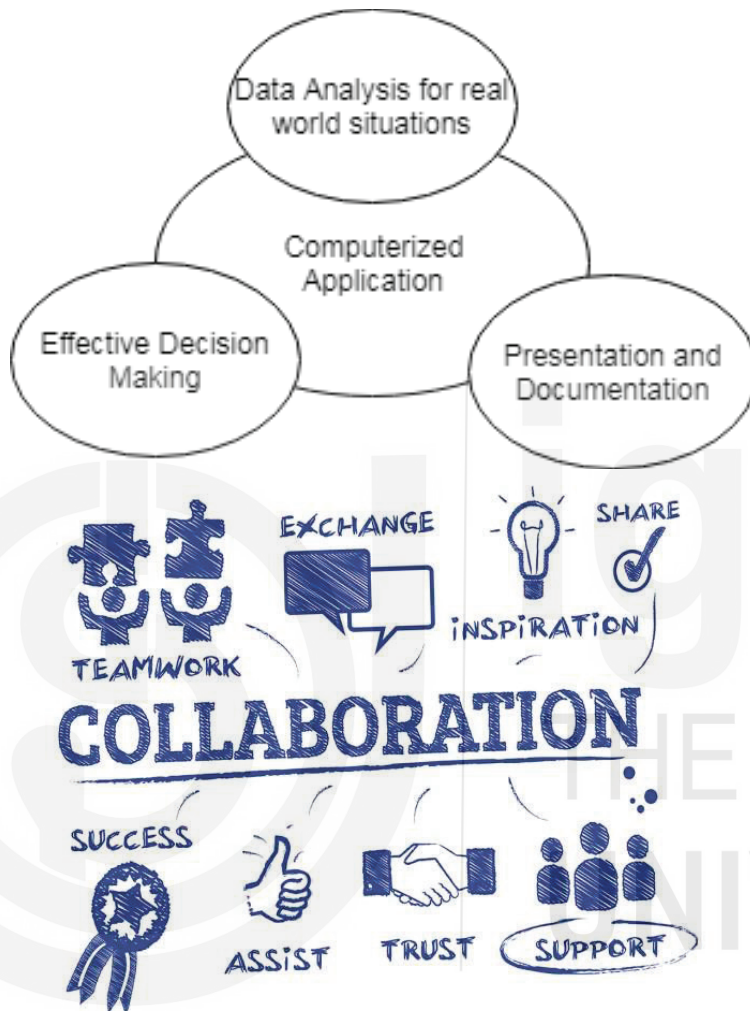
तालिका 5.3 और 5.4 एस.क्यू.एल. प्रश्न बनाने के लिए उपयोग किए जाने वाले विभिन्न प्रकार के एसक्यूएल कमांड और एसक्यूएल ऑपरेटरों को दर्शाती है।

तालिका 5.3: SQL कमांड और उनका विवरण

Sl.No.	SQL कमांड	SQL कमांड विवरण	
1	डेटा परिभाषा भाषा (DDL)	बनाएँ, बेहतर, ड्रॉप	CREATE, ALTER, DROP
2	डेटा हेरफेर भाषा (DML)	सम्मिलित करें, अपडेट करें, हटाएं	INSERT, UPDATE, DELETE
3	डेटा क्वेरी भाषा (DQL)	चयन करें <विशेषताओं की सूची>	SELECT <list of attributes> FROM <List of tables> WHERE <attributes of tables> GROUP BY <list of attributes> HAVING <predicate having aggregate values> ORDER BY ACS/DESC
4	डेटा नियंत्रण भाषा (DCL)	<तालिकाओं की सूची > से	GRANT, REVOKE
5	लेन-देन नियंत्रण विवरण (TCS)	कहाँ <तालिकाओं की विशेषताएँ>	SET TRANSACTION, SAVEPOINT, COMMIT, ROLLBACK

तालिका 5.4 : एस. क्यू. एल. ऑपरेटरस

निर्णय समर्थन प्रणाली प्रशिक्षण इनपुट (अल्पविकसित मापदंडों) पर काम करती है और फिर निर्णय, रिपोर्ट जैसे लक्ष्य का उत्पादन करती है। डीएसएस के विभिन्न प्रकार हैं: संचार-प्रेरित, डेटा संचालित, दस्तावेज संचालित, ज्ञान संचालित और मॉडल संचालित। DSS का मूल कार्य सूचना और मॉडल बनाना है, फिर उदाहरण के साथ अवलोकन के तहत स्थिति को विस्तृत करना, डोमेन इंटेलिजेंस के लिए ज्ञान को संसाधित करना जो अंततः डेटा विश्लेषण (चित्र 5.13) के लिए आवश्यक है।



चित्र 5.12: डिसीजन सपोर्ट सिस्टम की समग्र कार्यप्रणालियाँ

आज जटिल वातावरण में निर्णय लेना कठिन है, क्योंकि सूचना अधिभार और डेटा में विकृति है। इसलिए, निर्णय निर्माता “तथ्यात्मक सीखने और निर्णय लेने” के दृष्टिकोण पर जोर देते हैं।



*स्रोत : हेल्थ केटोलिस्ट

चित्र 5.13: कई विकल्पों के साथ प्रबंधकीय निर्णय लेना कठिन है

यह दृष्टिकोण न केवल समझने में आसान है, बल्कि निर्णय लेने की गुणवत्ता में सुधार करता है। इस प्रकार, निर्णय लेने की प्रक्रिया पारंपरिक दृष्टिकोण के विपरीत अधिक कुशल है। यह समझना भी महत्वपूर्ण है कि विश्लेषण किए जाने वाले डेटा की मात्रा बहुत तेज गति से बढ़ रही है। बर्नार्ड मार द्वारा फोर्ब्स के एक हालिया लेख के अनुसार, मई 2018 में, यह बताया गया है कि इंटरनेट पर हर रोज 2.5 क्विंटल बाइट्स डेटा बनाया जाता है। इस दिमागी आंकड़ों के साथ, यह ध्यान रखना आवश्यक है कि स्वचालित उपकरण होने की आवश्यकता है, जो इस विशाल डेटा का प्रभावी ढंग से विश्लेषण कर सकते हैं। व्यावसायिक परिदृश्य में, प्रबंधकों को जटिल वातावरण में निर्णय लेने की आवश्यकता होती है और उन्हें निर्णय के साथ शामिल लाभों और जोखिमों को समझना होता है। ऐसे मामलों में, प्रबंधक सूचित निर्णय ले सकते हैं और अपनी पसंद के प्रभावी डिजाइन और कार्यान्वयन का समर्थन कर सकते हैं।

उचित रूप से डिजाइन किया गया डी.एस.एस. एक कंप्यूटर आधारित सॉफ्टवेयर है, जो निर्णयकर्ता को जटिल समस्याओं को हल करने के लिए कच्चे डेटा, दस्तावेजों या व्यक्तिगत ज्ञान से उपयोगी जानकारी संकलित करने में मदद करता है। एक डी.एस.एस. की संरचना में मुख्य रूप से शामिल हैं:

प्रबंधक और कर्मचारी विशेषज्ञ

- कर्मचारी सहायक
- विशेषज्ञ उपकरण उपयोगकर्ता
- व्यापार विश्लेषक
- डी.एस.एस. सुविधा
- डी.एस.एस. की प्रमुख कार्यप्रणालियों को संक्षेप में प्रस्तुत किया जा सकता है:
- आम, व्यक्तियों या समूहों को सहायता प्रदान करें
- निर्णय लेने की प्रक्रिया को नियंत्रित और प्रबंधित करना
- व्यक्तिगत, समूह या अन्योन्याश्रित निर्णयों का समर्थन
- अनुकूली और उपयोगकर्ता के अनुकूल इंटरफेस
- संरचित या अर्ध संरचित स्थितियों में निर्णय लेने का समर्थन

निर्णय लेने की प्रक्रिया के लिए डेटा के विश्लेषण के पारंपरिक तरीकों में कुछ कमियां हैं। इनमें से कुछ में शामिल हैं – कम दक्षता, मैनुअल त्रुटि, व्यक्तिगत पूर्वाग्रह, ऊपर परीक्षण इन सीमाओं को पार करने के लिए, विभिन्न डीएसएस सहायता उपकरण उपलब्ध हैं। ये उपकरण निर्णय लेने की प्रक्रिया के विभिन्न महत्वपूर्ण पहलुओं के आसान प्रबंधन और विजुअलाइजेशन में मदद करते हैं। लोकप्रिय उपकरणों में से एक 'डीएसएस जनरेटर' है। एक DSS जेनरेटर हार्डवेयर और सॉफ्टवेयर का एक विशेष पैकेज है, जिसमें DSS के तौर-तरीकों को जल्दी और आसानी से बनाने की कार्यक्षमता होती है। जनरेटर लचीला और अनुकूली है और विशिष्ट DSS के व्यापक स्पेक्ट्रम के आसान विकास की अनुमति देता है। आज के जटिल वातावरण के साथ इसकी अतिरिक्त अनुकूलता के कारण, इसने एक्सेल और एक्सपर्ट च्वाइस को बाहर कर दिया है।

बड़े डेटाबेस, सॉफ्टवेयर इंजीनियरिंग, ऑप्टिमाइजेशन, आर्टिफिशियल इंटेलिजेंस और मानव कंप्यूटर इंटरैक्शन में तकनीक और तकनीकी प्रगति एक डीएसएस की कार्यक्षमता को बढ़ाती रहेगी।

5.6 एंटरप्राइज रिसोर्स प्लानिंग (ERP)

एंटरप्राइज रिसोर्स प्लानिंग (ईआरपी) एक प्लानिंग सिस्टम है जो मटेरियल रिसोर्स प्लानिंग II (MRP II) से विकसित होता है, जिसका उद्देश्य LAN, WAN, इंटरनेट आदि जैसे नेटवर्क का उपयोग करके ग्राहक, विक्रेता और निर्माता के बीच सूचना का एकीकरण प्रदान करना है। MRP II फिर से विकसित हुआ है। एम.आर.पी. सिस्टम से जो एक तकनीक है जो किसी दिए गए उत्पाद संरचना के लिए मास्टर प्रोडक्शन शेड्यूल (एम.पी.एस.) से प्राप्त अंतिम उत्पाद मांगों की पड़ताल करता है। इस उत्पाद संरचना को बिल ऑफ मटीरियल (बी.ओ.एम.) में सूची पर विचार करके नियोजित आदेशों की अनुसूची में ले जाया जाता है।

विभिन्न लाभों के बावजूद, MRP II में कुछ कमियां हैं:

- संसाधनों को साझा करने के लिए कई कार्यात्मक क्षेत्रों का अप्रभावी एकीकरण
- आवेदन में, प्रत्येक लेनदेन को अलग से व्यवहार किया जाता है
- कोई सामान्य कार्यक्षमता प्रदान नहीं की जाती है; विशिष्ट कार्य विशिष्ट अनुप्रयोगों को पूरा करते हैं।

कारोबारी माहौल के समग्र विकास के लिए उद्योग की मांगों को समझने की जरूरत है। ये मांगें लागत नियंत्रण की पहल, लागत विश्लेषण (उत्पाद आधारित या ग्राहक आधारित), व्यवसाय की आवश्यकता को बदलने, प्रभावी निर्णय लेने और कई और अधिक हो सकती हैं। ऐसी मांगों को संभालने के लिए कई एप्लिकेशन या प्लानिंग सिस्टम उपलब्ध हैं। उनमें से कुछ हैं:

- प्रबंधन सूचना प्रणाली (MIS)
- एकीकृत सूचना प्रणाली (IIS)
- कार्यकारी सूचना प्रणाली (EIS)
- कॉर्पोरेट सूचना प्रणाली (CIS)
- एंटरप्राइज वाइड सिस्टम (EWS)
- सामग्री संसाधन योजना (MRP)
- विनिर्माण संसाधन योजना (MRP II)
- मनी रिसोर्स प्लानिंग (MRP III)

एमआरपी II की तुलना में, ईआरपी मांग और आपूर्ति की भविष्यवाणी और संतुलन बनाने में प्रभावी है। अगले भाग में, मैनेजमेन्ट इन्फॉर्मेशन सिस्टम (MIS) का परिचय प्रबंधन प्रणाली के काम की बेहतर समझ प्राप्त करने के लिए प्रदान किया जाता है।

अब इस समय तक, पाठक बिजनेस इंटेलिजेंस (बीआई) और ईआरपी से परिचित हैं। दो बहुत महत्वपूर्ण अवधारणाओं को पेश करने का सही समय है: ऑन-लाइन विश्लेषणात्मक प्रसंस्करण (ओएलएपी) और ऑन-लाइन ट्रांसेक्शनल प्रोसेसिंग (ओएलटीपी)। Table 5.5, OLAP और OLTP के बीच अंतर को सामान्य करता है।

तालिका 5.5: OLAP और OLTP में अंतर

S.No	ऑनलाइन विश्लेषणात्मक प्रक्रिया (OLAP)	ऑनलाइन ट्रांसेक्शनल प्रोसेसिंग (OLTP) है।
1	इसमें अधिक लेनदेन (जटिल SQL क्वेरी) है	इसमें अपेक्षाकृत कम लेन-देन (सरल SQL क्वेरी) है।
2	इसमें अनुक्रमिक पहुंच और अपडेट शामिल हैं।	इसमें यादृच्छिक अद्यतन हैं।
3	डेटा को आयामी मॉडलिंग का उपयोग करके बनाया गया है।	डेटा को ER (Entity-Relationship) मॉडलिंग का उपयोग करके बनाया गया है
4	उदाहरण: बिजनेस इंटेलिजेंस (BI)	उदाहरण: एंटरप्राइज रिसोर्स प्लानिंग (ईआरपी)

बी.आई फ्रेमवर्क में मजबूत विश्लेषणात्मक अनुप्रयोग, संतुलित डैशबोर्ड और रिपोर्ट करने के लिए उच्च गति तक पहुंच है, जबकि ईआरपी एक ओएलटीपी होने के रूप में और जब वे होते हैं तो लेनदेन को रिकॉर्ड करता है। ERP सॉफ्टवेयर उच्च गति लेनदेन और न्यूनतम डिस्क स्थान उपयोग से निपटने के लिए डिजाइन किया गया है। यह बीआई संगठनों को चुस्त बनाता है और भविष्य की केंद्रित क्षमताएं रखता है, जबकि ईआरपी एक संगठन के लिए दक्षता प्रदान करता है। बीआई और ईआरपी दोनों के साथ समानता यह है कि वे व्यवसाय सुधार की ओर केंद्रित हैं और बहुत महत्वपूर्ण परिणाम देते हैं।

5.7 प्रबंधन सूचना प्रणाली (MIS)

सूचना प्रणाली को मोटे तौर पर दो प्रकारों में विभाजित किया जाता है: प्रबंधन सहायता प्रणाली और ऑपरेशन समर्थन प्रणाली। प्रबंधन सूचना प्रणाली (MIS) एक प्रकार की सूचना प्रणाली है जो प्रबंधन सहायता प्रणाली की श्रेणी में आती है। एक MIS एक DSS से अलग होता है। तालिका 5.6, उन प्रमुख पहलुओं पर प्रकाश डालती है जिन पर दोनों अलग-अलग हैं।

तालिका 5.6: MIS और DSS के बीच अंतर के प्रमुख पहलू

S.NO	पहलू	प्रबंधन सूचना प्रणाली (MIS)	निर्णय समर्थन प्रणाली (DSS)
1	निर्णय लेने का स्तर	प्राथमिक स्तर	उच्चतम स्तर
2	ऑपरेशनल मोड	रिपोर्ट और प्रलेखन	पसंद और उनके विश्लेषण का अभ्यास करें
3	उद्देश्य	कार्यकारी कुशलता	कंपनी के लिए प्रभावी निर्णय लेना
4	इनपुट	विभिन्न लेनदेन प्रसंस्करण इकाइयों से बड़ी मात्रा में डेटा	डेटा की कम मात्रा क्योंकि डेटा डी.एस.एस. में पहुंचने तक फिल्टर हो जाता है
5	उत्पादन	सारांश रिपोर्ट	निर्णय विश्लेषण

MIS के उदाहरण बैंक प्रबंधन प्रणाली, रेलवे प्रबंधन प्रणाली, इन्वेंटरी प्रबंधन प्रणाली हैं। किसी भी एमआईएस में कॉर्पोरेट कर्मचारियों के बीच प्रभावी संचार के लिए आवश्यक व्यापक रिपोर्ट जनरेशन शामिल है। विभिन्न परिसंपत्तियों के बावजूद जो एमआईएस प्रदान करता है, यह कई सीमाओं से भी ग्रस्त है। ऐसे क्षेत्र हैं जहां प्रबंधन प्रणाली को विभिन्न निर्भर और स्वतंत्र कारकों के बीच संबंधों को समझने की आवश्यकता होती है। ये क्षेत्र इस प्रकार हैं:

- रखरखाव
- लागत
- ग्राहक संबंध
- विभिन्न मॉड्यूल का उपयोग
- ग्राहक की आवश्यकताएं
- संगठन की विशेष आवश्यकताओं से अनभिज्ञ

किसी भी एम.आई.एस. का प्राथमिक उद्देश्य प्रबंधकों द्वारा आवश्यक जानकारी प्रदान करना है, जो उन्हें प्रभावी निर्णय लेने में सक्षम करेगा। प्रबंधक उन समस्याओं की पहचान करने के लिए एक साधन के रूप में एमआईएस का उपयोग कर सकते हैं, जिसका बाद में वह सामना कर सकते हैं। यह समस्या के अच्छे समाधान के निर्माण में भी मदद करता है। यह विभिन्न स्तरों पर प्रबंधकों को तुरंत पहुँच प्रदान करता है। यह भी समझा जाना चाहिए कि एमआईएस डिजाइन करते समय, प्रबंधकों को कर्मचारियों के व्यवहार संबंधी पहलुओं पर विचार करना चाहिए।

5.8 जनरल डेटा प्रोटेक्शन रेगुलेशन (GDPR)

आज के डिजिटलीकरण के युग में, लोगों के पास अपने व्यक्तिगत डेटा का बहुत सारा हिस्सा ऑनलाइन है। इसकी वजह है कि ऑनलाइन एप्लिकेशन का इस्तेमाल बढ़ गया है। इसलिए डेटा गोपनीयता की जरूरत को समझना जरूरी है। दुनिया भर की कंपनियां बहुत सारे व्यक्तिगत डेटा सुरक्षित और संग्रहित कर रही हैं, जिन्हें विनियमन की आवश्यकता है ताकि लोगों के व्यक्तिगत जीवन को प्रभावित होने से बचाया जा सके। एक व्यवसायिक व्यक्ति के रूप में, विभिन्न डेटा सुरक्षा कानूनों / विनियमों की समझ होना आवश्यक है। डेटा गोपनीयता की अवधारणा महत्वपूर्ण व्यक्तिगत जानकारी, नागरिक विशिष्ट पहचान, स्वास्थ्य और चिकित्सा रिकॉर्ड, वित्तीय डेटा, क्रेडिट / डेबिट कार्ड नंबर, निवास की जन्मतिथि, जन्म की तारीख आदि जैसी अधिक बुनियादी व्यक्तिगत जानकारी भर में फैली हुई है। यह सभी जानकारी व्यक्तिगत रूप से पहचान योग्य सूचना (PII) के अंतर्गत आती है और PII को सुरक्षित करने की आवश्यकता है। इसे देखते हुए, 1995 में यूरोपीय संघ ने डेटा संरक्षण निर्देश को आधिकारिक तौर पर निर्देश 95/46 / EC के रूप में जाना गया। व्यक्तिगत डेटा के प्रसंस्करण और संचलन के संरक्षण के उद्देश्य से निर्देश। चित्र 5.15, इस निर्देश की आधिकारिक सूचना दिखाता है।



EUR-Lex
Access to European Union law

31995L0046

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Official Journal L 281 , 23/11/1995 P. 0031 - 0050

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

Source: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>

जनरल डेटा प्रोटेक्शन रेगुलेशन के संक्षिप्त रूप में, जी.डी.पी.आर. द्वारा कई निर्देशों के अलावा इस निर्देश का समर्थन किया गया था। दिसंबर 2015 में, यूरोपीय संसद डेटा संरक्षण के लिए नए नियम तैयार करने के लिए एक समझौते पर पहुंची, “ईयू जनरल डेटा प्रोटेक्शन रेगुलेशन”। चित्र 5.14, जी.डी.पी.आर. कार्यात्मकताओं की प्रकृति को दर्शाता है।



स्रोत: endpoint protector

चित्र 5.14: सामान्य डेटा संरक्षण विनियमन का सचित्र प्रतिनिधित्व

जी.डी.पी.आर. का उद्देश्य सुरक्षा के विभिन्न स्तरों जैसे डेटा सुरक्षा के लिए बदलती आवश्यकताओं, व्यापक दायरे, इसके प्रवर्तन और दंड के गैर-अनुपालन के लिए डीपीडी को चरणबद्ध करना है। उनके बीच प्रमुख नीतिगत मतभेद तालिका 5.7 में सारणीबद्ध हैं। सभी विस्तारित कार्यात्मकताओं के अलावा, जीडीपीआर (GDPR) उन व्यवसायों के लिए एक सरल विनियामक वातावरण का अनुसरण करता है, जो उपयोगकर्ता के PII को संभालते हैं।

तालिका 5.7: डेटा प्रोटेक्शन डायरेक्टिव (DPD) बनाम जनरल डेटा प्रोटेक्शन रैनुलेशन (GDPR)

S.No	नीति जारी करना	डेटा प्रोटेक्शन डायरेक्टिव (DPD)	जनरल डेटा प्रोटेक्शन रैनुलेशन (GDPR)
1	व्यक्तिगत डेटा को फिर से परिभाषित करना	DPD ने नाम, पते, ईमेल, फोन, नागरिक की विशिष्ट आईडी जैसे डेटा के लिए गोपनीयता को शामिल किया	DPD में शामिल आंकड़ों के अलावा, GDPR में एक व्यक्ति (बायोमेट्रिक, आनुवंशिक, आर्थिक, सामाजिक पहचान) से संबंधित कोई भी जानकारी शामिल है।
2	व्यक्तिगत अधिकार	DPD में ऑफ्ट-आउट सहमति बहुत अनुकूल नहीं है	GDPR लोगों को उनके डेटा तक पहुंचने का अधिकार और भूल जाने का अधिकार देता है जहां उपयोगकर्ता स्पष्ट रूप से अपने डेटा डिस्प्ले के लिए विकल्प चुन सकता है।

डेटा हैंडलिंग

3	डेटा कंट्रोलर बनाम डेटा प्रोसेसर	डेटा के गलत इस्तेमाल के लिए केवल डेटा कंट्रोलर जिम्मेदार थे	डेटा प्रोसेसर और डेटा नियंत्रक गोपनीयता सुरक्षा की निगरानी के अनुपालन में हैं।
4	शासन और सुरक्षा	कड़े प्रवर्तन का अभाव	GDPR “डिजाइन द्वारा गोपनीयता” का पालन करता है और स्वचालित डेटा प्रोसेसिंग गतिविधियों का आकलन करने के लिए संगठन को प्रोत्साहित करता है।

बोध प्रश्न ख

- 1) भारत में छोटे व्यवसायों के समर्थन और स्थापना के लिए कौन सी योजनाएं उपलब्ध हैं?

.....

.....

.....

.....

.....

- 2) एक व्यवसाय के उद्देश्य क्या हैं? उदाहरणों की सहायता से समझाइए।

.....

.....

.....

.....

.....

- 3) सूचना प्रौद्योगिकी में सुरक्षा के मुद्दे क्या हैं?

.....

.....

.....

.....

- 4) दो प्रकार के डेटा मॉडल का नाम बताइए।

.....

.....

.....

.....

व्यापार और अर्थव्यवस्था के बीच एक अच्छा संबंध बनाए रखने के लिए, हमेशा अंतिम-उपयोगकर्ता (आपके उत्पाद का) को जानना फायदेमंद होता है। व्यावसायिक सूचना प्रणाली को एक उद्यम में प्रभावी निर्णय लेने का समर्थन करने के लिए डिजाइन किया गया है। प्रबंधन सूचना प्रणाली एक कम्प्यूटरीकृत डेटाबेस है, जो एक उद्यम की वित्तीय प्रबंधन की जानकारी को संभालने, प्रबंधित करने, संग्रहीत करने, स्टोर करने के लिए डिजाइन किया गया है और किसी भी प्रबंधन प्रणाली के लिए पहलुओं का उत्पादन करता है। कुशलता से काम करने के लिए बिजनेस प्लान, मार्केट एनालिसिस, सेल्स एंड फंडिंग, ऑर्गनाइजेशन मैनेजमेंट और फाइनेंशियल प्रोजेक्शन होते हैं।

अब एक दिन लोग डेटा एनालिटिक्स और आंकड़ों के बारे में बात करते हैं। ये शर्तें उपयुक्त डेटा के बिना कुछ भी नहीं हैं। यह डेटा व्यापारिक संगठनों द्वारा उत्पन्न किया जाता है, जो आगे ज्ञान की खोज और अन्य संभावित अनुप्रयोगों के लिए उपयोग किया जा सकता है। प्रभावी निर्णय लेने के लिए उत्पन्न आंकड़ों का विश्लेषण किया जाता है। यह विशेष सॉफ्टवेयर की मदद से किया जाता है जिसे सूचना प्रणाली कहा जाता है।

डेटा बेस मैनेजमेंट सिस्टम (जिसे लोकप्रिय रूप से डी.बी.एम.एस. के रूप में जाना जाता है) तार्किक रूप से संबंधित डेटा का एक संग्रह होता है और इस डेटा को एक्सेस करने के लिए आवश्यक संचालन का एक सेट होता है। एक डाटाबेस सिस्टम में अंततः बेस और डाटा बेस मैनेजमेंट सिस्टम होता है। किसी व्यवसाय में चल रही विभिन्न परिचालन इकाइयों से एकत्रित जानकारी / डेटा को भंडार में संग्रहित किया जाता है। इस कोश को डेटा बेस कहा जाता है। एक बार डेटा एकत्र हो जाने के बाद, अब जरूरत है कि डेटा का प्रभावी ढंग से विश्लेषण किया जाए।

रिलेशनल डेटा बेस मैनेजमेंट सिस्टम (RDBMS) रिलेशनल मॉडल पर आधारित है। यह सबसे अधिक इस्तेमाल किया जाने वाला रिकॉर्ड आधारित मॉडल है। डेटा एब्स्ट्रक्शन RDBMS का एक बहुत अभिन्न अंग है। यह आसान दृश्य और डेटाबेस योजना को लागू करने में मदद करता है ताकि निर्भर सुविधाओं में बहुत अधिक परिवर्तन न हो।

एक डिसीजन सपोर्ट सिस्टम (DSS) एक कंप्यूटर एप्लिकेशन है जो डेटा एनालिसिस (संगठनात्मक / संस्थागत) करता है और इसे इस तरह से प्रस्तुत करता है ताकि उपयोगकर्ता प्रभावी रूप से व्यावसायिक निर्णय ले सकें। यह “निर्णय → अधिनियम → समीक्षा” के मूल पर काम करता है। निर्णय समर्थन प्रणाली प्रशिक्षण इनपुट (अल्पविकसित मापदंडों) पर काम करती है और फिर निर्णय, रिपोर्ट जैसे लक्ष्य का उत्पादन करती है।

एंटरप्राइज रिसोर्स प्लानिंग (ईआरपी) एक प्लानिंग सिस्टम है जो मटेरियल रिसोर्स प्लानिंग II (MRP II) से विकसित होता है, जिसका उद्देश्य LAN, WAN, इंटरनेट आदि जैसे नेटवर्क का उपयोग करके ग्राहक, विक्रेता और निर्माता के बीच सूचना का

एकीकरण प्रदान करना है। MRP II फिर से विकसित हुआ है। एमआरपी सिस्टम एक तकनीक है, जो किसी दिए गए उत्पाद संरचना के लिए मास्टर प्रोडक्शन शेड्यूल (एम.पी.एस.) से प्राप्त अंतिम उत्पाद मांगों की पड़ताल करता है।

जी.डी.पी.आर. का उद्देश्य सुरक्षा के विभिन्न स्तरों जैसे डेटा सुरक्षा के लिए बदलती आवश्यकताओं, व्यापक दायरे, इसके प्रवर्तन और दंड के गैर-अनुपालन के लिए जी.पी.डी. को चरणबद्ध करना है। सभी विस्तारित कार्यात्मकताओं के अलावा, GDPR उन व्यवसायों के लिए एक सरल विनियामक वातावरण का अनुसरण करता है, जो उपयोगकर्ता के PII को संभालते हैं।

5.10 शब्दावली

व्यवसाय (Business) : व्यवसाय एक ऐसे व्यक्ति की व्यावसायिक गतिविधि है, जिसके पास नियमित व्यवसाय, व्यापार या किसी भी प्रकार का कार्य है। यह वस्तुओं या सेवाओं के आदान-प्रदान या धन के लिए एक दूसरे के द्वारा भी परिभाषित किया जाता है।

सूचना प्रौद्योगिकी (Information Technology) : सूचना प्रौद्योगिकी (आईटी) किसी भी कंप्यूटर, भंडारण, नेटवर्किंग और अन्य भौतिक उपकरणों, बुनियादी ढांचे और प्रक्रियाओं का उपयोग, इलेक्ट्रॉनिक डेटा के सभी रूपों को बनाने, संसाधित करने, स्टोर करने, सुरक्षित करने और विनिमय करने के लिए है।

डेटा गोपनीयता और संरक्षण (Data Privacy and Protection) : डेटा संरक्षण अनधिकृत पहुंच के खिलाफ डेटा हासिल करने के बारे में है। डेटा गोपनीयता अधिकृत पहुंच के बारे में है कि यह किसके पास है और कौन इसे परिभाषित करता है। इसे देखने का एक और तरीका यह है: डेटा सुरक्षा अनिवार्य रूप से एक तकनीकी समस्या है, जबकि डेटा गोपनीयता एक कानूनी है।

व्यापारिक सूचना (Business Intelligence) : व्यापारिक सूचना प्रक्रियाओं, आर्किटेक्चर, और प्रौद्योगिकियों का एक सेट है जो कच्चे डेटा को अर्थपूर्ण सूचनाओं में परिवर्तित करता है, जो लाभदायक व्यावसायिक कार्यों को चलाता है। यह सॉफ्टवेयर और सेवाओं का एक मेल है जो डेटा को कार्रवाई योग्य बुद्धिमत्ता और ज्ञान में परिवर्तित करता है।

डेटा और सूचना (Data and information) : एक डेटा, शाब्दिक अर्थ में, किसी भी वर्ण, शब्द, संख्या का मतलब होगा। यदि इस डेटा को प्रासंगिक संदर्भ में नहीं रखा गया है, तो इसका मतलब हमारे लिए कुछ भी नहीं है। दूसरी ओर, जानकारी को संसाधित डेटा के रूप में जाना जाता है, जिसका उपयोग प्रभावी निर्णय लेने के लिए किया जा सकता है।

डिसीजन सपोर्ट सिस्टम (Decision Support System) : एक डिसीजन सपोर्ट सिस्टम (DSS) एक कंप्यूटर एप्लिकेशन है, जो डेटा का विश्लेषण करता है और इसे इस तरह से प्रस्तुत करता है ताकि उपयोगकर्ता व्यावसायिक निर्णय प्रभावी ढंग से ले सकें।

डेटा एक्स्ट्रक्शन (Data Abstraction) : डेटा एक्स्ट्रक्शन RDBMS का एक बहुत अभिन्न अंग है। यह आसान दृश्य और डेटाबेस योजना को लागू करने में मदद करता है ताकि निर्भर सुविधाओं में बहुत अधिक परिवर्तन न हो।

5.11 स्वपरख प्रश्न

- 1) डेटा अमूर्तता के तीन स्तरों की व्याख्या करें। भौतिक और तार्किक डेटा स्वतंत्रता के बीच अंतर।
- 2) डी.बी.एम.एस. में डेटा डिक्शनरी की भूमिका को समझाइए।
- 3) सूचनात्मक रणनीतिक निर्णय लेने की विशेषताओं पर चर्चा करें।
- 4) व्यावसायिक बुद्धिमता में डेटा मॉडल के महत्व को स्पष्ट करें।
- 5) सूचना रणनीति दस्तावेज की भूमिका क्या है?
- 6) व्यापारिक संगठनों में केंद्रीकृत और विकेंद्रीकृत सूचना के लाभों और सीमाओं पर चर्चा करें।

नोट: ये प्रश्न आपके अभ्यास के लिए हैं। इनके उत्तर लिखने का अभ्यास करें किंतु उत्तरों को विश्वविद्यालय में मूल्यांकन के लिए न भेजें। प्रश्नों के उत्तर लिखकर आप स्वयं अपनी प्रगति की जाँच कर सकते हैं।

THE PEOPLE'S
UNIVERSITY

इकाई 6 व्यापार में आई.टी. सुरक्षा

इकाई की रूपरेखा

- 6.0 उद्देश्य
- 6.1 प्रस्तावना
- 6.2 सिस्टम सुरक्षित क्यों नहीं हैं
- 6.3 साइबर सुरक्षा
 - 6.3.1 साइबर सुरक्षा के सिद्धांत
- 6.4 पहचान की चोरी
- 6.5 प्रमुख सुरक्षा सिद्धांत
 - 6.5.1 पहचान
 - 6.5.2 प्रमाणीकरण
 - 6.5.3 प्राधिकरण
- 6.6 छह आवश्यक सुरक्षा कार्य
- 6.7 सूचना सुरक्षा नीति के सिद्धांतों को लागू करना
- 6.8 सुरक्षा स्व-मूल्यांकन
- 6.9 डिजिटल डिजिटेशन
 - 6.9.1 व्यवसाय में डिजिटल डिजिटेशन का प्रभाव
- 6.10 कैप्चा कोड (CAPTCHA CODE)
 - 6.10.1 कैप्चा का उद्देश्य
 - 6.10.2 कैप्चा का प्रकार
- 6.11 वन टाइम पासवर्ड (OTP)
 - 6.11.1 वन टाइम पासवर्ड कैसे प्राप्त करें
 - 6.11.2 वन-टाइम का पासवर्ड कैसे काम करता है
 - 6.11.3 वन टाइम पासवर्ड के लाभ
- 6.12 सारांश
- 6.13 शब्दावली
- 6.14 बोध प्रश्नों के उत्तर
- 6.15 स्वपरख प्रश्न

6.0 ਉਦ્ਦੇਸ਼

इस इकाई का अध्ययन करने के बाद आप इस योग्य हो सकेंगे कि

- साइबर सुरक्षा के अर्थ और महत्व को समझ सकें;
- पहचान, प्रमाणीकरण और प्राधिकरण के बीच अंतर को समझ सकें;
- डिजिटल हस्ताक्षर और डिजिटलीकरण को समझ सकें; और
- कैप्चा कोड और वन टाइम पासवर्ड (OTP) को समझ सकें।

6.1 प्रस्तावना

पिछली इकाई में हमने अनधिकृत उपयोगकर्ताओं जैसे हैकर्स से व्यापारिक संगठनों को सुरक्षित करने के बारे में कुछ सीखा है। इस इकाई में हम व्यापारिक संगठनों की संपत्ति को सुरक्षित रखने के लिए उठाए गए कदमों के बारे में चर्चा करेंगे। आपने आयामों के कारण छोटे व्यवसाय संगठन के लिए साइबर सुरक्षा की जांच करना सर्वोच्च प्राथमिकता नहीं होती है लेकिन यह पहलू उनके विकास व अस्तित्व के लिए महत्वपूर्ण है। सुरक्षा की जांच करने वाला छोटा व्यवसाय संगठन अपने आयामों के कारण सर्वोच्च प्राथमिकता नहीं है, लेकिन यह पहलू उनके विकास और अस्तित्व के लिए महत्वपूर्ण है। डिजिटल युग के वर्तमान परिदृश्य में, संगठन अपने ग्राहकों को बेहतर सेवा देने के लिए ऑनलाइन माइग्रेट कर रहे हैं और उनकी उपलब्धता को इंटरनेट का उपयोग करके बढ़ाया जाता है। ऑनलाइन माइग्रेट करने के कारण व्यापारिक संगठन साइबर खतरों की एक विस्तृत श्रृंखला के प्रति संवेदनशील है। संगठनों को लगातार निशाना बनाया जा रहा है और साथ ही सुरक्षा उल्लंघन भी हो रहे हैं, लेकिन वे इसे अपने व्यवसाय के लिए छिपा रहे हैं।

हैकर्स लगातार व्यापारिक संगठनों को हैक करना चाहते हैं और कई बार वे अपने प्रयासों में सफल होते हैं। अच्छी साइबर सुरक्षा प्रणाली व्यापारिक संगठनों और उनके हितों को इन हैकरों के खतरों से बचा सकती है। साइबर सुरक्षा किसी भी संगठन के लिए सबसे महत्वपूर्ण सुरक्षा है, इस कारण से इसे गंभीरता से लिया जाना चाहिए। साइबर सुरक्षा को अपनाकर न केवल संगठन सुरक्षित है बल्कि उनके कर्मचारी भी सुरक्षित है। सभी व्यावसायिक संगठन अपनी संपत्ति सुरक्षित करना चाहते हैं और इसलिए एक संगठन में साइबर सुरक्षा की भूमिका अत्यंत महत्वपूर्ण है। अगर किसी हमले से पहले एक व्यावसायिक संगठन के पास एक प्रभावी सुरक्षा योजना है, तो केवल वह अपनी संपत्ति को हैकर्स से बचा सकता है।

6.2 सिस्टम सुरक्षित क्यों नहीं हैं

सिस्टम सुरक्षा को दो श्रेणियों में वर्गीकृत किया जा सकता है। पहले एक भौतिक मशीन सुरक्षा है जिसका उपयोग कंप्यूटर हार्डवेयर की चोरी को रोकने के लिए किया जाता है। आजकल व्यावसायिक डेटा में उपलब्ध सूचना प्रणाली में चोरी या क्षति को रोकने के लिए यह बहुत अधिक महत्वपूर्ण है। इसके अलावा, आज के कॉर्पोरेट वर्ल्ड में डेटा पैसा है, इसका मूल्य लागत के मामले में हार्डवेयर के मूल्य से अधिक है। हम किसी भी व्यावसायिक संगठन के डेटा का उपयोग केवल रिमोट एक्सेस तकनीक और नेटवर्किंग उपकरणों का उपयोग करके कर सकते हैं, और इस प्रकार आज की डिजिटल दुनिया में भौतिक सुरक्षा का कोई मतलब और अर्थ नहीं है। हम केवल कंप्यूटर सिस्टम के भौतिक घटकों को भौतिक सुरक्षा द्वारा सुरक्षित कर सकते हैं। सिस्टम को सुरक्षित करने के लिए हमें हर प्रणाली पर नीति को परिभाषित करना होगा कि किसी विशेष प्रणाली पर क्या कार्य किए जा सकते हैं और किस समय। इस प्रकार हमें सामान्य श्रेणी और व्यवस्थापक उपयोगकर्ता जैसे उपयोगकर्ता श्रेणी और

ऐसे प्रत्येक श्रेणी उपयोगकर्ता के अधिकारों को पहले से परिभाषित करना होगा। यह विशिष्ट नीति से परे और समय बीतने पर प्रौद्योगिकी में प्रगति के लिए सुरक्षित नहीं हो सकता है।

हालांकि हाल के वर्षों में कंप्यूटर सुरक्षा की स्थिति में महत्वपूर्ण प्रगति हुई है, लेकिन ऑनलाइन धोखाधड़ी के कारण कंप्यूटर में जानकारी पहले से कहीं अधिक कमजोर है। कंप्यूटिंग सिस्टम में हर प्रमुख तकनीकी प्रगति नए सुरक्षा खतरों को लाती है और उन्हें हल करने के लिए हमें नए सुरक्षा समाधानों की आवश्यकता होती है। इसके अलावा, प्रौद्योगिकी उस दर से तेजी से आगे बढ़ती है जिस पर उस खतरे के ऐसे समाधान विकसित किए जा सकते हैं। समय बीतने के साथ ही हैकर्स जो विशेषज्ञता हासिल कर लेते हैं, उसकी वजह से हैकर्स से निपटने में बहुत सावधानी बरतनी पड़ती है। इसलिए, यदि हम किसी व्यवसाय संगठन के सिस्टम से समझौता करते हैं, तो हम एक हारी लड़ाई लड़ेंगे। सिस्टम सुरक्षा टीम वर्क है और इसे अकेले हासिल नहीं किया जा सकता है। व्यापार संगठन में एक अच्छी तरह से परिभाषित सुरक्षा वास्तुकला के तार्किक टुकड़े का पालन करके हम बाहरी खतरों और हैकर्स से हमारे सिस्टम की रक्षा कर सकते हैं।

हमारे पास दुनिया के काम करने के तरीके पर नियंत्रण नहीं है, और यह हमारी कल्पना और दायरे से परे भी है, लेकिन सिर्फ यह समझने से कि यह काम क्यों करता है और जिस तरह से यह काम करता है, हम विशेष नुकसान से बच सकते हैं और किसी भी संगठन के लिए स्वीकार्य सुरक्षा चुन सकते हैं। इकाई में कुछ बुनियादी और मूलभूत कारण हैं कि क्यों कंप्यूटर सुरक्षा का कार्यान्वयन किसी भी व्यावसायिक संगठन के लिए आसान काम नहीं है।

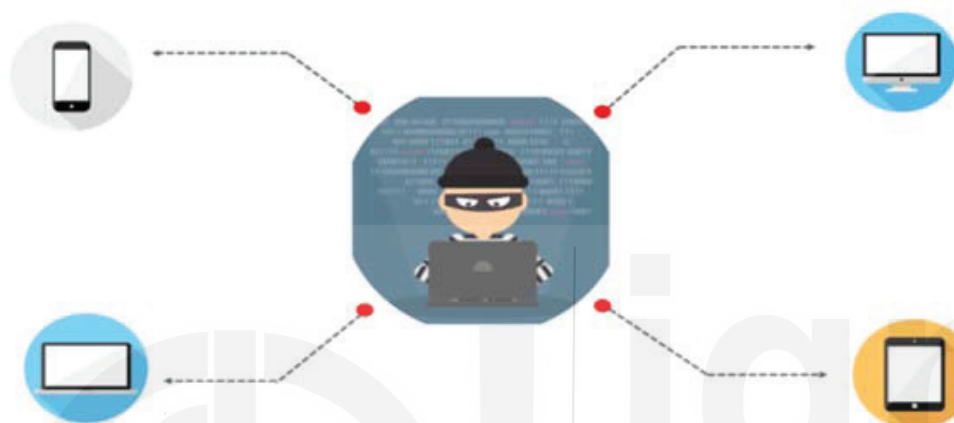
6.3 साइबर सुरक्षा

वर्तमान परिदृश्य में, साइबर अपराध किसी देश की समस्या नहीं है, बल्कि यह एक वैश्विक समस्या है। साइबर क्राइम की सीमाएँ अदृश्य हैं और दुनिया भर में फैली हुई हैं। साइबर अपराध की खबरें हाल के दिनों में सुर्खियां बन रही हैं। साइबर अपराध व्यक्तिगत सुरक्षा और बड़ी अंतरराष्ट्रीय कंपनियों, बैंकों, सरकारी संगठनों और व्यावसायिक संगठनों के लिए एक बड़ा खतरा है। साइबर अपराध एक प्रकार का संगठित अपराध है जो बड़े संगठित और कुशल साइबर अपराधियों द्वारा ऑनलाइन किया जाता है। साइबर अपराधी अक्सर उच्च प्रशिक्षित डेवलपर्स को नियुक्त करते हैं और ये डेवलपर्स अपने ऑनलाइन हमलों को लगातार सुधार करते रहते हैं। सभी व्यावसायिक संगठनों के लिए साइबर सुरक्षा अब आवश्यक हो गई है, क्योंकि कोई भी व्यावसायिक संगठन वर्तमान डिजिटल दुनिया में ऑनलाइन हमलों को बर्दाश्त नहीं कर सकता है। हम निम्नलिखित शब्दों में साइबर सुरक्षा को परिभाषित कर सकते हैं:

साइबर सुरक्षा कंप्यूटर नेटवर्क, कार्यक्रमों, और व्यावसायिक संगठनों के डेटा को हमले, क्षति या अनधिकृत पहुंच से बचाने के लिए उपयोग की जाने वाली तकनीकों का एक पूर्व-निर्धारित सेट है। व्यावसायिक डेटा की सुरक्षा में दो महत्वपूर्ण घटक होते हैं, और ये हैं साइबर सुरक्षा और भौतिक सुरक्षा। उद्यमों को भौतिक सुरक्षा के साथ-साथ साइबर खतरे से अनधिकृत पहुंच के खिलाफ अपने गोपनीय डेटा की रक्षा

करना है। सूचना सुरक्षा शब्द, हर समय और सभी साधनों की गोपनीयता, अखंडता और डेटा की उपलब्धता को बनाए रखने के लिए डिजाइन किया गया है। साइबर सुरक्षा का उपयोग साइबर हमलों, डेटा उल्लंघनों और पहचान की चोरी को रोकने में मदद कर सकता है और जोखिम प्रबंधन में सहायता कर सकता है।

साइबर सुरक्षा में सिस्टम को अनाधिकृत उपयोग, अनाधिकृत बरबादी और हैकर्स से गैर-अधिकृत संशोधन से सुरक्षा प्रदान करना शामिल है। साइबर सुरक्षा एक प्रोटोकॉल प्रदान करती है जो सभी साइबर हमलों से बचाता है और यह सुनिश्चित करता है कि व्यावसायिक डेटा हैकर्स से सुरक्षित है।



चित्र: 6.1 : हैकर्स के द्वारा उत्पन्न किए गये साइबर खतरे

वर्तमान पीढ़ी स्मार्ट फोन का उपयोग करती है और हर समय इंटरनेट से जुड़ी रहती है, और इस बात का कोई अंदाजा नहीं है कि असुरक्षित मीडिया से उनके कंप्यूटरों तक जानकारी कैसे पहुंचती है। यह हैकर्स को देश की युवा पीढ़ियों से डेटा हैक करने का सुनहरा अवसर प्रदान करता है। हैकर्स द्वारा शोषण करने के लिए बहुत सारे एक्सेस पॉइंट, सार्वजनिक आई.पी. और निरंतर ट्रैफिक और टन डेटा हैं। इसके अलावा, साइबर हमले दिन पर दिन विकसित हो रहे हैं। हैकर्स अपने प्रशिक्षकों से प्रशिक्षण प्राप्त करने की कला के साथ अब और अधिक रचनात्मक हो रहे हैं। बड़ी कंपनियों के सिक््योरिटी एडमिनिस्ट्रेटर के लिए हैकरों को हराना और उनके डेटा को माल वेयर और वायरस से बचाना बहुत कठिन काम होता है, और जो कि संगठन के फायरवॉल को बायपास करने के लिए हैकर्स द्वारा इस्तेमाल किए जाने वाले उपकरण (टूल) होते हैं।

6.3.1 साइबर सुरक्षा के सिद्धांत

साइबर सुरक्षा को लागू करने में, दो विशिष्ट लक्ष्यों को प्राप्त करना है: पहला, संभावित साइबर हमलावरों और अन्य अनधिकृत व्यक्तियों की पहुंच से बाहर गोपनीय जानकारी को रखा जाना चाहिए। दूसरा, साइबर सुरक्षा उपायों को अधिकृत उपयोगकर्ताओं की जानकारी तक पहुँच में बाधा नहीं होनी चाहिए। साइबर सुरक्षा के तीन मुख्य सिद्धांत इस प्रकार हैं:

- 1) **गोपनीयता** : साइबर सुरक्षा यह सुनिश्चित करना चाहिए कि सुरक्षित की जाने वाली जानकारी केवल अधिकृत उपयोगकर्ताओं के लिए ही सुलभ हो और

अनधिकृत पार्टियों को जानकारी के प्रकटीकरण को रोकती है। उदाहरण के लिए, क्लाउड-आधारित ग्राहक संबंध प्रबंधन CRM प्रणाली पर कंपनी की जानकारी की गोपनीयता को लागू करने के लिए, सही उपयोगकर्ता नाम-पासवर्ड संयोजन के साथ उपयोगकर्ताओं तक पहुंच को प्रतिबंधित किया जा सकता है। अधिकांश सिस्टम डेटा एन्क्रिप्शन के माध्यम से गोपनीयता को भी लागू करते हैं, जो सुरक्षा की एक अतिरिक्त परत है। डेटा की डिक्రిप्शन को अपेक्षित कुंजी का उपयोग करके प्रयास करने के लिए एक व्यक्ति या प्रणाली की आवश्यकता होती है।

- 2) **प्रमाणिकता** : साइबर सुरक्षा प्रयासों से यह सुनिश्चित होना चाहिए कि जानकारी सटीक, सुसंगत और अनधिकृत संशोधन के अधीन न हो। उदाहरण के लिए, उपलब्ध कराए गए सी.आर.एम.(CRM) उदाहरण से, प्रमाणिकता निधि और ग्राहक के बीच ईमेल संचार एक घुसपैठिए द्वारा अवरोधित और संशोधित नहीं किया जाता है जब यह अभी भी पारगमन में है।
- 3) **उपलब्धता** : साइबरस्पेस में सूचना को सुरक्षित करने का प्रयास एक अधिकृत पार्टी द्वारा इसकी पहुंच में बाधा नहीं बनना चाहिए। इसके अतिरिक्त, साइबर सुरक्षा कार्यान्वयन को किसी भी आउटेज के मामले में अतिरिक्त तक पहुंच प्रदान करना है। उदाहरण के लिए, क्लाउड-आधारित सी.आर.एम.(CRM) सिस्टम का उपयोग करने वाली कंपनी डिनायल ऑफ सार्विस (डी ओ एस) हमलों के खिलाफ सुरक्षा उपाय के रूप में प्रॉक्सी सर्वर और फायरवॉल को लागू कर सकती है, जो सफल होने पर सिस्टम की अनुपलब्धता पैदा करेगा।

6.4 पहचान की चोरी (Identify Theft)

पहचान की चोरी शब्द का अर्थ है साइबर अपराधी अवैध रूप से निर्दोष उपयोगकर्ताओं की जानकारी (क्रेडेंशियल) प्राप्त करते हैं और अपनी वास्तविक पहचान छिपाकर और अन्य निर्दोष उपयोगकर्ताओं की पहचान का उपयोग करके ऑनलाइन साइबर अपराध करने के लिए इन क्रेडेंशियल का उपयोग करते हैं। यह एक अपराध करने के इरादे से व्यक्ति की गई सहमति के बिना किसी अन्य व्यक्ति की पहचान को गैरकानूनी और भ्रामक रूप से आपराधिक कृत्य है; (असुरक्षित वेबसाइटों के उपयोग के माध्यम से व्यक्तिगत जानकारी की धोखाधड़ी और अवैध प्राप्ति) इलेक्ट्रॉनिक अधिग्रहण के अवैध साधनों पर चुराए गए दस्तावेज के उपयोग के माध्यम से – व्यक्ति इंटरनेट का उपयोग करके धोखाधड़ी की खरीदारी और अवैध आर्थिक लाभ में संलग्न होने के लिए दूसरों की पहचान को धोखा दे सकते हैं। दूसरे शब्दों में, पहचान की चोरी को पहचान धोखाधड़ी के रूप में भी जाना जाता है। किसी व्यक्ति की सहमति के बिना किसी अन्य व्यक्ति के बारे में अवैध रूप से जानकारी प्राप्त करने का कार्य है। हैकर्स उपयोगकर्ताओं के बारे में ध्यानपूर्वक जैसे पूर्ण नाम, युवती का नाम, पता, जन्मतिथि, यू.आई.डी., पासवर्ड, फोन नंबर, ई-मेल, और क्रेडिट कार्ड नंबर और सी.वी.वी.(cvv) नंबर आदि उपयोगकर्ताओं को नुकसान पहुंचाने के लिए जानने की कोशिश करते हैं।



चित्र: 6.2 हैकर्स से यूजर क्रेडेंशियल की सुरक्षा करना

हैकर्स तब इस जानकारी का उपयोग उपयोगकर्ताओं के अन्य विवरणों जैसे उनके बैंक खातों, ई-मेल, सेल फोन आदि तक पहुंच प्राप्त करने के लिए करते हैं, इस तरह के कृत्य करना, दूसरों के बारे में अवैध रूप से जानकारी प्राप्त करना आई.टी. अधिनियम 2008 के तहत एक अपराध है। आई.टी अधिनियम के तहत न्यायपालिका द्वारा सख्त सजा का भागी होता है और ऐसे व्यक्तियों को दोषी पाए जाने पर पूरे जीवन के लिए कारावास में भेजा जा सकता है।

पहचान की चोरी रोकने के तरीके:

- i) इंटरनेट पर किसी भी व्यक्तिगत जानकारी को दर्ज करने के समय, कृपया सुनिश्चित करें वह कनेक्शन एन्क्रिप्टेड है।
- ii) यदि आप इंटरनेट पर ऑनलाइन खरीदारी करते हैं तो किसी भी वेबसाइट पर क्रेडिट कार्ड या व्यक्तिगत जानकारी संग्रहीत करने से बचें।
- iii) क्या आपके पास सक्रिय और अपटूडेट स्पायवेयर सुरक्षा सॉफ्टवेयर और एंटीवायरस सॉफ्टवेयर हैं।
- iv) नकली ई-मेल और फिशिंग ई-मेल के बारे में खुद को जागरूक करें जो कंपनी होने का दावा करते हैं
- v) कभी भी अज्ञात और असुरक्षित सिस्टम और स्मार्ट फोन का उपयोग न करें।
- vi) हमेशा मजबूत पासवर्ड रखें और गुप्त प्रश्न का उत्तर अनपेक्षित रखें।

बोध प्रश्न क

भाग क: बहुविकल्प प्रश्न

- 1) प्रॉक्सी सर्वर की क्या आवश्यकता है?
 - i) इसका उपयोग लक्ष्य के साथ मजबूत संबंध बनाने के लिए किया जाता है।
 - ii) इसका उपयोग नेटवर्क पर एक घोस्ट सर्वर बनाने के लिए किया जाता है।
 - iii) इसका उपयोग रिमोट एक्सेस कनेक्शन प्राप्त करने के लिए किया जाता है।
 - iv) इसका उपयोग नेटवर्क पर दुर्भावनापूर्ण गतिविधि को छिपाने के लिए किया जाता है।
- 2) एक हमले के खिलाफ पर्यावरण को सुरक्षित करने में निम्नलिखित में से किसकी आवश्यकता नहीं है?

- i) हमलावर का शिक्षा स्तर
 - ii) प्रणाली का विन्यास
 - iii) नेटवर्क का आर्किटेक्चर
 - iv) कंपनियों की व्यापारिक रणनीति
 - v) कर्मचारियों को वेबसाइट तक पहुंच का स्तर
- 3) किसी तस्वीर के अंदर जानकारी छिपाने के लिए किस तकनीक का उपयोग किया जाता है,
- i) रूटकिट्स
 - ii) बिटमैपिंग
 - iii) स्टेग्नोग्राफी
 - iv) छवि प्रसंस्करण
- 4) सर्विस अटैक का खंडन क्यों किया जाता है?
- i) टी.सी.पी. / आई.पी. स्टैक में कमजोरी का फायदा उठाने के लिए
 - ii) एक सिस्टम पर ट्रोजन को निष्पादित करने के लिए
 - iii) केवल एक विशेष प्रणाली को ओवरलोड करने के लिए ताकि यह अब चालू न हो
 - iv) सेवा बंद करके उन्हें बंद कर दिया

भाग ख : लघुत्तरात्मक प्रश्न

- 1) साइबर सुरक्षा से आपका क्या अभिप्राय है?

.....

.....

.....

.....

- 2) सिस्टम को सुरक्षित नहीं करने के कारण बताएं।

.....

.....

.....

.....

- 3) पहचान की चोरी से आपका क्या मतलब है? उदाहरण सहित स्पष्ट कीजिए।

.....

.....

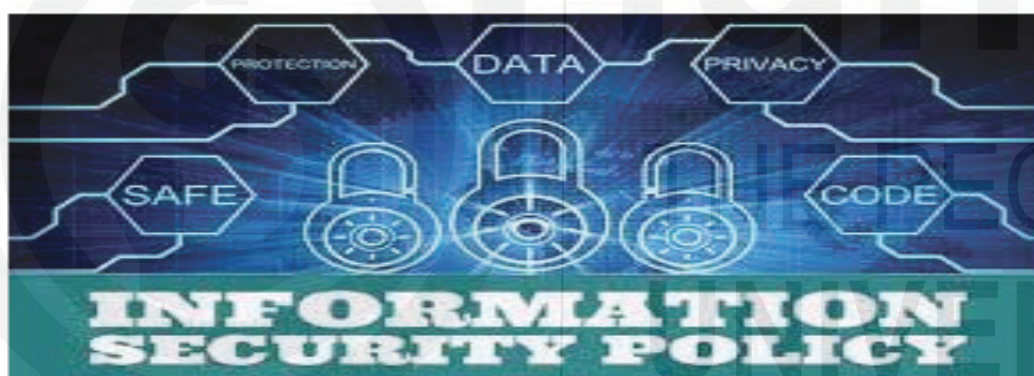
.....

.....

6.5 प्रमुख सुरक्षा सिद्धांत

आई.टी. सुरक्षा को तीन विरोधाभासी अनुरोधों का सम्मान करना होगा गोपनीयता की सुरक्षा, अखंडता और सूचना की उपलब्धता। मुख्य आई.टी. सुरक्षा सिद्धांत पहचान, प्रमाणीकरण और प्राधिकरण हैं। सुरक्षा नीतियों को परिभाषित करना और सुरक्षा तत्वों को डिजाइन करना खुले और गतिशील व्यापार प्रणालियों के लिए मुख्य समर्थन के रूप में सूचना प्रणालियों के लिए एक सुरक्षित वातावरण का नेतृत्व करता है। उपयोगकर्ता की पहचान एक प्रक्रिया है जिसके दौरान एक संभावित उपयोगकर्ता उसे लॉग इन करते समय सूचना प्रणाली की पहचान करता है। आम तौर पर, यह एक प्रक्रिया है जिसके दौरान एक इकाई खुद का परिचय देती है और किसी अन्य इकाई की पहचान करती है।

प्रमाणीकरण, प्रामाणिकता की जाँच प्रक्रिया है, अर्थात् यह आधार में संग्रहीत लोगों के साथ इकाई से प्राप्त डेटा की तुलना करके उपयोगकर्ता की पहचान की जाँच करता है। यह उल्लेख किया जाना चाहिए कि इकाई अखंडता आवश्यक नहीं है। उदाहरण के लिए, आई.एस.पी पर लॉग इन करते समय एक ही उपयोगकर्ता नाम और पासवर्ड के तहत एक ही टेलीफोन लाइन और एक ही कंप्यूटर से अधिक लोगों को जोड़ना संभव है।



चित्र: 6.3 सूचना सुरक्षा नीति के चरणों को प्रदर्शित करना

प्राधिकरण प्रणाली एक उपयोगकर्ता अभिगम अधिकार परिभाषा की प्रक्रिया है और सबसे अधिक बार यह प्रमाणीकरण का एक हिस्सा है। हम इस खंड में आई.टी. सुरक्षा के इन तीन सिद्धांतों के विवरण पर चर्चा करेंगे।

6.5.1 पहचान

कंप्यूटर विज्ञान में पहचान शब्द का उपयोग नेटवर्क पर व्यक्तिगत उपयोगकर्ताओं की भूमिकाओं और विशेषाधिकार तक पहुंच को परिभाषित करने और प्रबंधित करने के लिए किया जाता है। यह उन परिस्थितियों से भी निपटता है जिसमें उपयोगकर्ता उन विशेषाधिकारों को प्रदान (या अस्वीकृत) करते हैं। उपयोगकर्ता कंपनी के ग्राहक या कर्मचारी हो सकते हैं। पहचान का उपयोग प्रति व्यक्ति को डिजिटल पहचान देने के लिए किया जाता है, और एक बार डिजिटल पहचान स्थापित हो जाने के बाद, इसे

प्रत्येक उपयोगकर्ता के “एक्सेस जीवनचक्र” के दौरान अपडेट, रखरखाव और निगरानी करनी चाहिए।

दूसरे शब्दों में: कंप्यूटर विज्ञान में पहचान उपयोगकर्ताओं की पहचान, प्रमाणीकरण और अधिकृत करने के लिए एक संगठनात्मक प्रक्रिया है, जो प्रत्येक उपयोगकर्ता के विशिष्ट अधिकारों और प्रतिबंधों को स्थापित पहचानों के साथ जोड़कर अनुप्रयोगों, प्रणालियों या नेटवर्क तक पहुंच प्राप्त करने के लिए अधिकृत करती है। पहचान को सॉफ्टवेयर प्रक्रियाओं के रूप में भी जाना जाता है। जिन्हें संगठनात्मक प्रणालियों तक पहुंच की आवश्यकता होती है। पहचान का उपयोग एक मात्र के उपयोगकर्ता के साथ सिस्टम में चल रहें अनुप्रयोग के पहचान के लिए भी किया जाता है। अधिकांश सूचना प्रणालियों में एक उपयोगकर्ता नाम और पासवर्ड का उपयोग वैध उपयोगकर्ता की पहचान की जाँच के लिए किया जाता है। जो भी उपयोगकर्ता सही नाम और पासवर्ड दर्ज करता है, वह सूचना प्रणाली के लिए एक वैध उपयोगकर्ता है। इसलिए, सिस्टम की सुरक्षा के लिए हमें उपयोगकर्ता नाम और पासवर्ड को हमेशा गुप्त रखना चाहिए; अन्यथा सिस्टम में संग्रहीत जानकारी सुरक्षित नहीं होगी। जब तक उपयोगकर्ता नाम और पासवर्ड का संयोजन गुप्त है डेटाबेस में संग्रहीत जानकारी सुरक्षित है।

6.5.2 प्रमाणीकरण

प्रमाणीकरण प्रणाली संसाधनों का उपयोग करने से पहले उपयोगकर्ताओं की क्रेडेंशियल्स की जांच करने की प्रक्रिया है। यह साबित करने की क्षमता है कि उपयोगकर्ता या एप्लिकेशन वास्तविक है और इस आधार पर यह संगठन या नेटवर्क के संसाधनों का उपयोग कर सकता है। प्रमाणीकरण पहचान उपयोगकर्ता की पहचान के आधार पर की जाती है। प्राधिकरण प्रक्रिया में उपयोगकर्ता नाम, एक प्रक्रिया आईडी, एक स्मार्ट कार्ड, या कुछ और जो प्रमाणीकरण के समय उस वस्तु की विशिष्ट पहचान कर सकता है, को शामिल करता है। यदि कोई उपयोगकर्ता किसी सर्वर पर उपलब्ध सूचना प्रणाली को एक्सेस करना चाहता है तो उसे अपनी पहचान दिखानी होगी। प्रमाणीकरण में, उपयोगकर्ता को संसाधनों का उपयोग करने की अनुमति देने से पहले सर्वर या क्लाइंट को अपनी पहचान साबित करनी होगी।

जब कोई उपयोगकर्ता अपनी पहचान साबित करने के लिए उचित क्रेडेंशियल्स प्रदान करता है, तो केवल संसाधनों का उपयोग करने की अनुमति दी जाती है और इस प्रक्रिया को प्राधिकरण के रूप में जाना जाता है। उदाहरण के लिए, जब कोई उपयोगकर्ता सही उपयोगकर्ता नाम और सही पासवर्ड दर्ज करता है, तो यह साबित होता है कि उपयोगकर्ता नाम का वैध स्वामी (lawful owner) है संक्षेप में, प्रमाणीकरण दावा की गई पहचान का प्रमाण और संसाधनों तक पहुंचने की अनुमति देता है। सर्वर यह जानने के लिए प्रमाणीकरण प्रक्रिया का उपयोग करता है कि उनकी जानकारी या साइट पर कौन पहुँच रहा है। प्रमाणीकरण का उपयोग क्लाइंट द्वारा सर्वर के साथ संबंध स्थापित करने के लिए किया जाता है। प्रमाणीकरण की कई परिभाषाएँ हैं; उनमें से कुछ नीचे दिए गए हैं:

- i) सर्वर अपने उपयोगकर्ता नाम और पासवर्ड द्वारा एक उपयोगकर्ता की पहचान करता है। एक प्रणाली में प्रमाणित करने के अन्य तरीके कार्ड, रेटिना स्कैन, आवाज पहचान और उंगलियों के निशान के माध्यम से होते हैं।

- ii) तीसरे विश्वसनीय पार्टी जैसे वैरीसाइन का उपयोग प्रत्येक उपयोगकर्ता प्रमाणपत्र की वैधता की जांच करने के लिए किया जाता है, इससे पहले कि उपयोगकर्ता द्वारा लॉगिन करने की अनुमति दी जाये।
- iii) बैंक वेबसाइटों में, प्रमाणीकरण के लिए पासवर्ड और कैप्चा का उपयोग किया जाता है।
- iv) प्रमाणीकरण केवल पहचानता है और पुष्टि करता है कि व्यक्ति या प्रणाली कौन है।
- v) बैंक के एटीएम के पासवर्ड या पिन का उपयोग प्रमाणीकरण उद्देश्य के लिए किया जाता है।
- vi) संगठन में स्मार्ट कार्ड और बायोमेट्रिक क्रेडेंशियल का उपयोग कर्मचारियों द्वारा अपनी पहचान साबित करने के लिए किया जाता है।

6.5.3 प्राधिकरण

नाम प्राधिकरण सॉफ्टवेयर कंपनियों द्वारा अपनाई जाने वाली कार्यप्रणाली है, जो वैध उपयोगकर्ताओं को फाइल, सेवाओं, कंप्यूटर प्रोग्राम, डेटा और एप्लिकेशन प्रोग्राम सहित सिस्टम संसाधनों की अनुमति देती है। यह उपयोगकर्ता की पहचान के आधार पर एक नेटवर्क संसाधन तक पहुंचने से इनकार करने की प्रक्रिया है। प्राधिकरण को निम्नलिखित शब्दों में भी परिभाषित किया जा सकता है:

- i) यह एक प्रक्रिया है जिसके द्वारा एक सर्वर निर्धारित करता है कि क्लाइंट के पास नेटवर्क पर उपलब्ध संसाधन का उपयोग करने की अनुमति है या नहीं।
- ii) प्राधिकरण सर्वर द्वारा प्रमाणीकरण के बाद होता है और यह निर्धारित करता है कि ग्राहक कौन है और वह नेटवर्क पर क्या अनुरोध कर रहा है।
- iii) कई प्रकार के प्राधिकरण हैं और उनमें से प्रत्येक के लिए दूसरे से आवश्यकता भिन्न हो सकती है; दूसरों से।
- iv) कुछ मामलों में कोई प्राधिकरण नहीं है और कुछ प्राधिकरणों में यह आवश्यक है।

कुछ वेब सुरक्षा प्रणालियाँ दो-चरणीय प्राधिकरण प्रक्रिया पर आधारित होती हैं, जिसमें पहला चरण प्रमाणीकरण प्रक्रिया है, और दूसरा चरण प्राधिकरण प्रक्रिया है। वर्तमान ऑपरेटिंग सिस्टम संसाधनों के अनुप्रयोग परिनियोजन और प्रबंधन को सुविधाजनक बनाने के लिए प्रभावी रूप से डिजाइन किए गए प्राधिकरण प्रक्रियाओं पर काम करते हैं। मुख्य कारक जिन पर आधुनिक ऑपरेटिंग सिस्टम काम करते हैं: सिस्टम को लॉगिन करने के लिए उपयोगकर्ताओं की संख्या और उनकी साख। जिस समय किसी उपयोगकर्ता की पहचान की जाती है और उसे प्रमाणित किया जाता है, उसे उसके प्रोफाइल के आधार पर प्राधिकरण प्रदान किया जा सकता है।

दूसरे शब्दों में, यदि सभी उपयोगकर्ता एक ही खाते का उपयोग करके लॉग ऑन करते हैं, तो उन्हें संसाधनों तक पहुंचने की अनुमति होगी। ऐसी स्थितियों में सिस्टम के उपयोगकर्ताओं के बीच अंतर करना बहुत मुश्किल है। इसके अलावा, यदि उपयोगकर्ताओं को विभिन्न उपयोगकर्ता खातों द्वारा प्रमाणित किया गया है, तो उन्हें

अपनी पहचान और प्रोफाइल के आधार पर विभिन्न संसाधनों तक पहुंच प्रदान की जा सकती है।

बोध प्रश्न ख

भाग (क): बहुविकल्प प्रश्न

- 1) प्रमाणीकरण का उद्देश्य है
 - क) उपयोगकर्ता कौन से संचालन / डेटा को प्रतिबंधित कर सकता है
 - ख) निर्धारित करें कि क्या उपयोगकर्ता हमलावर है
 - ग) उपयोगकर्ता को चिन्हित करें यदि वह गलत व्यवहार करता है
 - घ) निर्धारित करें कि उपयोगकर्ता कौन है
 - ड) इनमें से कोई भी नहीं
- 2) साइबर हमला है
 - क) डॉस अटैक
 - ख) फिशिंग अटैक
 - ग) मालवेयर भेजना
 - घ) उपर्युक्त सभी
- 3) प्रमाणीकरण विधि है
 - क) गुप्त प्रश्न
 - ख) बायोमैट्रिक
 - ग) पासवर्ड
 - घ) एसएमएस कोड
 - ड) ऊपर के सभी
- 4) भूमिका-आधारित अभिगम नियंत्रण में, प्रत्येक उपयोगकर्ता को एक या एक से अधिक भूमिकाएँ सौंपी जाती हैं, और भूमिकाएँ निर्धारित करती हैं कि उपयोगकर्ता को किस सिस्टम तक पहुँचने की अनुमति है।
 - क) सत्य
 - ख) असत्य

भाग ख : लघुत्तरात्मक प्रश्न

- 1) व्यावसायिक संगठन के लिए आई.टी. सुरक्षा के प्रमुख सुरक्षा सिद्धांत क्या हैं? उदाहरण सहित स्पष्ट कीजिए।

.....

.....

.....

.....

.....

2) ऑनलाइन बैंकिंग प्रणाली में उपयोगकर्ता की पहचान की आवश्यकता बताएं

.....

.....

.....

.....

.....

3) प्रमाणीकरण से आपका क्या मतलब है? उदाहरण सहित स्पष्ट कीजिए।

.....

.....

.....

.....

.....

4) प्रमाणीकरण और प्राधिकरण के बीच क्या अंतर है? उदाहरण सहित स्पष्ट कीजिए।

.....

.....

.....

.....

.....

6.6 छह आवश्यक सुरक्षा कार्य

सभी व्यावसायिक संगठनों को अपने आई.टी. सुरक्षा को अनाधिकृत उपयोगकर्ताओं से सुरक्षित रखना होगा और उन्हें अवैध उपयोगकर्ताओं से बचाने के लिए कदम उठाने होंगे। साइबर हमलों की संख्या दिन-प्रतिदिन बढ़ रही है और सभी आकारों के व्यवसायों को प्रभावित कर रही है। ऐसी स्थितियों में, यह आवश्यक है कि प्रत्येक कंपनी साइबर अपराधियों द्वारा उत्पन्न खतरों से अवगत हो और ऐसे अपराधियों से अपने डेटा को सुरक्षित रखने के लिए तैयार हो और उनके पास उचित सुरक्षा तंत्र हो। बाजार में प्रणालियों को सुरक्षित करने के लिए कई दृष्टिकोण हैं और स्थापना लागत और उपयोग का समय भी उनके चयन में शामिल है।

लेकिन जो सबसे अच्छा सुरक्षा उपकरण है और जो किसी संगठन में उपयोग किया जा सकता है वह विभिन्न मापदंडों पर निर्भर करता है। अगर किसी सुरक्षा उपकरण के पैरामीटर किसी भी संगठन के लिए सबसे उपयुक्त हैं, तो उसे खरीदना और स्थापित करना होगा। इसके अलावा, संगठनों के प्रमुख और सुरक्षा कंपनी के प्रमुख उस सॉफ्टवेयर को अंतिम रूप देने के लिए चर्चा और बातचीत कर सकते हैं जो किसी भी कंपनी के लिए सबसे अच्छा है। हमें यह भी ध्यान रखना होगा कि जो सॉफ्टवेयर सबसे उन्नत है और जो दीर्घकालिक सुरक्षा प्रदान करता है, उसे लघु सुरक्षा समय पर प्राथमिकता दी जा सकती है।

लगभग सभी छोटे व्यवसाय संगठन लेनदेन करने के लिए वेब-आधारित प्रौद्योगिकी उपकरणों का उपयोग करते हैं। उदाहरण के लिए, लंबी दूरी के सम्मेलन आयोजित करना, विज्ञापन देना, विपणन उत्पाद, अनुसंधान करना, नए बाजारों की पहचान करना और ग्राहकों और आपूर्तिकर्ताओं के साथ संवाद करना, छोटे व्यवसाय संगठनों के सुचारु कामकाज का अभिन्न अंग बन गए हैं।



चित्र: 6.4 व्यापार संगठन में चोरी से हार्डवेयर को सुरक्षित करना

अब हम सिस्टम की भौतिक चोरी से बचाने के लिए कैमरा स्थापित कर सकते हैं। तकनीकी सहायता और अत्याधुनिक सुरक्षा कैमरों की प्रगति ने भौतिक चोरी को नगण्य बना दिया है। वर्तमान डिजिटल युग में आभासी दुनिया से बराबरी करना आसान नहीं है और बाहरी दुनिया से डेटा की रक्षा के लिए तकनीकी कौशल की आवश्यकता है। आधुनिक संगठन इंटरनेट और नवीनतम नेटवर्किंग उपकरणों द्वारा दुनिया भर में जुड़े हुए हैं, जो एक वरदान है और संचार को आसान बनाता है, लेकिन एक ही समय में ऑनलाइन चोरी की चपेट में है। इंटरनेट के कई लाभों के साथ, डिजिटल युग में कई जोखिम शामिल हैं और यह हर दिन बढ़ रहा है। छोटे व्यवसायों के संगठनों में कई खामियां हैं, क्योंकि वे साइबर हमलावरों से ग्रस्त हैं। संगठन को साइबर हमलों से बचाने के लिए छः उपायों को अपनाना आवश्यक है।

- 1) **फायरवॉल (Firewall) :** फायरवॉल एक प्रकार की वर्चुअल प्रोटेक्शन वॉल है जो नेटवर्क ट्रैफिकबाउंड और आउटबाउंड को कहीं भी असंगठित होने से बचाने में मदद करती है। यह अनधिकृत हैकर्स को संगठनों के सिस्टम से अवरुद्ध करके नेटवर्क पर हमला करने से रोकता है। फायरवॉल को इस तरह से प्रोग्राम किया जाता है कि वे नेटवर्क को मालिकाना डेटा और गोपनीय ईमेल भेजने से रोकते हैं। वर्तमान युग के हैकर्स कला हैकिंग प्रौद्योगिकियों की स्थिति के साथ अधिक परिष्कृत हो गए हैं इस कारण संगठन के नेटवर्क से उन्हें रोकने के लिए फायरवॉल अप्रचलित हो गए हैं।

संगठनों की फायरवॉल किसी भी संगठन के सुरक्षा उपकरण का सबसे मुख्य हिस्सा है, और आने वाले समय के लिए भी जारी रहेगा। फायरवॉल व्यापारिक संगठनों की सुरक्षा के लिए उपयोगी होते हैं, लेकिन उनकी सीमाएँ भी होती हैं। प्रशिक्षित और कुशल हैकर्स ने यह सीखा है कि फायरवॉल को धोखा देने वाले

डेटा और प्रोग्राम कैसे बनाए जाते हैं, जो यह मानते हैं कि वे विश्वसनीय हैं। इससे उन्हें बिना किसी परेशानी का सामना किए फायरवॉल से गुजरना पड़ता है। उपरोक्त सीमाओं के बावजूद, व्यावसायिक संगठनों के डेटा पर अनधिकृत और कम परिष्कृत दुर्भावनापूर्ण हमलों का पता लगाने में फायरवॉल अभी भी बहुत प्रभावी हैं।

- 2) **एंटीवायरस सॉफ्टवेयर:** एंटीवायरस प्रोग्राम का उपयोग व्यावसायिक संगठनों के सिस्टम और नेटवर्क से वायरस को हटाने के लिए किया जाता है। यह बुनियादी सॉफ्टवेयर है जो किसी भी साइबर सुरक्षा प्रणाली का हिस्सा होना चाहिए। इसके अलावा अब एंटी-मालवेयर सॉफ्टवेयर का उपयोग भी आवश्यक है। एंटीवायरस व्यावसायिक संगठनों के नेटवर्क को घुसपैठ करने से अवांछित हमलों को सुरक्षित करने और बचाव करने में अंतिम सीमा के रूप में काम करता है। एंटीवायरस वायरस और मालवेयर, एडवेयर और स्पाइवेयर को नेटवर्क से डिटेक्ट और रिमूव करके काम करता है। यह सभी संगठनों के सिस्टम के संभावित हानिकारक डाउनलोड और ईमेल को स्कैन और फिल्टर भी करता है। इनस्टॉल एंटीवायरस और एंटी-स्पाइवेयर सॉफ्टवेयर – किसी संगठन द्वारा उपयोग किए जाने वाले किसी भी कंप्यूटर या नेटवर्क को एक अच्छे फायरवॉल के साथ सुरक्षित किया जाना चाहिए जो वाई-फाई को ध्यान में रखता है। एंटी-स्पाइवेयर और एंटीवायरस सॉफ्टवेयर के नवीनतम संस्करण इंस्टॉल किए जाने चाहिए। विक्रेता सॉफ्टवेयर के लिए सुरक्षा पैच और अपडेट प्रदान करते हैं, इसलिए नियमित रूप से नवीनतम संस्करण में अपडेट करना सुनिश्चित करें। स्वचालित रूप से अपडेट स्थापित करने के लिए सभी सॉफ्टवेयर को कॉन्फिगर करें।
- 3) **जटिल पासवर्ड का उपयोग करें:** नेटवर्क पर व्यवसाय संगठन के संसाधनों तक पहुंचने के लिए उपयोगकर्ता का आई.डी और पासवर्ड आवश्यक है। हमारे पास हमेशा मजबूत पासवर्ड होना चाहिए और इसे हैकर्स से गोपनीय रखना चाहिए। पासवर्ड को समय-समय पर बदला जाना चाहिए। जटिल पासवर्ड उपयोगकर्ताओं के लिए क्रैक करना (खोलना) मुश्किल है और इस प्रकार डेटा को सुरक्षित बनाता है। हमें गोपनीय और जटिल सवालों के जवाब का चयन करना चाहिए ताकि वे आसानी से क्रैक न हो सकें। हमें सोशल मीडिया साइट्स पर मजबूत पासवर्ड रखना चाहिए ताकि इन साइटों पर हमारा डेटा सुरक्षित रहे और इसकी सुरक्षा से कोई समझौता न हो। हमें पासवर्ड को हैकिंग सिस्टम से हैक करने से पहले या उसके बाद स्पेस बटन का उपयोग करना चाहिए। स्पेस बटन रखने से अज्ञात व्यक्तियों द्वारा अनुमान लगाना मुश्किल हो जाता है। यदि कोई आपके पासवर्ड तक पहुंच जाता है, लेकिन इस बात से अनजान है कि पासवर्ड में स्पेस है तो वह आपके डेटा तक नहीं पहुंच सकता है। हमें ऊपरी और निचले वर्णों और विशेष वर्णों के संयोजन का उपयोग करना चाहिए ताकि उपयोगकर्ताओं को अनुमान लगाने या तोड़ने के लिए इसे जटिल बनाया जा सके। पासवर्ड को मजबूत बनाने के लिए अक्षराकीय वर्णों (Alphanumeric) और प्रतीकों के संयोजन का भी उपयोग किया जा सकता है।

- 4) **नियमित बैकअप:** डेटा को नियमित रूप से सहेजने और बैकअप लेने की प्रक्रिया संगठनों को डेटा हानि के जोखिमों से बचाती है। डेटा हानि के मामले में बैकअप बहुत उपयोगी है और इसका उपयोग व्यावसायिक संगठन में डेटा को पुनर्स्थापित करने के लिए किया जा सकता है। हैकिंग तकनीक में प्रगति के साथ अब कोई भी नेटवर्क सुरक्षित और सही नहीं है। वर्तमान समय में बैंकों से डेटा हैकिंग और मनी हैकिंग उन अखबारों में सुर्खियां बनते हैं जिनमें हैकर्स बैंक नेटवर्क की सुरक्षा को दरकिनार कर अवैध तरीके से पैसे चुराने की कोशिश करते हैं। हार्डवेयर विफलता के मामले में व्यवसाय को सुचारु रूप से चलाने के लिए बैकअप डेटा बहुत महत्वपूर्ण है और नियमित रूप से बैकअप के साथ व्यावसायिक हित सुरक्षित हो सकते हैं।

जोखिम को कम करने के लिए, डेटा का नियमित बैकअप बहुत आवश्यक है। हमें आधुनिक व्यावसायिक संगठन के सर्वर में स्वचालित बैकअप विकल्प सेट करना चाहिए। यदि बैकअप नियमित रूप से लिया जाता है तो यह प्रबंधन को दिमागी शांति प्रदान करता है और बाजार में व्यवसाय के हितों की रक्षा करने में मदद करता है। वर्तमान डिजिटल युग में हमारे महत्वपूर्ण दस्तावेजों की कई भौतिक प्रतियां होनी चाहिए ताकि भौतिक या सॉफ्टवेयर विफलताओं से डेटा के नुकसान के मामले में हम इसे वापस पा सकें, जब हमारे सिस्टम के मामले में हैकर्स द्वारा समझौता किया जाता है।

- 5) **भेदन परीक्षण और महत्वपूर्ण डेटा तक सीमित पहुंच:** इसका उपयोग सॉफ्टवेयर का परीक्षण करने में किया जा सकता है ताकि उसमें दोष पाए जा सकें। सॉफ्टवेयर इंजीनियरिंग में कई प्रकार के परीक्षण होते हैं और पैनिट्रेशन परीक्षण उनमें से एक है। व्यावसायिक डेटा की नेटवर्क सुरक्षा का परीक्षण करने के लिए सुरक्षा पेशेवरों को कॉल करके व्यावसायिक संगठनों की सुरक्षा का परीक्षण करने के लिए प्रवेश/भेदन (penetration) परीक्षण का उपयोग किया जाता है। सुरक्षा पेशेवर उसी तकनीक का उपयोग करें जो हैकर सिस्टम में संभावित कमजोरी और भेद्यता को खोजने के लिए उपयोग करते हैं। हमें सुरक्षा पेशेवरों की सलाह का पालन करना चाहिए और सर्वरों की सुरक्षा को और बढ़ाने के लिए उनके सुझावों के अनुसार अधिक सुरक्षा उपकरण जोड़ना चाहिए।

व्यावसायिक संगठनों में डेटा की सुरक्षा को सुरक्षित करने और बढ़ाने के लिए भेदन परीक्षण एक तरीका है। इसके अतिरिक्त हमें अपने कर्मचारियों से महत्वपूर्ण व्यावसायिक डेटा की पहुंच पर प्रतिबंध लगाना चाहिए। महत्वपूर्ण डेटा को केवल अधिकृत उपयोगकर्ताओं द्वारा और प्रमाणीकरण और प्राधिकरण के माध्यम से प्राप्त किया जाना चाहिए। अनधिकृत और बाहरी लोगों को महत्वपूर्ण डेटा तक पहुंचने की अनुमति नहीं दी जानी चाहिए और इस संबंध में जरूरतमंदों को तंत्र का उपयोग करना चाहिए। हमें महत्वपूर्ण डेटा तक पहुंच रखने वाले लोगों की संख्या कम से कम रखनी चाहिए जैसे कि कंपनी के सीईओ और मुट्ठी भर भरोसेमंद कर्मचारी और केवल एक स्पष्ट योजना होनी चाहिए जिसमें उल्लेख किया गया हो कि किस व्यक्ति के पास किस संवेदनशील जानकारी की जवाबदेही है।

- 6) **कर्मचारी प्रशिक्षण:** महत्वपूर्ण डेटा को संभालने वाले व्यावसायिक संगठनों के सभी कर्मचारियों को डेटा को सुरक्षित करने की जिम्मेदारी दिए जाने से पहले प्रशिक्षित किया जाना चाहिए। कई प्रकार के हमले हैं और फिशिंग उनमें से एक है। व्यापारिक संगठनों को फिशिंग हमलों से बचाने के लिए कर्मचारियों को प्रशिक्षित किया जाना चाहिए कि ऐसे हमलों से सुरक्षित डेटा को कैसे संभालना है।

यदि कर्मचारी को फिशिंग हमलों के लिए पर्याप्त प्रशिक्षित किया जाता है, तो केवल वह महत्वपूर्ण डेटा को नुकसान से बचा सकता है। फिशिंग अटैक मूल जैसी वेबसाइटों को बना रहा है, और ग्राहकों को लक्षित कर रहा है और उनके उपयोगकर्ता आईडी और पासवर्ड को अवैध रूप से चुरा रहा है। एक बार फिशिंग वेबसाइटों पर उपयोगकर्ता जानकारी एकत्र कर लिए जाते हैं और फिर बाद में इन जानकारीयों का उपयोग मूल उपयोगकर्ताओं को अवैध रूप से नुकसान पहुंचाने के लिए पैसे निकालने के लिए किया जा सकता है। इस प्रकार कर्मचारियों का प्रशिक्षण ऑनलाइन हमलों से संगठन को सुरक्षित बनाता है और इस प्रकार डेटा को अनधिकृत पहुंच से सुरक्षित किया जाता है।

कर्मचारी जो सुरक्षा उपकरण संभाल रहा है, उसे संगठन को सुरक्षित करने की जिम्मेदारी देने से पहले उसे ठीक से संभालने के लिए प्रशिक्षित किया जाना चाहिए। ऑनलाइन खतरों से संगठन को सुरक्षित करने के लिए पहला कदम खतरे को पहचानना है। दूसरा कदम खतरे को ट्रैक करना है। तीसरा कदम है, खतरे को हल करने के लिए उपकरण और एंटीवायरस को दृढ़ना। नेटवर्क का उपयोग करने वाले कर्मचारियों या उपयोगकर्ताओं को उन जोखिमों और सावधानियों के बारे में प्रशिक्षित किया जाना चाहिए जिनके बारे में उन्होंने व्यावसायिक संगठन में साइबर हमले के मामले में आवेदन किया है ताकि जोखिम कम से कम हो। इसके अलावा, ऑनलाइन उपयोग, उपयोग नीति, उपयोग अधिकार और उपयोग प्रोफाइल के मामले में कर्मचारियों के व्यवहार को जानने और अवैध हाथों से व्यापार डेटा की सुरक्षा के लिए निगरानी की जानी चाहिए।

6.7 सूचना सुरक्षा नीति के सिद्धांतों को लागू करना

सभी संगठनों के लिए सूचना सुरक्षा को साइबर सुरक्षा विशेषज्ञों के सुझावों और सिफारिशों के अनुसार इसकी सुरक्षा के स्तर को ध्यान में रखते हुए तैयार किया जाना चाहिए। महत्वपूर्ण सूचना सुरक्षा प्रथाओं को लागू किया जाना चाहिए और किसी भी कीमत पर सुरक्षा टीम द्वारा अनदेखी नहीं की जानी चाहिए। जैसा कि हम जानते हैं कि रोकथाम इलाज से बेहतर है और अगर हमारे पास सभी सुरक्षा उपाय हैं तो हम व्यापार डेटा को गलत हाथों से सुरक्षित करते हैं। व्यवसायों को अपने संगठनों के अंदर सूचना सुरक्षा के लिए सख्त नीतियों का पालन करना चाहिए।

यह देखा गया है कि निवारक कदम केवल व्यापार डेटा के अंदर साइबर हमलों के बाद उठाए जाते हैं। हमें हमलों के होने की प्रतीक्षा नहीं करनी चाहिए बल्कि बाजार में आने वाली व्यावसायिक इकाई के पहले दिन से डेटा को सुरक्षित करने के लिए कदम उठाने चाहिए। किसी भी व्यावसायिक संगठन के व्यावसायिक डेटा की सुरक्षा

के लिए कई कदम हैं। साइबर हमलों के अलावा स्व-प्रसार संबंधी कुकृत्य हैं जो व्यापारिक संगठनों के लिए जोखिम हैं। सभी व्यवसाय संगठन चाहते हैं कि उनकी ऑनलाइन उपस्थिति उनके व्यवसाय को बढ़ावा दे इस कारण से उनकी सुरक्षा प्रबंधन के लिए प्रमुख कारक और अधिक महत्वपूर्ण हो जाती है।

उपरोक्त के मद्देनजर, व्यवसाय को अपनी सुरक्षा नीतियों को मजबूत करने की आवश्यकता है, इससे पहले कि उनके लिए कार्य करने में बहुत देर हो जाए। इस खंड में हम कुछ चरणों का उल्लेख करेंगे, जिन्हें वर्तमान डिजिटल युग में व्यावसायिक डेटा को सुरक्षित करने के लिए अपनाया जाना चाहिए। ये हैं:



चित्र 6.5 : व्यवसाय में आईटी सुरक्षा नीति लागू करना

- 1) **एक्सेस कंट्रोल पॉलिसी (Access Control Policy):** मैनेजमेंट शब्द बाहरी लोगों के महत्वपूर्ण डेटा को सुरक्षित करने में बहुत महत्वपूर्ण भूमिका निभाता है। प्रत्येक व्यवसाय संगठन को डेटा की सुरक्षा के लिए एक्सेस कंट्रोल नीतियों को सख्ती से लागू करना चाहिए। अब सोशल वेबसाइट्स व्यावसायिक संगठनों के लिए खतरा बन गई हैं। सोशल वेबसाइट और इंटरनेट खुद में डेटा के लिए बहुत सारे छिपे हुए खतरे हैं और हमें एक्सेस कंट्रोल पॉलिसी लागू करके इन खतरों से प्रभावी ढंग से निपटना चाहिए।

बेहतर पासवर्ड प्रबंधन तकनीक वर्तमान डिजिटल युग में शामिल ऑनलाइन जोखिमों को कम करने में मदद करती है। सिस्टम व्यवस्थापक को नियमित रूप से ऑनलाइन खतरों की निगरानी करनी चाहिए और व्यापारिक संगठन के सभी उपयोगकर्ताओं को संगठन में उपयोग की जाने वाली सुरक्षा नीति का पालन करने की सलाह देनी चाहिए। सिस्टम व्यवस्थापक को सभी उपयोगकर्ताओं को समय-समय पर कुछ महीनों के बाद अपना पासवर्ड बदलने और सिस्टम को हैकर्स से सुरक्षित बनाने की सलाह देनी चाहिए। केवल अधिकृत उपयोगकर्ताओं को सिस्टम के संसाधनों का उपयोग करने की अनुमति दी जानी चाहिए और सिस्टम तक पहुंचने के लिए अनधिकृत उपयोगकर्ताओं को रोका जाना चाहिए।

- 2) **टू-फैक्टर ऑथेंटिकेशन पॉलिसी: (Two-Factor Authentication Policy) :** वन टाइम पासवर्ड (OTP) तकनीक को टू फैक्टर ऑथेंटिकेशन पॉलिसी के रूप में भी जाना जाता है और इसे खातों के अवैध उपयोग को कम करने के लिए लागू किया जा सकता है। इस तंत्र में एक समय पासवर्ड उपयोगकर्ता के पंजीकृत

मोबाइल नंबर पर भेजा जाता है। फिर उपयोगकर्ता को एसएमएस के माध्यम से प्राप्त किए गए वनटाइम पासवर्ड (OTP) दर्ज करने के लिए कहा जाता है। यदि उपयोगकर्ता सही वन टाइम पासवर्ड दर्ज करता है तो उसका प्रमाणीकरण अधिकृत है और उसे ऑनलाइन संसाधनों का उपयोग करने की अनुमति है।

वन टाइम पासवर्ड तकनीक की कुछ सीमाएँ भी होती हैं और यह टू-फैक्टर ऑथेंटिकेशन नीति के लिए सर्वोत्तम तकनीक नहीं है। वैकल्पिक ईमेल प्रमाणीकरण प्रक्रिया व्यावसायिक संगठनों में उपयोगकर्ताओं के दोहरे प्रमाणीकरण के लिए एक और तरीका है। व्यापार संगठन के महत्वपूर्ण डेटा को सुरक्षित बनाने के लिए हमें दोहरी प्रमाणीकरण नीति का उपयोग करना चाहिए।

- 3) **अपने इंटरैक्शन को एन्क्रिप्ट करें:** एन्क्रिप्शन शब्द का अर्थ है प्लेन टैक्स्ट डेटा को छिपाना और इसे कुछ कोड में बदलना जो बाहरी व्यक्ति के लिए तोड़ना मुश्किल है। असुरक्षित डेटा का उपयोग करके स्रोत कंप्यूटर से गंतव्य कंप्यूटर पर भेजने से पहले इसे बाहरी लोगों के गोपनीय डेटा की सुरक्षा के लिए एन्क्रिप्ट किया गया है। एक बार एन्क्रिप्टेड डेटा गंतव्य कंप्यूटर तक पहुंच जाता है, यह एक बार फिर डिक्लिप्शन तकनीकों का उपयोग करके वास्तविक रूप में परिवर्तित हो जाता है।

असुरक्षित नेटवर्क पर एन्क्रिप्टेड डेटा भेजने का यह तरीका एन्क्रिप्शन और डिक्लिप्शन के रूप में जाना जाता है। एन्क्रिप्शन शब्द का उपयोग प्लेन टैक्स्ट को कोडित रूप में बदलने के लिए किया जाता है, और गंतव्य सर्वर पर कोडित फॉर्म को प्लेन टैक्स्ट में परिवर्तित करने के लिए डिक्लिप्शन का उपयोग किया जाता है। एन्क्रिप्शन और डिक्लिप्शन तकनीकों का उपयोग करके हम हैकर्स के हाथों से महत्वपूर्ण व्यावसायिक डेटा की रक्षा कर सकते हैं।

- 4) **अपनी की (Key) को सुरक्षित रखें:** डेटा को अनचाहे हाथों से बचाने के लिए लॉगिन क्रेडेंशियल्स को गुप्त रखना बहुत महत्वपूर्ण है, और की (Key) का उपयोग जानकारी तक पहुंच प्रदान करता है। इसके अलावा, भौतिक लॉकरों के मामले में हमेशा की का दूसरा सेट होना चाहिए जो पहले सेट खो जाने या चोरी हो जाने की स्थिति में उपयोग किया जा सकता है। इसके अलावा की के नुकसान के मामले में लॉकर खोलने के लिए की के दूसरे सेट का उपयोग किया जाना चाहिए और व्यवसाय संगठन से डेटा या जानकारी के नुकसान से बचने के लिए बाद के समय में बदल सकता है। इस प्रकार की की सुरक्षा करके हम व्यावसायिक संगठनों के डेटा और सूचनाओं को अनधिकृत उपयोगकर्ताओं और हैकर्स से बचा सकते हैं।

- 5) **अपनी जानकारी का बैकअप लें और सुनिश्चित करें कि बैकअप सुरक्षित और संरक्षित है:** शब्द बैकअप का मतलब है कि हार्डवेयर की विफलता या सॉफ्टवेयर विफलता के मामले में डेटा की हानि से बचने के लिए व्यवसायिक डेटा की प्रतियां बनाना और इसे नियमित स्थान पर सुरक्षित रूप से संग्रहीत करना। व्यावसायिक डेटा और जानकारी सुलभ होनी चाहिए और इसे सुरक्षित स्थान पर एन्क्रिप्ट और संग्रहित किया जाना चाहिए। आमतौर पर व्यापारिक अनुबंधों में गोपनीय जानकारी खंड होती है, जिसे किसी भी संगठन को नहीं बताना चाहिए जो अपने लाभ के लिए उस जानकारी का दुरुपयोग कर सकते

हैं। इस तरह के गोपनीय डेटा को हमेशा गोपनीय रखा जाना चाहिए और प्रतिस्पर्धी संगठन को इसका खुलासा नहीं करना चाहिए।

व्यावसायिक संगठन बाजार में अपना व्यवसाय चलाने के उद्देश्य से विभिन्न प्रकार की साझेदारी और एक दूसरे से वस्तुओं के आदान-प्रदान के लिए समझौता ज्ञापन (एमओयू) पर हस्ताक्षर करते हैं। ऐसे एमओयू को हमेशा गोपनीय रखा जाना चाहिए और किसी भी तीसरे पक्ष का खुलासा नहीं किया जाना चाहिए, जिसमें दो व्यावसायिक संगठनों के बीच एमओयू के डेटा और सूचना का दुरुपयोग करने की क्षमता है। निजी और गोपनीय डेटा के किसी भी दुरुपयोग के मामले में और अन्य प्रतिस्पर्धी संगठन द्वारा एक व्यावसायिक संगठन की जानकारी को कानून की अदालत में चुनौती दी जा सकती है और किसी भी व्यवसाय संगठन के नुकसान की भरपाई के लिए अदालतों द्वारा सजा और जुर्माना की मात्रा दी जाती है।

सहयोग संगठनों के बीच भी हस्ताक्षरित समझौता ज्ञापन समझौते के बिना गोपनीयता भंग हो सकती है। भारत में, किसी व्यावसायिक संगठन के कर्मचारियों को अपने सेवा समय के दौरान किसी अन्य पार्टी द्वारा उन्हें बताई गई किसी गुप्त जानकारी को गोपनीय रखने की आवश्यकता होती है। इसके अलावा, यदि कर्मचारी गोपनीयता का उल्लंघन करता है तो उसे न्याय पाने के लिए अदालतों में चुनौती दी जा सकती है। अदालत दोनों पक्षों की दलील सुन सकती है और अदालत में पेश की गई कार्यवाही और सबूत के अनुसार मामले को तय करने के लिए न्याय दे सकती है। सुनवाई के दौरान निम्नलिखित प्रकार के प्रश्न न्यायालय द्वारा पूछे जा सकते हैं:

- i) तथ्यों की गोपनीयता के बारे में जानकारी
- ii) क्या प्रकटीकरण के मामले की परिस्थितियों में कोई लिंक है
- iii) क्या जिस पार्टी को सूचना मिली, उसने इसका दुरुपयोग किया था या नहीं

इसके अलावा, यह उल्लेख किया जाना चाहिए कि यद्यपि कानून गोपनीयता के एक कर्तव्य का उल्लेख करता है – इसका दायरा, प्रकृति, और दायित्व अनिश्चित हैं और न्यायिक निर्धारण के अधीन हैं। अदालतों में बहस के दौरान गोपनीय डेटा के लीकेज (भेद खुलने) की आवृत्ति और इसकी प्रकृति को अत्यंत गोपनीय रूप से निपटाया जाना चाहिए। ऐसे मामलों के कुछ उदाहरण नीचे दिए गए हैं जो डेटा और जानकारी की गोपनीयता को समझते हैं

- i) चोरी (लैपटॉप, कंप्यूटर, कागज, एमओयू आदि – शारीरिक सुरक्षा)
- ii) गोपनीय जानकारी का अनुचित निपटान
- iii) अनधिकृत एक्सेस प्रकार और इसकी प्रकृति (एक्सेस नियंत्रण, प्रमाणीकरण, गोपनीयता समझौते की समझ की कमी, लापरवाही, आदि)।
- iv) गोपनीय डेटा की हानि की मात्रा (लापरवाही, आदि)
- v) हैकिंग घटना लॉग आदि (सबसे अधिक बार इंटरनेट सुरक्षा)
- vi) गोपनीय डेटा के लीकेज (भेद खुलना) का तरीका साइबर सुरक्षा विशेषज्ञों द्वारा मापा जाता है।

6.8 सुरक्षा स्व-मूल्यांकन

संगठनों के भीतर बदलते आई.टी. परिवेश में प्रौद्योगिकी मंच, नए उपकरणों को अपनाना, सदस्यता और समाधान शामिल हैं। यह इस कारण से है कि उद्यमों को लगातार रोजमर्रा की दिनचर्या की वास्तविकता के साथ बने रहना चाहिए जो अंततः व्यवसाय को संचालित करते हैं (या इसे धीमा करते हैं)। एक साल पहले की गई कार्यकुशलता तेजी से कम हो सकती है और आज सीमित हो सकती है। नियमित सुरक्षा जोखिम मूल्यांकन संगठनों को सक्रिय रहने में मदद कर सकते हैं। सही क्लाउड उपकरण और नियंत्रण के साथ, उद्यम वर्तमान परिवर्तनों के अनुकूल हो सकते हैं।

यह सुनिश्चित करना महत्वपूर्ण है कि भौतिक उपकरणों को भौतिक चोरी से व्यवसाय संगठन में अच्छी तरह से सुरक्षित किया जाता है। व्यवसायिक संगठन में भौतिक चोरी को रोकने और मना करने के लिए नीतिगत स्थानों पर कैमरे लगाए जाने चाहिए। हमलावर इंटरनेट-सक्षम उपकरणों और अन-पैच किए गए कारनामों के माध्यम से व्यापारिक संगठनों के सर्वर तक पहुंचने का प्रयास करते हैं। व्यवसायिक संगठन के पूरे नेटवर्क का उपयोग करने के लिए वायरलेस नेटवर्किंग जैसे कि वायरलेस प्रिंटर, वाई-फाई राउटर, हब, यूटीपी केबल और चल डिवाइस का उपयोग हैकर्स द्वारा किया जाता है। कंप्यूटर नेटवर्क की सुरक्षा में खामियों की जांच करने और इसे हल करने के उपायों का सुझाव देने के लिए व्यवसाय संगठनों द्वारा जोखिम मूल्यांकन और साइबर सुरक्षा विशेषज्ञों के विभिन्न स्तरों का उपयोग किया जा सकता है। व्यावसायिक संगठन का सुरक्षा विश्लेषण व्यावसायिक संगठन के विशेषज्ञ नेटवर्क व्यवस्थापक द्वारा भी किया जा सकता है। नेटवर्क को सुरक्षित करने के साधनों और तरीकों का सुझाव देने के लिए ग्राहकों के लिए भेद्यता और जोखिम मूल्यांकन परीक्षण में विशेष साइबर सुरक्षा कंपनियों को सवार किया जा सकता है। साइबर सुरक्षा विशेषज्ञों की सेवाओं में कुछ लागत शामिल है, और यह लागत छोटे व्यापारिक संगठनों के लिए संभव नहीं है।

व्यावसायिक संगठन के कर्मचारियों को जोखिम मूल्यांकन करना चाहिए और इस व्यवसाय उद्योग के आकार और पैमाने के बावजूद भी इसे एक नियमित प्रक्रिया बनाना चाहिए। सुरक्षा उल्लंघन किसी भी व्यावसायिक संगठन, विशेष रूप से छोटे व्यवसायों के लिए हो सकता है, क्योंकि ये तो हैकर्स का मानना है कि वे संयोग से एक बड़ी कंपनी को तोड़ने का आसान लक्ष्य हैं। व्यावसायिक संपत्ति हासिल करने के लिए स्व-मूल्यांकन और निगरानी को अनिवार्य और निरंतर प्रक्रिया बनाया जाना चाहिए। इसके अलावा, एक व्यापक सुरक्षा जोखिम मूल्यांकन को वर्ष में कम से कम एक या दो बार आयोजित किया जाना चाहिए, जो सूचना प्रणाली लेखा परीक्षा और नियंत्रण संघ द्वारा सुझाया गया है।

किसी भी व्यावसायिक संगठन में कमजोरियों को खोजने के लिए स्व मूल्यांकन का तरीका बहुत प्रभावी है। यह आईटी कर्मचारियों की जिम्मेदारी है कि वे नेटवर्क में भेद्यता का पता लगाने के लिए प्रबंधन के साथ स्व-मूल्यांकन योजना पेश करें और प्रबंधन के साथ इसे लागू करें। एक नेटवर्क का निर्माता नेटवर्क संरचना को अच्छी तरह से समझता है और नेटवर्क में भेद्यता का आकलन करने के लिए उसकी सेवाएं ली जा सकती हैं। चूंकि वह नेटवर्क निर्माता है और इसलिए वह दूसरों की तुलना में

जल्दी नेटवर्क में सुरक्षा का आकलन कर सकेगा। व्यवसाय की सुरक्षा के लिए हमें पहले नेटवर्क को सुरक्षित करना चाहिए और समय-समय पर आवश्यक मूल्यांकन करना चाहिए।

इसके अलावा, यदि किसी व्यवसाय संगठन द्वारा ऑनलाइन लेन-देन स्वीकार किया जाता है, तो साइबर सुरक्षा द्वारा प्राप्त सुझावों के अनुसार नेटवर्क को सुरक्षित करने के लिए चरणों की शुरुआत करके नेटवर्क में भेद्यता का आकलन करने और भेद्यता को ठीक करने के लिए साइबर सुरक्षा विशेषज्ञों को बुलाना बहुत आवश्यक है। यदि किसी व्यावसायिक संगठन ने सुरक्षा मूल्यांकन नहीं किया है, तो यह साइबर चोरी का खतरा है और इसे जल्द से जल्द सुरक्षा मूल्यांकन के लिए कदम उठाने चाहिए। आज की डिजिटल दुनिया में व्यावसायिक संगठनों पर साइबर हमले हर रोज बढ़ रहे हैं यह एक वास्तविकता है। पिछले सालों में प्रिंट और इलेक्ट्रॉनिक मीडिया द्वारा कई साइबर हमलों की सूचना दी गई थी जैसे फिशिंग स्कैम, फिरोती आदि। भविष्य में साइबर हमलावरों द्वारा व्यवसाय संगठन के डेटा और जानकारी को चोरी करने के लिए कई साइबर हमले किए जाएंगे। यह दुनिया की सभी इंटरनेट गवर्निंग एजेंसियों का कर्तव्य है कि वे साइबर हमलों की जाँच करने के लिए रणनीति बनाने के लिए एक साथ बैठें और दुनिया भर में हैकरों को दंडित करने के लिए नीतियों का ढाँचा तैयार करें, ताकि व्यापारिक संगठनों को सुरक्षित रखने के लिए दुनिया भर में व्यापार संगठनों के हितों का विरोध किया जा सके।

एक जोखिम मूल्यांकन के बुनियादी चरण

सुरक्षा मूल्यांकन के मूल चरण निम्नानुसार हो सकते हैं:

- 1) **पहचानें:** सिस्टम को व्यवस्थित करें (प्रक्रिया, कार्य या अनुप्रयोग)
- 2) **सुरक्षा:** खतरों को पहचानें
- 3) **पता लगाएँ:** निहित जोखिम और प्रभाव का निर्धारण करें
- 4) **प्रतिक्रिया:** नियंत्रण पर्यावरण का विश्लेषण करें
- 5) **पुनर्प्राप्त:** सिस्टम और सुधार की बहाली

उपयोगकर्ताओं को सशक्त बनाना: ज्यादातर मामलों में, एक संगठन में सबसे बड़ा खतरा उन लोगों के लिए होता है जो संगठन के भीतर काम करते हैं। एक संगठन के भीतर कर्मचारी साइबर सुरक्षा के लिए मुख्य खतरा हैं। जिनके पास ज्ञान नहीं है उनके पास आपके डेटा को उजागर करने के बहुत अवसर दूसरे वे विक्रेता जिनके पास आपके सिस्टम का एक्सेस है। फिशिंग ईमेल को पहचानने और फिशिंग ईमेल के उपयोगकर्ता प्रबंधन और प्रमाणीकरण के उचित प्रबंधन के लिए, उपयोगकर्ता आपकी सुरक्षा बना सकते हैं या तोड़ सकते हैं। कर्मचारियों को शिक्षित रखना हमलों को रोकने और उन्हें सही ढंग से जवाब देने के लिए महत्वपूर्ण है।

एक जोखिम मूल्यांकन बनाना: आज की डिजिटल दुनिया में 85% व्यापारिक संपत्ति डिजिटल रूप में है। इसलिए, यह महत्वपूर्ण है कि संगठन बहुत देर से पहले सावधानी बरतें। किसी भी व्यावसायिक संगठन के जोखिम मूल्यांकन का आकलन आवेदन कार्यक्रम, कार्यात्मक भाग या उस संगठन द्वारा अपनाई जाने वाली प्रक्रियाओं सहित साइबर विशेषज्ञों द्वारा किया जाना चाहिए। सबसे पहले हमें सुरक्षा आकलन के लिए व्यापार संगठन के आकार, दायरे और जटिलता को समझना होगा। एक बार जब

यह अनुमान लगाया जाता है तो सुरक्षा मूल्यांकन के लिए आवश्यक समय, लागत और श्रमशक्ति का भी अनुमान लगाया जाना चाहिए। जोखिम आकलन प्रक्रिया में हमें व्यावसायिक संगठन की आंतरिक और बाहरी प्रणालियों की पहचान करनी होगी जो संगठन को चलाने के लिए महत्वपूर्ण हैं। इस प्रक्रिया में हमें संवेदनशील व्यावसायिक डेटा का संचालन, प्रक्रिया, कानूनी एमओयू, क्रेडिट कार्ड की जानकारी और कई और अधिक का बैकअप लेना होगा, इससे पहले कि हम सुरक्षा मूल्यांकन शुरू करें।

जोखिम मूल्यांकन महत्वपूर्णता और सूचना की संवेदनशीलता के आधार पर किया जा सकता है। मूल्यांकन के परिणाम हमें यह पता लगाते हैं कि व्यावसायिक डेटा को कैसे सुरक्षित किया जाए, कितने समय की जरूरत है और किस कार्यप्रणाली का पालन किया जाना है और दिए गए समय अवधि में डेटा को सुरक्षित करने के लिए कितनी मैनपावर की आवश्यकता है। ये सभी हमें लापता टुकड़े को पहचानने में मदद करते हैं।

व्यापार डेटा हाल के वर्षों में कई व्यावसायिक उपकरण और एप्लीकेशन को सॉफ्टवेयर डेवलपर्स ने नए बिजनेस संगठन की नेटवर्क सुरक्षा का आकलन करने के लिए विकसित किया है। कुछ उपकरण खुले स्रोत हैं और आप उन्हें इंटरनेट से सीधे डाउनलोड कर सकते हैं। कुछ उपकरण का भुगतान किया जाता है और आप उन्हें केवल मामूली शुल्क देकर ऑनलाइन डाउनलोड कर सकते हैं और अपने व्यावसायिक संगठन को सुरक्षित करने के लिए उनका उपयोग कर सकते हैं। माइक्रोसॉफ्ट विंडोज-10 सुरक्षा मूल्यांकन उपकरण से लैस है और इसका उपयोग व्यावसायिक संगठन के डेटा की सुरक्षा के लिए किया जा सकता है।

बोध प्रश्न ग

भाग क: बहुविकल्प प्रश्न

1) नेटवर्क लेयर फायरवॉल निम्नलिखित के अनुसार काम करता है

- क) परेम फिल्टर
- ख) पैकेट फिल्टर
- ग) दोनों परेम के साथ ही पैकेट फिल्टर
- घ) उल्लेखित कोई नहीं

2) फायरवॉल क्या है

- क) एक हार्डवेयर
- ख) एक सॉफ्टवेयर
- ग) एक हार्डवेयर और साथ ही सॉफ्टवेयर
- घ) न तो हार्डवेयर और न ही सॉफ्टवेयर

3) डी. पी. आई. (DPI) का पूर्ण रूप है

- क) डॉट्स प्रोसेसिंग इंच
- ख) डॉट्स पर इंच
- ग) डाइग्राम पर इंच
- घ) डाइग्राम प्रौद्योगिक इंच

भाग ख: लघुतरात्मक प्रश्न

1) उदाहरण के साथ कार्रवाई के लिए छह सुरक्षा अनिवार्य बताएं।

.....

.....

.....

.....

.....

2) उदाहरण के साथ आई.टी. सुरक्षा के सिद्धांतों की व्याख्या करें।

.....

.....

.....

.....

.....

3) सुरक्षा स्व-मूल्यांकन से आपका क्या मतलब है ? इसे कैसे लागू किया जाता है?

.....

.....

.....

.....

.....

4) उपयोगकर्ताओं को सशक्त बनाने से आपका क्या तात्पर्य है? उदाहरण सहित स्पष्ट कीजिए।

.....

.....

.....

.....

.....

6.9 डिजिटल डिजिटेशन

डिजिटल डिजिटेशन शब्द का उपयोग कागज आधारित डेटा और सूचना को बचत के इलेक्ट्रॉनिक तरीके में बदलने के लिए किया जाता है, ताकि इसे कंप्यूटर सिस्टम का उपयोग करके पुनर्प्राप्त, संसाधित और अद्यतन किया जा सके। कंप्यूटर पठनीय प्रारूप में डिजिटल प्रौद्योगिकियों के एकीकरण को डिजिटल डिजिटेशन के रूप में जाना जाता है। कंप्यूटर प्रणाली और मोबाइल फोन जैसे इलेक्ट्रॉनिक उपकरणों का उपयोग करके रोजमर्रा की नियमित चीजों को डिजिटल बनाया जा सकता है। सूचनाओं को

डिजिटल स्वरूप में परिवर्तित करने की एक प्रक्रिया है। डिजिटल प्रारूप में सूचना और डेटा को डेटा की एक अलग में जैसे कि हार्ड डिस्क में संयोजित और संसोदित किया जा सकता है। जिन्हें अलग से पहचाना और संबोधित किया जा सकता है। डिजिटलीकरण में डेटा को बाइनरी नंबर के रूप में हार्ड डिस्क संग्रहीत किया जाता है, जिसे कंप्यूटर सिस्टम का उपयोग करके संसाधित किया जा सकता है।

टैक्सट ऑडियो, चित्र और वीडियो डेटा स्कैनर, कैमरा और एप्लिकेशन का उपयोग करके डिजिटल किए जा सकते हैं। स्कैनर का उपयोग इमेज को स्कैन करने और उन्हें jpg या बिटमैप छवियों के रूप में सहेजने के लिए किया जाता है, जिसे भविष्य में उपयोग के लिए कंप्यूटर मेमोरी में संग्रहीत किया जा सकता है। ऑप्टिकल कैरेक्टर रिकग्निशन (OCR) तकनीक का उपयोग चैक पर लिखे अंकों और डेटा का विश्लेषण और पहचान करने और हर कैरेक्टर को ए.एस.सी.आई.आई. (American Standard Code for Information Interchange [ASCII]) कोड में परिवर्तित करना में होता है।

कंप्यूटर प्रणाली का उपयोग करके ऑडियो और वीडियो डिजिटलीकरण का उपयोग एनालॉग-टू-डिजिटल और विपरीतता में परिवर्तित किया जाता है। इस प्रक्रिया में एनालॉग सिग्नल को डिजिटल सिग्नल में परिवर्तित किया जाता है और उनकी गुणवत्ता को उपकरण और एप्लिकेशन का उपयोग करके बढ़ाया जाता है, बिना चित्र डेटा की वास्तविक बुनियादी सामग्री से समझौता किए। इस प्रक्रिया में एनालॉग सिग्नल की शक्ति भी बढ़ जाती है और कंप्यूटर सॉफ्टवेयर का उपयोग करके इसके वियोजन को बढ़ाया जा सकता है। इस प्रकार डिजिटलीकरण प्रक्रिया लंबे समय तक और ज्ञान समाज के लिए भविष्य के संदर्भ उद्देश्य के लिए कागजी प्रारूप को बनाए रखने में बहुत मददगार है। उदाहरण के लिए सभी कोर्ट पेपर पर आधारित निर्णयों को अब भारत में डिजिटल किया जा रहा है और कंप्यूटर में बाइनरी फॉर्मेट में संग्रहित किया जा रहा है, जिसे न्यायालयों में न्यायाधीश द्वारा किसी अन्य मामले में आसानी से संदर्भित किया जा सकता है।

डिजिटल जानकारी इंटरनेट और कंप्यूटर नेटवर्क का उपयोग करके इसे संरक्षित, प्राप्त करना और साझा करना आसान बनाती है। उदाहरण के लिए, एक मूल ऐतिहासिक दस्तावेज केवल उन लोगों के लिए सुलभ हो सकता है जो इसके भौतिक स्थान पर जाते हैं, लेकिन यदि दस्तावेज को डिजिटल कर दिया जाता है, तो इसे पूरे देश के लोगों और यहां तक कि पूरी दुनिया के लिए भी उपलब्ध कराया जा सकता है। आज के डिजिटल दुनिया में हमारे देश में ऐतिहासिक और सांस्कृतिक रूप से डेटा के डिजिटलीकरण की ओर रुझान बढ़ रहा है।

6.9.1 व्यवसाय में डिजिटাইजेशन का प्रभाव

वर्तमान डिजिटल युग में व्यापार की दुनिया में डिजिटাইजेशन बहुत महत्वपूर्ण है। इसे व्यवसाय संगठन में निरंतर परिवर्तन और विकास की आवश्यकता है। हार्डवेयर और सॉफ्टवेयर प्रौद्योगिकी में प्रगति के साथ, डिजिटাইजेशन अब दशकों पहले की तुलना में बहुत आसान काम है। डिजिटাইजेशन ने जीवन को सरल बना दिया डिजिटल डिजिटल की मदद से डिजिटल डेटा नवीनतम इंटरनेट प्रौद्योगिकी के साथ

उपयोक्ता के लिए 24 × 7 उपलब्ध है। वर्तमान डिजिटल युग में डिजिटাইजेशन तेजी से व्यापार की दुनिया को बदल रहा है और सभी व्यावसायिक घरानों को अपने ग्राहकों तक पहुंचने के लिए वर्तमान डिजिटल युग में जीवित रहने के लिए डिजिटाइजेशन को अपनाना होगा।

- 1) **आर्टिफिशियल इंटेलिजेंस (ए.आई.):** आर्टिफिशियल इंटेलिजेंस ऐसी आर्टिफिशियल इंटेलिजेंट मशीन को डिजाइन और विकसित करता है, जो मनुष्य की तरह काम करती है। ए.आई. ने पहले से ही व्यापार की दुनिया को इस हद तक बदल दिया है, कि सभी व्यापारिक संगठन अपने उत्पादों में ए.आई. का उपयोग कर रहे हैं। उदाहरण के लिए, एसी, रेफ्रिजरेटर और सभी घरेलू उपकरण, इंटरनेट ऑफ थिंग्स (IOT) आधारित नहीं हैं और ये बेहतर उपयोग के लिए संचार कर सकते हैं और इनके उपयोग को अनुकूलित किया जा सकता है। अब ए.आई. (AI) का उपयोग भारत सहित पूरी दुनिया में डेटा विश्लेषण करने, एल्गोरिदम बनाने, और यहां तक कि ग्राहक और कंपनी के संचार को बेहतर बनाने के लिए किया जा रहा है।
- 2) **लचीले कार्य :** डिजिटাইजेशन ने आई.टी. कर्मचारियों को कार्यालय के बजाय घर से काम करने का विकल्प दिया है, इस प्रकार यात्रा समय, लागत और कार्यालय व्यय के संदर्भ में बचत होती है। आजकल सभी डेटा और सूचना डिजिटल मीडिया पर संग्रहीत है और इसे घर बैठे ही एक्सेस किया जा सकता है। कई आईटी कंपनियां अब अपने कर्मचारियों को कंपनी की लागत कम करने और उत्पादकता बढ़ाने के लिए घरेलू नौकरियों की पेशकश कर रही हैं। आज के डिजिटल युग में तकनीकी प्रगति और डिजिटাইजेशन ने हमारी व्यक्तिगत जरूरतों और जीवन शैली के अनुसार कार्य अनुसूची को समायोजित करना संभव बना दिया है। लचीलेपन और बेहतर उत्पादकता के कारण अधिक से अधिक आईटी कंपनियां इंटरनेट और अत्याधुनिक नेटवर्क तकनीकों का उपयोग करके उनके लिए काम करने के लिए फ्रीलांसरों और दूरदराज के श्रमिकों पर भरोसा कर रही हैं।
- 3) **नवपरिवर्तन:** डिजिटাইजेशन अब कंप्यूटर सिस्टम में संग्रहित किए जाने वाले कागज डेटा को बाइनरी रूप में परिवर्तित करने के लिए उपयोग किया जा रहा है। ये डिजिटल कंटेंट अब पूरे भारत और विश्व के बाकी हिस्सों में विश्वविद्यालयों और कॉलेजों के कई अनुसंधान विद्वानों द्वारा अनुसंधान करने के लिए व्यापक रूप से उपयोग किए जा रहे हैं। डिजिटাইजेशन ने शोधकर्ताओं के लिए डिजिटल डेटा 24 × 7 की उपलब्धता बना दी है, जिसके कारण कई शोधकर्ता बाजार में नए और नए उत्पादों का विकास कर रहे हैं। डिजिटাইजेशन के कई नए, नए समाधान बाजार में आ गए हैं और इस तरह ये हर तरह के लोगों के जीवन को सरल बना रहे हैं यह व्यापार दुनिया के लगभग किसी भी पहलू पर लागू किया जा सकता है, जिसमें यातायात प्रबंधन, कार्यबल प्रबंधन, उत्पादन प्रबंधन और कई और अधिक शामिल हैं। प्रौद्योगिकी के परिवर्तन ने व्यापार जगत में नए विचारों को उत्पन्न किया है ताकि वे अपने उत्पाद को ऑनलाइन बेचने के लिए एक व्यापक इंटरनेट प्रेमी ग्राहक तक पहुंच सकें,

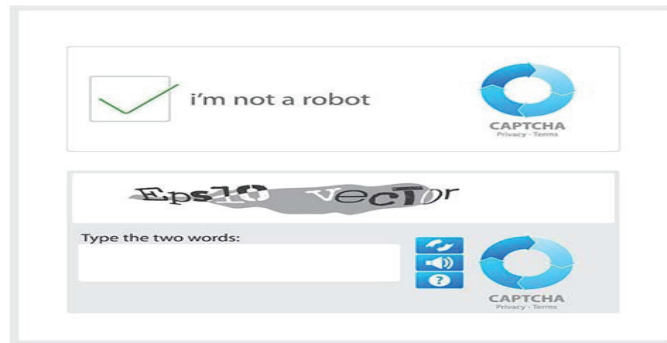
जिससे ग्राहक खुश, संतुष्ट और उत्पाद इंटरनेट और नेटवर्क के माध्यम से ग्राहक को 24 × 7 उपलब्ध हो सकें।

- 4) **नया व्यवसाय मॉडल:** आज की डिजिटल दुनिया में डिजिटাইजेशन ने ग्राहकों को डील और ऑफर करने के लिए कई नए बिजनेस मॉडल बनाना संभव बना दिया है। हम भौतिक रूप से दुकानों पर जाने और यात्रा की लागत और समय का भुगतान करने के बजाय उत्पादों को ऑनलाइन खरीद सकते हैं। आज के डिजिटल युग में जानकारी और उपकरण ऑनलाइन उपलब्ध हैं, और व्यावसायिक संगठन अपने ग्राहकों के लिए अपने व्यवसाय मॉडल स्वतंत्र रूप से और आसानी से बना और प्रचारित कर सकते हैं। कंपनियां अपने उत्पादों को बेचने और विपणन करने के लिए ग्राहकों तक पहुंचने के लिए नए विचार लागू कर सकती हैं और दिन-प्रतिदिन अपने व्यवसाय को समृद्ध बना रही हैं।
- 5) **संचार:** व्यावसायिक संगठनों को अपनी व्यावसायिक प्रक्रिया में अपने समकक्षों पार्ट्स और ग्राहकों के साथ संवाद करना होगा। इंटरनेट और सोशल मीडिया जैसे कि फेसबुक, व्हाट्सएप, इंस्टाग्राम ने आज के डिजिटल युग में संचार को बहुत सरल बना दिया है। इसके अलावा, संचार जीवन के साथ-साथ व्यवसाय में भी बहुत महत्वपूर्ण भूमिका निभाता है। उचित संचार व्यवसाय को सफल और विकसित करता है और ग्राहक को सही उत्पाद प्रस्तुत करता है। सही सूचना हस्तांतरण की कमी से गलतफहमी और उलझनें पैदा होती हैं। यहां कई उपकरण, चैनल और ऐप हैं जिनके माध्यम से एक व्यवसाय दोनों कर्मचारियों और उसके ग्राहकों के साथ संवाद कर सकता है, इंटरनेट ने कंपनी और उसके उपयोगकर्ताओं के बीच सूचना के सुचारु आदान-प्रदान और यहां तक कि फाइलों, दस्तावेजों, डेटा आदि के लिए विभिन्न मंच प्रदान किए हैं। आज के डिजिटल युग में, स्काईप (Skype), स्लैक, ब्लॉग्स, वीडियो, फेसबुक और अन्य “टूल” का उपयोग अपने ग्राहकों और सहयोगी संगठनों के साथ अपने विचारों को संप्रेषित करने और उनका आदान-प्रदान करने के लिए कर सकते हैं।

6.10 कैप्चा कोड (CAPTCHA CODE)

कैप्चा स्पैम के खिलाफ वेबसाइटों की सुरक्षा के लिए इस्तेमाल किया जाने वाला एक तरीका है। लक्ष्य स्वचालित रूप से उत्पन्न इनपुट को फिल्टर करके संवादात्मक वेबसाइटों को स्पैम होने से रोकना है। कैप्चा का पूर्ण रूप ‘कंप्यूटर और मनुष्यों को अलग बताने के लिए पूरी तरह से स्वचालित सार्वजनिक ट्यूरिंग परीक्षण’ है। कैप्चा का आविष्कार लुइस वॉन आह, मैनुअल ब्लम, निकोलस जे हॉपर और जॉन लैंगफोर्ड ने वर्ष 2003 में किया था। वर्ष 1950 की शुरुआत में, कंप्यूटर वैज्ञानिक एलन ट्यूरिंग ने आर्टिफिशियल इंटेलिजेंस के परीक्षण के लिए एक तरीका सुझाया था। कंप्यूटर पायनियर के अनुसार, एक मशीन मानव मन की नकल करने में सक्षम है जब यह एक चैट में लोगों के साथ बातचीत करने का प्रबंधन करता है, तब यह एहसास होता है कि यह एक कंप्यूटर है। स्पैम को रोकने के लिए आई.टी. कंपनियां उपयोगकर्ताओं के रूप में उपयोगकर्ताओं और कंप्यूटरों के बीच अंतर करने के लिए कैप्चा कोड का उपयोग करती हैं। कैप्चा का उपयोग सुरक्षित वेबसाइटों द्वारा लॉगिन प्रक्रिया में किया

जाता है। कैप्चा पत्र यह जांचने का एक तरीका है कि क्या वेबसाइट में पंजीकरण करने वाला व्यक्ति वास्तविक जीवित मानव है या वेबसाइट में स्पैम का प्रयास करने वाला कंप्यूटर प्रोग्राम है।



स्रोत : कैप्चा

चित्र 6.6 : सिस्टम निर्मित कैप्चा कोड

कैप्चा का उपयोग वेबसाइट को हैकर्स से सुरक्षित बनाता है, लेकिन साथ ही यह वास्तविक उपयोगकर्ताओं को परेशान करता है। कैप्चा का उपयोग करके हम अनधिकृत उपयोगकर्ताओं से स्पैम ईमेल प्राप्त करने से सुरक्षित हो सकते हैं, इस प्रकार यह वेबसाइट को उपयोगकर्ताओं के लिए सुरक्षित बनाता है।

6.10.1 कैप्चा का उद्देश्य

कैप्चा आमतौर पर उपयोग किया जाता है जब वेब एप्लिकेशन को उपयोगकर्ता इनपुट की आवश्यकता होती है। कल्पना कीजिए कि आप एक ऑनलाइन स्टोर चला रहे हैं और अपने ग्राहकों को एक कमेंट सेक्शन में प्रोडक्ट रिव्यू लिखने का अवसर देना चाहते हैं। इस मामले में, आप यह सुनिश्चित करना चाहते हैं कि प्रविष्टियाँ वास्तव में आपके ग्राहकों से हों या कम से कम मानव साइट विज़ीटर से।

आप कैप्चा के साथ ऑनलाइन फॉर्म की सुरक्षा करके, उपयोगकर्ताओं को यह सत्यापित करने के लिए कि वे मानव हैं इससे पहले कि वे अपनी टिप्पणी प्रस्तुत कर सकें, इससे होने वाले जोखिम को कम कर सकते हैं। कैप्चा अब लगभग सभी क्षेत्रों में पाए जाते हैं जहां मानव उपयोगकर्ताओं को बॉट्स से अलग होने की आवश्यकता होती है। उदाहरण के लिए, इसमें ई-मेल सेवाओं, समाचार पत्र, समुदायों और सामाजिक नेटवर्क के साथ-साथ ऑनलाइन सर्वेक्षण या वेब सेवाओं, जैसे सर्च इंजन सर्विसेज सेवाओं के लिए पंजीकरण फॉर्म शामिल हैं।

6.10.2 कैप्चा का प्रकार

मानव सत्यापन के लिए कैप्चा-आधारित विधियों को मोटे तौर पर टैक्स्ट और इमेज-आधारित कैप्चा, ऑडियो कैप्चा, गणितीय कैप्चा, लॉजिक कैप्चा और गैमिफिकेशन कैप्चा में विभाजित किया जा सकता है।

- 1) **टेक्स्ट-आधारित कैप्चा:** मानव सत्यापन का सबसे पुराना रूप टेक्स्ट-आधारित कैप्चा है। ज्ञात शब्दों या अक्षरों और अंकों के अत्यवस्थित (Random) संयोजन अलग-थलग हैं। जारी रखने के लिए, एक उपयोगकर्ता को कैप्चा बॉक्स में

दर्शाए गए कोड को समझने और पाठ बॉक्स में समाधान दर्ज करना होगा। टेक्स्ट-आधारित कैप्चा बनाने के लिए उपयोग की जाने वाली क्लासिक तकनीकें हैं जिम्पी, ईज-जिम्पी, जिम्पी-आर और सिमर की एचआईपी।

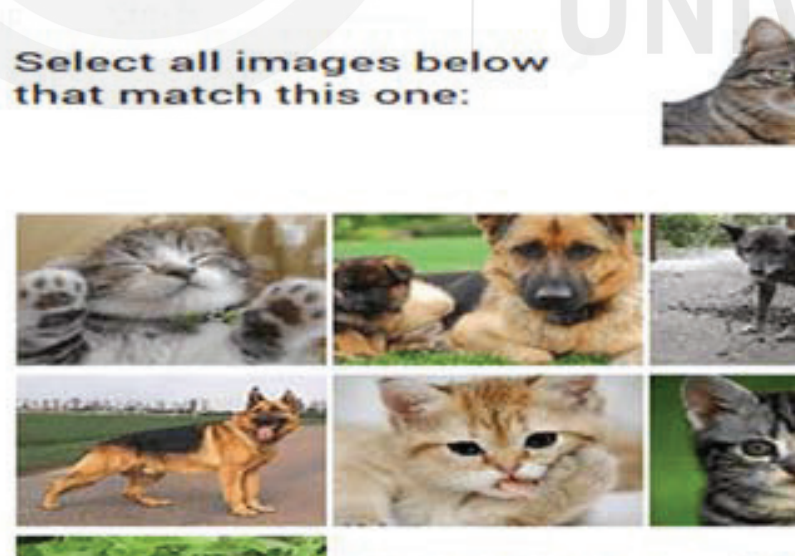


चित्र: 6.7 : टेक्स्ट आधारित कैप्चा

पाठ विरूपण और पृष्ठभूमि शोर को पहचानने की प्रणाली को पढ़ना मुश्किल बना देना चाहिए। टेक्स्ट कैप्चा केवल स्पैम के खिलाफ विश्वसनीय सुरक्षा प्रदान करता है जब समाधान को स्वचालित टेक्स्ट मान्यता वाले कार्यक्रमों द्वारा क्रैक नहीं किया जा सकता है।

- 1) **छवि-आधारित कैप्चा:** टेक्स्ट कैप्चा का विकल्प छवि-आधारित विधि है। उपयोगकर्ताओं को अंकों और अक्षरों से युक्त एक अलग-थलग समाधान के साथ प्रस्तुत करने के बजाय, छवि-आधारित कैप्चा जल्दी पहचाने जाने योग्य रेखांकन तत्वों पर आधारित होते हैं। एक नियम के रूप में, रोजमर्रा की वस्तुओं की कई तस्वीरें एक के बाद एक मिलाकर दिखाई जाती हैं। उपयोगकर्ता को उन छवियों पर क्लिक करना होगा जो मूल छवि के समान हैं, या यह दिखाने के लिए कि कौन सी शब्दार्थ सामग्री का दर्शाता है। यह अगला उदाहरण एक बिल्ली को मुख्य छवि के रूप में दिखाता है। तब उपयोगकर्ता को यह तय करना होगा कि अन्य 9 तस्वीरों में से कौन सी बिल्लियों को दर्शाती है, और फिर कैप्चा को पूरा करने के लिए उन पर क्लिक करें।

नीचे दी गई सभी छवियों का चयन इस एक से करें।



चित्र: 6.8 : चित्र आधारित कैप्चा

- 2) **ऑडियो कैप्चा:** टेक्स्ट और इमेज कैप्चा को ग्राफिकल ह्यूमन वेरिफिकेशन प्रोसेस को सौंपा जा सकता है। क्या कोई मानव उपयोगकर्ता आसानी से इस

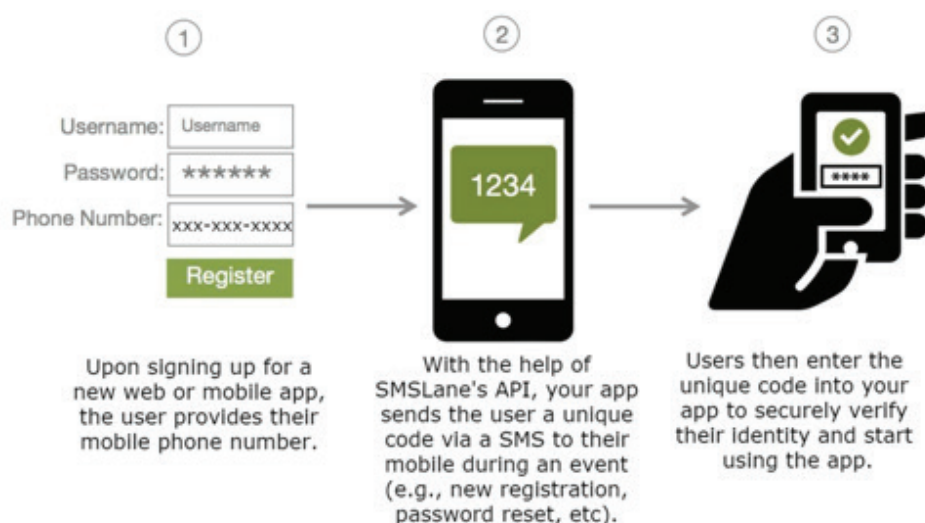
चरण को पार कर सकता है, यह इस बात पर निर्भर करता है कि प्रदर्शित टैक्स्ट या छवि जानकारी को पहचानने की उनकी क्षमता कितनी अच्छी है। एक नेत्रहीन व्यक्ति एक कैप्चा कैसे पढ़ पाएगा? वेबसाइट संचालकों को यह सुनिश्चित करना चाहिए कि उनकी चयनित कैप्चा विधि में उनकी वेबसाइट की उपयोगिता बढ़ाने के लिए कई समाधान हैं। ताकि दृष्टिबाधित लोग भी कैप्चा कोड को सफलतापूर्वक हल कर सकें, टैक्स्ट-आधारित या इमेज-आधारित परीक्षण विधियां आमतौर पर तथाकथित ऑडियो कैप्चा के साथ संयुक्त होती हैं। अक्सर एक अतिरिक्त बटन होता है जिसे उपयोगकर्ता ऑडियो रिकॉर्डिंग सुनने के लिए दबा सकता है, उदाहरण के लिए संख्याओं का एक छोटा अनुक्रम, जो तब इनपुट क्षेत्र में प्रवेश करता है।

- 3) **गणितीय कार्य और तर्क कैप्चा:** एक कैप्चा विकल्प, जो दृष्टिहीनों की जरूरतों को भी ध्यान में रखता है, गणित के कार्यों या पहेलियों पर निर्भर करता है ताकि स्पैम्बोट्स को फिल्टर किया जा सके। यदि आवश्यक हो तो निम्नलिखित कार्य को स्क्रीन रीडर से पढ़ा जा सकता है, तो इसका अर्थ है कि इसका उपयोग गैर-विजुअल आउटपुट डिवाइस वाले उपयोगकर्ताओं द्वारा भी किया जा सकता है। स्वयं को मानव के रूप में सत्यापित करने के लिए, उपयोगकर्ताओं को एक गणितीय समस्या को हल करना होगा। ये गणितीय समीकरण हल करने में सरल हैं, लेकिन समस्या यह है कि वे कंप्यूटर के लिए बहुत बाधा नहीं हैं क्योंकि कंप्यूटर लोग संख्याओं से निपटने में अच्छे हैं। इस प्रकार के कैप्चा को अक्सर विभिन्न प्रकार के पाठ अलगाव के साथ जोड़ा जाता है ताकि स्क्रीन पाठकों के लिए इसका अर्थ निकालना असंभव हो। उदाहरण के लिए 7×7 की गणना करें और केवल बॉक्स में परिणाम का पहला अंक दर्ज करें। परिणाम 49 होगा, इसलिए कैप्चा समाधान 4 होगा।

6.11 ओटीपी (वन टाइम पासवर्ड)

ओ.टी.पी.(OTP) का फुल फॉर्म वन-टाइम पासवर्ड है। इसे वन-टाइम पिन के रूप में भी जाना जाता है। ओटीपी एक पासवर्ड है जिसका उपयोग केवल एक बार कंप्यूटर सिस्टम में लॉगिन करने और सुरक्षित ऑनलाइन लेनदेन करने के लिए किया जा सकता है। ओ.टी.पी.(OTP) संख्यात्मक या अल्फान्यूमेरिक स्वचालित जनरेटेड स्ट्रिंग है जिसका उपयोग एकल लेनदेन या लॉगिन सत्र के लिए वन-टाइम पासवर्ड के रूप में किया जाता है। ओटीपी एक स्थिर पासवर्ड की तुलना में अधिक सुरक्षित है, और इसे उपयोगकर्ता के पंजीकृत मोबाइल नंबर पर भेजा जाता है। चूंकि ओटीपी (OTP) उपयोगकर्ता के पंजीकृत मोबाइल नंबर पर प्राप्त होता है इस कारण से साइबर हैकर्स द्वारा इसके दुरुपयोग की संभावना कम होती है। ओ.टी.पी.(OTP) अतिरिक्त प्रमाणीकरण प्रक्रिया है जिसका उपयोग वास्तविक उपयोगकर्ता को प्रमाणित करने के लिए वेबसाइट द्वारा डबल ऑथेंटिकेट (Double Authenticate) करने के लिए किया जाता है इससे पहले कि वह संसाधनों के उपयोग की अनुमति दे। कंप्यूटर सिस्टम या कोई सर्वर को दें। ओ.टी.पी.(OTP) सुरक्षा टोकन माइक्रोप्रोसेसर-आधारित स्मार्ट कार्ड या पॉकेट-आकार के प्रमुख फॉन्स हैं जो सिस्टम या लेनदेन की

पहुंच को प्रमाणित करने के लिए एक संख्यात्मक या अल्फान्यूमेरिक कोड का उत्पादन करते हैं।



Source: smslane.com

चित्र 6.9 : टू फैक्टर एस.एम.एस. आथेंटिकेशन

यह गुप्त कोड हर 30 या 60 सेकंड में बदलता है, यह इस बात पर निर्भर करता है कि टोकन कैसे कॉन्फिगर किया गया है। मोबाइल उपकरण ऐप, जैसे कि गूगल (Google) प्रमाणक, टू-स्टेप सत्यापन के लिए वन-टाइम पासवर्ड जनरेट करने के लिए टोकन डिवाइस और पिन पर निर्भर करते हैं। ओ.टी.पी. (OTP) सुरक्षा टोकन को हार्डवेयर, सॉफ्टवेयर या मांग के आधार पर लागू किया जा सकता है। पारंपरिक पासवर्डों के विपरीत जो स्थिर रहते हैं यह हर 30 से 60 दिनों में समाप्त हो जाते हैं, वन-टाइम पासवर्ड का उपयोग एक लेनदेन या लॉगिन सत्र के लिए किया जाता है।

6.11.1 वन-टाइम पासवर्ड कैसे प्राप्त करें

जब कोई अनधिकृत उपयोगकर्ता किसी सिस्टम पर पहुंचने या डिवाइस पर लेन-देन करने का प्रयास करता है, तो नेटवर्क सर्वर पर एक प्रमाणीकरण प्रबंधक एक बार के पासवर्ड एल्गोरिदम का उपयोग करके, एक नंबर या साझा किए गए रहस्य को उत्पन्न करता है। एक ही नंबर और एल्गोरिथ्म का उपयोग स्मार्ट कार्ड या डिवाइस पर सुरक्षा टोकन द्वारा एक बार के पासवर्ड और उपयोगकर्ता के मिलान और सत्यापन के लिए किया जाता है। कई कंपनियां दूसरे प्रमाणीकरण कारक के लिए पाठ के माध्यम से एक अस्थायी पास-कोड प्रदान करने के लिए लघु संदेश सेवा (एसएमएस) का उपयोग करती हैं। अस्थायी पास कोड सेल फोन संचार के माध्यम से प्राप्त किया जाता है जब उपयोगकर्ता इंकॉर्पोरेशन सिस्टम (सूचना प्रणाली) और लेन-देन वेब इप्लिकेशन पर अपने उपयोगकर्ता नाम और पासवर्ड दर्ज करता है। टू फैक्टर ऑथेंटिकेशन (2FA) के लिए, उपयोगकर्ता खाता या सिस्टम तक पहुंचने के लिए अपनी यूजर आईडी, पारंपरिक पासवर्ड और अस्थायी पास-कोड दर्ज करता है।

6.11.2 वन-टाइम का पासवर्ड कैसे काम करता है

साइबर सुरक्षा की एन्क्रिप्शन और डिक्రిप्शन तकनीकों का उपयोग ओटीपी उत्पन्न करने के लिए किया जाता है। हम ओ.टी.पी.(OTP) – आधारित प्रमाणीकरण संदेश उत्पन्न करने के लिए साइबर सुरक्षा के गणितीय मैसेज औथेंटिकेशन कोड (HMAC) एल्गोरिथ्म का उपयोग करते हैं। यह ओटीपी संदेश तब पंजीकृत मोबाइल नंबर के उपयोगकर्ताओं को भेजा जाता है। सुरक्षा कारणों से ओ.टी.पी.(OTP) मान उनकी पीढ़ियों के कुछ सेकंड के लिए मान्य हैं और उपयोगकर्ताओं को कंप्यूटर सिस्टम या सर्वर के संसाधनों तक पहुंचने के लिए लॉगिन करने के लिए उस निर्दिष्ट समय के दौरान उन्हें दर्ज करना चाहिए। वन-टाइम पासवर्ड कई चैनलों के माध्यम से एक उपयोगकर्ता को दिया जाता है, जैसे कि एसएमएस-आधारित टैक्स्ट संदेश, ईमेल या अंतिम बिंदु पर एक समर्पित एप्लिकेशन।

6.11.3 वन-टाइम पासवर्ड के लाभ

ओ.टी.पी.(OTP) का उपयोग वास्तविक उपयोगकर्ताओं को उनके क्रेडेंशियल के साथ-साथ सुरक्षित रूप से प्राप्त ओ.टी.पी.(OTP) पाठ संदेश को उपयोगकर्ता के पंजीकृत मोबाइल नंबर पर प्राप्त करने के लिए सुरक्षित वेबसाइट पर लॉग इन करने की अनुमति देने के लिए किया जाता है। यह आईटी प्रबंधकों के लिए किसी भी व्यावसायिक संगठन के आईटी प्रशासकों के लिए बहुत उपयोगी है और उपयोगकर्ताओं के साथ-साथ कंपनी के ग्राहकों के लिए वेबसाइट को सुरक्षित बनाता है। ओटीपी का लाभ यह है कि वे सेकेंडों में अमान्य हो जाते हैं और इस प्रकार अनधिकृत हमलावरों को गुप्त कोड प्राप्त करने से और अवैध रूप से व्यावसायिक डेटा को फिर से हैक करने से रोकता है।

बोध प्रश्न घ

भाग क : बहुविकल्प प्रश्न

- 1) साइबर अपराध क्या है?
 - क) वायरस का हमला
 - ख) वॉर्म का हमला
 - ग) सिस्टम हैक करना
 - घ) उपरोक्त सभी
- 2) किसी व्यक्ति या व्यक्तियों के समूह को परेशान करने के लिए इंटरनेट का उपयोग:
 - क) कैबरेनेट
 - ख) साइबर पुलिसिंग
 - ग) साइबर स्टैकिंग
 - घ) साइबर स्पेस
- 3) हमें इंटरनेट का उपयोग करके उत्पीड़न को रोकने के लिए नीचे दिए गए चरणों का पालन करना चाहिए

- क) एंटी-वायरस स्थापित करके
 - ख) अनियमित बैंक-अप लेने से
 - ग) अज्ञात लिंक पर क्लिक न करके
 - घ) उपरोक्त सभी
- 4) बड़ी संख्या में व्यक्तियों को उनकी सहमति के बिना भेजे गए एक अवांछित मेल के रूप में जाना जाता है
- क) वॉर्म
 - ख) स्पैम
 - ग) ट्रोजन
 - घ) ऑनलाइन विपणन

भाग ख : लघुतरात्मक प्रश्न

- 1) डिजिटलइजेशन शब्द की व्याख्या कीजिए?

.....

.....

.....

.....

.....

- 2) कैप्चा क्या है? उपयोगकर्ता प्रमाणीकरण में उनके उपयोग की व्याख्या करें।

.....

.....

.....

.....

.....

- 3) व्यावसायिक संगठनों में डिजिटलीकरण और आईटी सुरक्षा के प्रभाव को समझाइए।

.....

.....

.....

.....

.....

- 4) ओ.टी.पी. (OTP) का पूर्ण रूप क्या है? इसका उपयोग बैंकिंग क्षेत्र में ऑनलाइन लेनदेन के लिए कैसे किया जाता है।

.....

.....

.....

6.12 सारांश

पहचान, प्रमाणीकरण और प्राधिकरण डेटा सामग्री सुरक्षा और खुले वितरित सिस्टम के उपयोगकर्ताओं के बीच सुरक्षित संचार के लिए मुख्य विशेषाधिकार हैं। ये उपाय भौतिक और तार्किक स्तर पर किए जाते हैं, और इंटरनेट और इंटरनेट के बीच संचार पर विशेष ध्यान दिया जाता है। कार्यान्वयन, स्वयं सुरक्षा सिद्धांतों का पालन किए बिना, उनके परिचय और उपयोग के लिए महत्वपूर्ण, सुरक्षा की गारंटी नहीं देता है – न तो डेटाबेस में डेटा सामग्री, या संचार में।

डेटा सामग्री को क्रिप्टोग्राफिक एल्गोरिदम के माध्यम से संरक्षित किया जाना चाहिए, जो जटिलता और गति आवश्यक सुरक्षा स्तर पर निर्भर करती है। इसका उदाहरण एक इलेक्ट्रॉनिक हस्ताक्षर, सटीकता की पुष्टि और संदेश की विश्वसनीयता का साधन है। प्रामाणिकता प्रोटोकॉल, यहां तक कि पूर्ण प्रमाणीकरण प्रणाली को गतिशील और वितरित प्रणालियों में क्रिप्टोग्राफिक एल्गोरिदम कार्यान्वयन, सुरक्षा विधियों और सिद्धांतों (डेटा सामग्री के) के रूप में उत्पन्न किया गया था, जो इलेक्ट्रॉनिक वित्तीय लेनदेन, यानी इलेक्ट्रॉनिक नकद भुगतान प्रोटोकॉल के मामले में बहुत महत्वपूर्ण हो जाते हैं।

6.13 शब्दावली

की (Key): क्रिप्टोग्राफी में, एक की जानकारी का एक टुकड़ा है जो क्रिप्टोग्राफिक एल्गोरिदम के कार्यात्मक उत्पादन को निर्धारित करता है। एन्क्रिप्शन एल्गोरिदम के लिए, एक की सिफरटेक्स्ट में प्लेनटेक्स्ट के रूपांतरण को निर्दिष्ट करता है, और इसके विपरीत डिक्रिप्शन एल्गोरिदम के लिए।

निजी की (Private Key): एक निजी की कोड का एक छोटा सा हिस्सा होता है, जिसे टेक्स्ट एन्क्रिप्शन और डिक्रिप्शन के लिए एल्गोरिदम सेट करने के लिए एक सार्वजनिक की के साथ जोड़ा जाता है।

सार्वजनिक की (Public Key): सार्वजनिक— की क्रिप्टोग्राफी, या असममित क्रिप्टोग्राफी, एक क्रिप्टोग्राफिक प्रणाली, है जो कुंजियों के जोड़े का उपयोग करती है: सार्वजनिक की जो व्यापक रूप से प्रसारित की जा सकती है, और निजी की जो केवल स्वामी को ज्ञात होती है।

एन्क्रिप्शन (Encryption): एन्क्रिप्शन किसी संदेश या सूचना को इस तरह से एन्कोडिंग करने की प्रक्रिया है कि केवल अधिकृत पक्ष ही इसे प्राप्त कर सकते हैं और जो अधिकृत नहीं हैं वे नहीं कर सकते।

डिक्रिप्शन (Decryption): डिक्रिप्शन एन्कोडेड या एनक्रिप्टेड टेक्स्ट या अन्य डेटा लेने की प्रक्रिया है और इसे वापस टेक्स्ट में परिवर्तित करना है जिसे आप या कंप्यूटर पढ़ और समझ सकते हैं। इस शब्द का उपयोग मैन्युअल रूप से डेटा को अनएन्क्रिप्ट करने या उचित कोड या कुंजी का उपयोग करके डेटा को अनएन्क्रिप्ट करने की विधि का वर्णन करने के लिए किया जा सकता है।

ओटीपी (OTP): ओ. टी. पी. (OTP) एक पासवर्ड है, जिसका उपयोग केवल एक बार कंप्यूटर सिस्टम में लॉगिन करने और सुरक्षित ऑनलाइन लेनदेन करने के लिए किया जा सकता है। यह संख्यात्मक या अल्फान्यूमेरिक स्वचालित उत्पन्न स्ट्रिंग है।

कैप्चा (CAPTCHA): मानव सत्यापन के लिए कैप्चा—आधारित तरीकों को मोटे तौर पर टेक्स्ट और इमेज—आधारित कैप्चा, ऑडियो कैप्चा, गणितीय कैप्चा, लॉजिक कैप्चा और गैमिफिकेशन कैप्चा में विभाजित किया जा सकता है।

प्रमाणीकरण (Authentication): प्रमाणीकरण प्रणाली उपयोगकर्ताओं के जानकारीयों की जांच करने की प्रक्रिया है इससे पहले कि उन्हें सिस्टम के संसाधनों का उपयोग करने के लिए प्राप्त किया जाए। यह साबित करने की क्षमता है कि उपयोगकर्ता या एप्लिकेशन वास्तविक है और इस आधार पर यह संगठन या नेटवर्क के संसाधनों का उपयोग कर सकता है।

प्राधिकरण (Authorization) : सॉफ्टवेयर कंपनियों द्वारा कानूनी तरीके से फाइल, सेवाओं, कंप्यूटर प्रोग्राम, डेटा और एप्लिकेशन प्रोग्राम सहित सिस्टम संसाधनों के लिए अनुमति देने के लिए प्राधिकरण को अपनाया जाता है। यह उपयोगकर्ता की पहचान के आधार पर एक नेटवर्क संसाधन तक पहुंच देने से इनकार करने की प्रक्रिया है।

6.14 बोध प्रश्नों के उत्तर

बोध प्रश्न क

- 1) IV
- 2) IV
- 3) III
- 4) III

बोध प्रश्न ख

- 1) घ
- 2) घ
- 3) ड
- 4) क

बोध प्रश्न ग

- 1) ख
- 2) ग
- 3) ख

बोध प्रश्न घ

- 1) घ
- 2) ग
- 3) घ
- 4) ख

6.15 स्वपरख प्रश्न

- 1) फिशिंग क्या है?
- 2) कुछ सुरक्षा हमलों की सूची बनाएं।
- 3) कौन सी तकनीक वेरनाम सिफर पर आधारित है?
- 4) क्रिप्टोनलिसिस को परिभाषित करें।
- 5) प्लेन टेक्स्ट सिफर कोडेड और कोडेड टेक्स्ट क्या है? इसके बारे में बताएं।
- 6) डिजिटल हस्ताक्षर की व्याख्या करें।
- 7) अखंडता और गैर-प्रत्यावर्तन को परिभाषित करें।
- 8) किन्हीं दो शास्त्रीय सिफरों की व्याख्या कीजिए।
- 9) वन टाइम पासवर्ड की व्याख्या कीजिए।
- 10) सक्रिय और निष्क्रिय हमले क्या हैं? उपयुक्त उदाहरण के साथ समझाइए।
- 11) क्रिप्टोग्राफी में डी.ई.एस. (DES) का क्या मतलब है?
- 12) क्रिप्टोग्राफी में उपयोग हैश फंक्शन को समझाइए।
- 13) निजी और सार्वजनिक कुंजी से आपका क्या अभिप्राय है?
- 14) हैकर्स द्वारा आपका क्या मतलब है? एथिकल हैकिंग (Ethical hacking) के बारे में भी बताएं।
- 15) डिजिटल हस्ताक्षर पर चर्चा करें?

नोट: ये प्रश्न आपके अभ्यास के लिए हैं। इनके उत्तर लिखने का अभ्यास करें किंतु उत्तरों को विश्वविद्यालय में मूल्यांकन के लिए न भेजें। प्रश्नों के उत्तर लिखकर आप स्वयं अपनी प्रगति की जाँच कर सकते हैं।

इकाई 7 इंटरनेट सेवाएं और ई-मेल कॉन्फिगरेशन

इकाई की रूपरेखा

- 7.0 उद्देश्य
- 7.1 प्रस्तावना
- 7.2 इंटरनेट के बारे में
 - 7.2.1 इंटरनेट कैसे काम करता है।
- 7.3 इंटरनेट सेवाओं के प्रकार
- 7.4 ई-मेल और इसके कॉन्फिगरेशन के बारे में
- 7.5 वेब ब्राउजर्स
- 7.6 WWW (वर्ल्ड वाइड वेब)
- 7.7 यू .आर .एल. (URL) (यूनिफॉर्म रिसोर्स लोकेटर)
- 7.8 डोमेन नाम
- 7.9 सारांश
- 7.10 शब्दावली
- 7.11 बोध प्रश्नों के उत्तर
- 7.12 स्वपरख प्रश्न

7.0 उद्देश्य

इस इकाई को पढ़ने के बाद आप इस योग्य हो सकेंगे कि

- इंटरनेट के विभिन्न उपयोगों और लाभों की पहचान कर सकें;
- इंटरनेट कैसे कार्य करता है यह समझ सकें;
- विभिन्न प्रकार की इंटरनेट सेवाओं का वर्णन कर सकें; और
- कार्यक्षेत्र का नाम और यू आर .एल.(URL) के महत्व का वर्णन कर सकें।

7.1 प्रस्तावना

सूचना प्रौद्योगिकी के क्षेत्र में विकास के साथ, इंटरनेट सूचना के आदान प्रदान, ऐसे अवसर प्रदान करने, जो कि कभी नहीं सुने हों, सूचना के आदान प्रदान को आसान बनाने आदि के लिए एक सर्वव्यापी साधन बन गया है। यह हमें लोगों और संसाधनों तक पहुंचने, बातचीत करने और कनेक्ट करने के लिए एक प्रवेश द्वार प्रदान करता है। इंटरनेट की लोकप्रियता में वृद्धि इसके लिए प्रदान की जाने वाली सेवाओं के लिए जिम्मेदार हो सकती है, जिनका उपयोग व्यापार, विचार-विमर्श ज्ञान में सुधार/बैंकिंग, आदि के लिए किया जाता है।

ई-मेल (इलेक्ट्रॉनिक मेल) इंटरनेट द्वारा प्रदान की जाने वाली सबसे लोकप्रिय सेवा है। ई-मेल मूल रूप से दुनिया भर के लोगों के बीच इलेक्ट्रॉनिक संदेश संचार है।

कुछ अन्य लोकप्रिय सेवाओं में डब्ल्यू. डब्ल्यू. डब्ल्यू. (वर्ल्ड वाइड वेब), वेब सेवाएं, एफ. टी. पी. (फाइल ट्रांसफर प्रोटोकॉल), चैट रूम, वीडियो कॉन्फ्रेंसिंग, न्यूज ग्रुप्स, इंस्टेंट मैसेजिंग आदि शामिल हैं। इन सेवाओं में से अधिकांश में यूनिट के आगामी वर्गों के बारे में विस्तार से चर्चा की गई है।

7.2 इंटरनेट के बारे में

जैसा कि स्ट्रॉस, एल-अंसारी, फ्रॉस्ट (2003) द्वारा परिभाषित किया गया है “इंटरनेट एक संपूर्ण नेटवर्क है जो एक दूसरे से जुड़े हुए हैं। इस नेटवर्क के कुछ कंप्यूटर वेब फाइलों जैसे फाइलों को संग्रहीत करते हैं, जिन्हें सभी नेटवर्क कंप्यूटरों द्वारा एक्सेस किया जा सकता है।” जबकि ओ ब्रायन (2003) ने कहा कि “इंटरनेट लाखों व्यवसायों, शिक्षा और सरकारी नेटवर्क का तेजी से बढ़ता कंप्यूटर नेटवर्क है जो 200 से अधिक देशों के उपयोगकर्ताओं की संख्या में परस्पर जुड़ा हुआ है।”

उपरोक्त परिभाषाओं के आधार पर इंटरनेट की मूल अवधारणा सूचनाओं के आदान-प्रदान के लिए भौतिक रूप से जुड़े उपकरणों का वैश्विक नेटवर्क है। इसे ‘नेटवर्कों के नेटवर्क’ के रूप में संदर्भित किया जा सकता है, जिसमें नेटवर्किंग तकनीक से जुड़े लाखों इंटरकनेक्टेड डिवाइस शामिल हैं। इंटरनेट असंख्य साथ और अवसर प्रदान करता है। उनमें से कुछ हैं:

- **संचार में आसानी:** ईमेल और चैटिंग के उपलब्ध विकल्पों के साथ, हम आसानी से वास्तविक समय में अन्य व्यक्तियों से जुड़ सकते हैं।
- **चौबीसों घंटे उपलब्ध:** इंटरनेट सेवाएं चौबीसों घंटे उपलब्ध हैं।
- **सूचना स्रोत:** इंटरनेट ने हमें धरती पर कहीं से भी असीमित मात्रा में इंटरनेट का उपयोग करने में सक्षम बनाया है।
- **ई-कॉमर्स:** इलेक्ट्रॉनिक कॉमर्स का जन्म इंटरनेट से हुआ है। हम सिर्फ एक क्लिक पर विभिन्न वेबसाइटों पर ऑनलाइन खरीदारी कर सकते हैं। हमें चीजों को ऑर्डर करने के लिए दुकानों पर जाने की आवश्यकता नहीं है।
- **अन्य सेवाएं:** इंटरनेट बैंकिंग, होटल बुकिंग, टिकट बुकिंग, नौकरी की खोज, यहां तक कि परामर्श सेवाएं भी इंटरनेट द्वारा उपलब्ध कराई जा रही हैं।

7.2.1 इंटरनेट कैसे काम करता है।

इंटरनेट विशेष रूप से आई. पी. (इंटरनेट प्रोटोकॉल) टी. सी. पी. (ट्रांसपोर्ट कंट्रोल प्रोटोकॉल) जो कि पैकेट रूटिंग नेटवर्क का पालन करते हैं के द्वारा काम करता है।

- **प्रोटोकॉल:** कंप्यूटर के अनुसार एक दूसरे के साथ संचार के नियमों का सेट प्रोटोकॉल के रूप में जाना जाता है।
- **पैकेट रूटिंग नेटवर्क** इंटरनेट पर भेजे गए डेटा के टुकड़ों को पैकेट कहा जाता है। पैकेट रूटिंग नेटवर्क के मामले में, पैकेट को गंतव्य कंप्यूटर के लिए स्रोत निर्देशित किया जाता है।

- **इंटरनेट प्रोटोकॉल:** इसके द्वारा भेजे गए डेटा पर पतों को संलग्न करके जानकारी को कैसे रूट किया जाए, यह निर्दिष्ट करने के लिए नियमों का सेट।
- **परिवहन नियंत्रण प्रोटोकॉल:** टी.सी.पी. गंतव्य पर संदेश के पुनर्निर्माण यदि कोई सूचना छूट जाये जो उसे दोबारा भेजने को संभालता है।

7.3 इंटरनेट सेवाओं के प्रकार

जैसा कि पिछले भाग में बताया गया है, इंटरनेट एक जुड़ा हुआ वैश्विक कंप्यूटर नेटवर्क है, जो प्रोटोकॉल नामक नियमों के निश्चित समूह के माध्यम से संचालित होता है। अंत-उपयोगकर्ता के दृष्टिकोण से यह इंटरनेट को प्रदान करने वाली सेवाओं को लोकप्रिय बनाता है।

- क) **ई-मेल (इलेक्ट्रॉनिक मेल):** ई-मेल लोगों के बीच संदेश विनिमय का डिजिटल रूप है। दुनिया भर में संदेश को सेकंडों में भेजने की क्षमता ने इसे संदेश संचार का सबसे लोकप्रिय रूप बना दिया है और इसने जीवन के कई क्षेत्रों में इस्तेमाल होने वाले संचार के हर दूसरे भौतिक रूप जैसे पत्र की जगह ले ली है।
- ख) **वर्ल्ड वाइड वेब:** इंटरनेट की सबसे महत्वपूर्ण सेवा जो अनिवार्य रूप से वैश्विक जानकारी साझा करने के लिए है। यह सभी संसाधनों का संयोजन है—टेक्स्ट पेज, डिजिटल फोटोग्राफ, संगीत फाइलें, वीडियो और संचार मॉडल के माध्यम से इंटरनेट पर सूचनाओं के आदान-प्रदान को सक्षम बनाता है।
- ग) **वेब सेवाएँ:** वेब सेवाएँ इंटरनेट पर क्लाइंट और सर्वर अनुप्रयोगों के बीच संचार के प्रसार के लिए मानकीकृत माध्यम हैं।
- घ) **फाइल ट्रांसफर प्रोटोकॉल (एफ.टी.पी.):** एफटीपी का उपयोग इंटरनेट के माध्यम से कंप्यूटर पर फाइलों के आदान-प्रदान के लिए किया जाता है।
- ङ) **चैट रूम:** वे माध्यम हैं जिनका उपयोग व्यक्तियों के बीच वास्तविक समय की बातचीत, टेक्स्ट, वॉइस या वीडियो के रूप किया जाता है।
- च) **मेलिंग सूची:** यह उन लोगों को शामिल करने के लिए नाम या / और पते का संग्रह है जो नियमित आधार पर डाक वितरण की सदस्यता लेते हैं।
- छ) **न्यूज ग्रुप्स:** यह दुनिया भर में विभिन्न उपयोगकर्ताओं को दूरस्थ रूप से जोड़ने के द्वारा विभिन्न विषयों पर चर्चा के लिए एक इंटरनेट-आधारित मंच है।

बोध प्रश्न क

- 1) इंटरनेट क्या है?

.....

.....

.....

.....

.....

.....

2) इंटरनेट के किसी भी चार लाभों को सूचीबद्ध करें।

.....

.....

.....

.....

.....

3) रिक्त स्थान भरें:

- 1) ऐसे माध्यम हैं जो व्यक्तियों के बीच वास्तविक समय की गई बातचीत टेक्स्ट, वॉयस या वीडियो के रूप में उपयोग किए जाते हैं।
- 2) एक नेटवर्क है जो पैकेट को स्रोत से गंतव्य कंप्यूटर तक निर्देशित करता है।
- 3) इंटरनेट के माध्यम से कंप्यूटरों में फाइलों के आदान-प्रदान के लिए उपयोग किया जाता है।
- 4) को नेटवर्क ऑफ नेटवर्क 'कहा जा सकता है।

7.4 ई-मेल और इसके कॉन्फिगरेशन के बारे में

ई-मेल या इलेक्ट्रॉनिक मेल इंटरनेट द्वारा प्रदान की जाने वाली सबसे लोकप्रिय सेवाओं में से एक है, जहां हम इंटरनेट पर सेकंड में दुनिया में कहीं भी बैठे लोगों से संदेश भेज सकते हैं या प्राप्त कर सकते हैं। इलेक्ट्रॉनिक मेल 1960 के दशक में पेश किया गया था। आज की दुनिया में हम में से ज्यादातर लोग अपने जीवन को आसान बनाने के लिए ईमेल का उपयोग कर रहे हैं।

एक इलेक्ट्रॉनिक मेल में संचार आमतौर पर तीन प्रोटोकॉल के माध्यम से किया जाता है:

- **एस.एम.टी.पी. (SMTP)** एस.एम.टी.पी. का अर्थ "सिंपल मेल ट्रांसफर प्रोटोकॉल" है जो मेल भेजने के लिए उपयोग किया जाता है। मेल में संदेश एक मेल क्लाइंट (जैसे जीमेल) द्वारा एक रिसीवर को भेजा जाता है जिसमें ईमेल सर्वर प्राप्त करना शामिल होता है। ईमेल भेजने की प्रक्रिया को पूरा करने के लिए प्रेषक SMTP सर्वर का उपयोग करता है।
- **आई.एम.ए.पी. (IMAP)** : आई.एम.ए.पी. (IMAP) का अर्थ "इंटरनेट मेल एक्सेस प्रोटोकॉल" है जो सर्वर प्राप्त करने से ईमेल को प्रबंधित और पुनः प्राप्त करने से संबंधित है"। ये प्रोटोकॉल केवल ईमेल प्राप्त करते समय उपयोग किए जाते हैं और ईमेल भेजने के लिए इनका उपयोग नहीं किया जा सकता है। ईमेल सर्वर में मौजूद होंगे और उपयोगकर्ता के डिवाइस पर डाउनलोड नहीं किए जाएंगे और उन्हें संपादित (एडिटेड) किया जा सकता है जैसे कि वे उपयोगकर्ता के डिवाइस पर हैं। उपयोगकर्ता एक साथ कई उपकरणों से सर्वर से जुड़ सकता है।

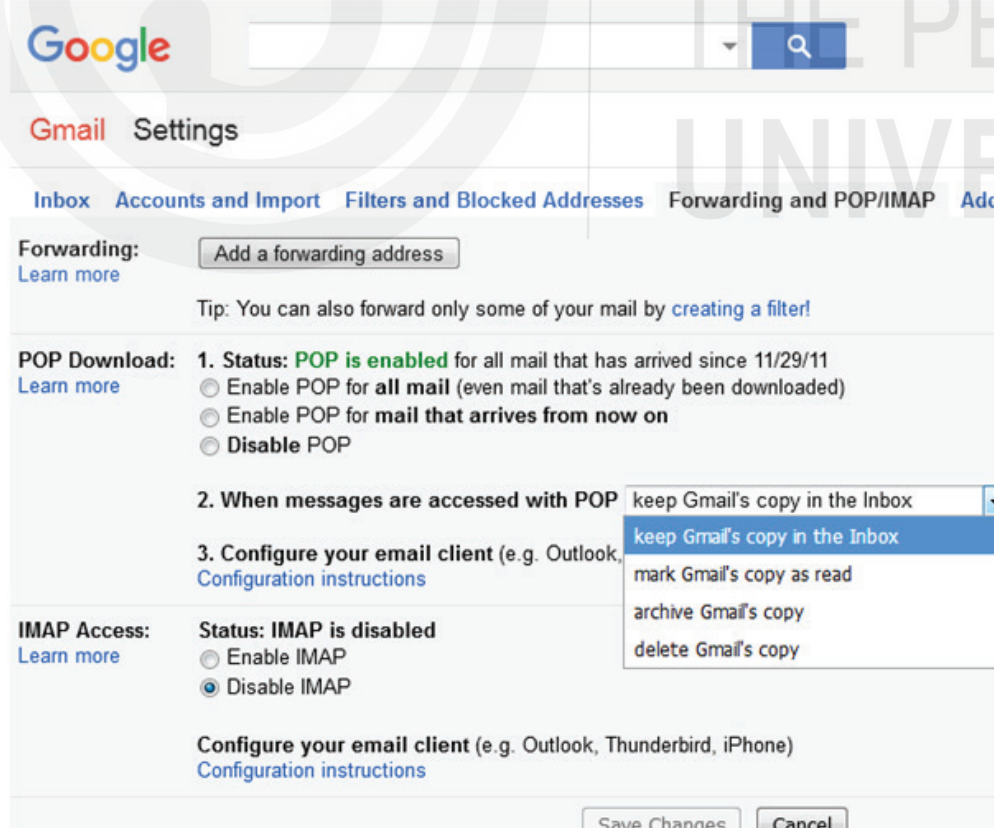
- **पी.ओ.पी. :** पी.ओ.पी. का अर्थ है “पोस्ट ऑफिस प्रोटोकॉल जो आने वाले ईमेल के लिए भी उपयोग किया जाता है”। वर्तमान संस्करण 3 है और POP3 सबसे व्यापक रूप से उपयोग किया जाने वाला संस्करण है। आई.एम.ए.पी के विपरीत यह संपूर्ण ईमेल को स्थानीय उपयोगकर्ता डिवाइस में डाउनलोड करता है। उपयोगकर्ता सिस्टम पर मेल डाउनलोड हो जाने के बाद, यह सर्वर पर डेटा को हटा देता है तथा सर्वर को बचाने में सहायक है। यह एक डाकघर की तरह काम करता है, जहां अंतिम उपयोगकर्ता को वितरित किए जाने से पहले पत्र अस्थायी रूप से संग्रहीत किए जाते हैं।

क्या आपको आई.एम.पी. (IMAP) या पी.ओ.पी. 3(POP3) का उपयोग करना चाहिए?

अनिवार्य रूप से, यह उस तरीके पर निर्भर करता है जिस तरह से हम अपने ईमेल तक पहुंच सकते हैं। कई उपकरणों पर काम करने के मामले में ईमेल प्राप्त करने के लिए अनुशंसित विधि आई.एम.ए.पी (IMAP) या इंटरनेट मेल एक्सेस प्रोटोकॉल होगी। हालांकि, अगर हमारे पास ईमेल के लिए एक निर्दिष्ट उपकरण है और सभी ईमेलों को ऑफलाइन एक्सेस करना पसंद करते हैं, तो हम पीओपी (POP) के साथ उपयुक्त विकल्प के रूप में जा सकते हैं।

जी मेल में आई.एम.ए.पी और POP3 सेटिंग्स

उदाहरण के रूप में हम जीमेल में आई.एम.ए.पी और पी.ओ.पी.3 सेटिंग्स को कैसे कॉन्फिगर किया जाएगा दिखायेंगे।



चित्र 7.1 : गूगल में में आई.एम.पी.पी.ओ.पी सेटिंग्स

7.5 वेब ब्राउजर्स

कल्पना कीजिए कि आप पिकनिक के लिए बाहर जाना चाहते हैं, आप वहां कैसे पहुंचेंगे? हम अपनी पसंद और सुविधा के आधार पर कार, सार्वजनिक बस, मेट्रो, रिक्शा या परिवहन के किसी अन्य तरीके का विकल्प चुन सकते हैं। एक वेब ब्राउजर परिवहन का एक डिजिटल मोड है जो हमें इंटरनेट के माध्यम से यात्रा करने और हमारी पसंदीदा वेबसाइटों पर जाने की अनुमति देता है। हमारे पसंद और सुविधा के आधार पर, हम किसी भी वेब ब्राउजर के लिए जा सकते हैं।

वेब ब्राउजर एक कंप्यूटर में स्थापित कंप्यूटर सॉफ्टवेयर एप्लीकेशन है, जिसका उपयोग इंटरनेट पर वेब पेज देखने के लिए किया जाता है। आज विभिन्न वेब ब्राउजर का उपयोग किया जाता है। उनमें से सबसे लोकप्रिय हैं:



Source: Interactive Powers' Elaboration

चित्र 7.2 : विभिन्न वेब ब्राउजर

- **गूगल क्रोम (Google Chrome):** यह वेब ब्राउजर 2008 में Google द्वारा एक है।
- **मोजिला फायरफॉक्स (Mozilla Firefox):** इस ब्राउजर को 2004 में जारी मोजिला द्वारा विकसित किया गया था और आज यह दूसरा सबसे लोकप्रिय ब्राउजर है।
- **माइक्रोसोफ्ट इंटरनेट एक्सप्लोरर (Microsoft Internet Explorer):** इंटरनेट एक्सप्लोरर को सॉफ्टवेयर दिग्गज माइक्रोसोफ्ट द्वारा विकसित किया गया है, यह 1995 में पेश किया गया था।
- **ओपेरा ब्राउजर (Opera Browser) :** ओपेरा 1996 में पहली बार ओपेरा सॉफ्टवेयर द्वारा प्रकाशित किया गया था जो कि सभी ब्राउजर से छोटा और तेज था।
- **ऐप्पल सफारी (Apple Safari):** सफारी एक वेब ब्राउजर है जिसे ऐप्पल इंकॉर्पोरेशन- द्वारा विकसित किया गया है। यह ऐप्पल द्वारा पहली बार 2003 में जारी किया गया था।

ये सभी ब्राउजर डाउनलोड करने के लिए स्वतंत्र हैं। वे उपयोगकर्ताओं को संसाधनों में मौजूद हाइपरलिंक के माध्यम से सर्वर पर संग्रहीत किए गए संसाधनों तक पहुंचने

की अनुमति देते हैं। उदाहरण यदि आप www.ignou.ac.in पर जाते हैं, तो आप वास्तव में हाइपर टेक्स्ट मार्क—अप भाषा या एच.टी.एम.एल. का उपयोग करके वेब ब्राउजर के माध्यम से प्रदर्शित होने वाली फाइल देख रहे हैं। वेब ब्राउजर न केवल वेब पेज देखने के लिए अच्छा है, बल्कि इसका उपयोग एफ.टी.पी. का उपयोग करके फाइलों को डाउनलोड करने और अपलोड करने के लिए किया जा सकता है।

बोध प्रश्न ख

1) ईमेल के माध्यम से संचार करने के लिए तीन प्रोटोकॉल क्या हैं?

.....

.....

.....

.....

.....

2) वेब ब्राउजर क्या है?

.....

.....

.....

.....

3) रिक्त स्थान भरें:

- i)ऐप्पल इंकॉर्पोरेशन द्वारा विकसित एक वेब ब्राउजर है।
- ii) वेब ब्राउजर न केवल वेब पेज देखने के लिए अच्छा है, बल्कि इसका उपयोगका उपयोग करके फाइलों को डाउनलोड करने और अपलोड करने के लिए किया जा सकता है।
- iii)2008 में गूगल द्वारा वेब ब्राउजर विकसित किया गया था।
- iv) प्रोटोकॉल एक पोस्ट ऑफिस की तरह काम करता है जहां अंतिम उपयोगकर्ता को वितरित किए जाने से पहले पत्र अस्थायी रूप से संग्रहीत होते हैं।

7.6 WWW (वर्ल्ड वाइड वेब)

वर्ल्ड वाइड वेब या डब्ल्यू.डब्ल्यू.डब्ल्यू. को आमतौर पर 1989 में टिमोथी बर्नर्स ली द्वारा बनाए गए वेब के रूप में जाना जाता है जो जेनेवाफोर में यूरोपीय कण भौतिकी प्रयोगशाला में शोधकर्ताओं को प्रयोगशाला में एक साथ काम करने की अनुमति देता है। आखिरकार 1996 में, यह वर्ल्ड वाइड वेब बन गया।

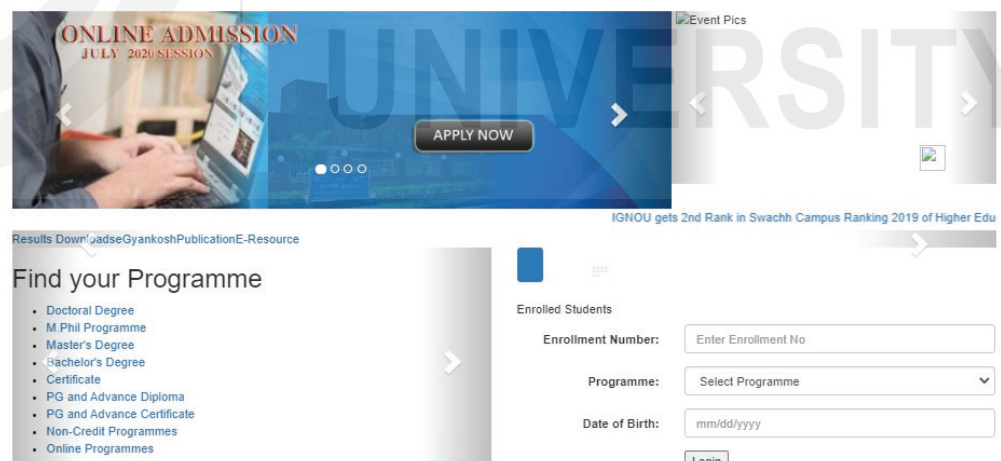
वर्ल्ड वाइड वेब केवल इंटरनेट पर कंप्यूटर के बीच सूचना के आदान-प्रदान का एक तरीका है। जानकारी अनिवार्य रूप से दस्तावेज और अन्य वेब संसाधन हैं जो

हाइपरटेक्स्ट के माध्यम से जुड़े हुए हैं और यू.आर.एल. (यूनिफॉर्म रिसोर्स लोकेटर) द्वारा पहचाने जाते हैं; जिस पर हम आगामी अनुभागों में चर्चा करेंगे। डब्ल्यू. डब्ल्यू. डब्ल्यू या वेब के इन संसाधनों को पहले एच. टी. टी. पी. के माध्यम से स्थानांतरित किया जाता है और फिर उपयोगकर्ताओं द्वारा उन वेब ब्राउजर के माध्यम से एक्सेस किया जा सकता है, जिनके बारे में हमने पहले ही ऊपर चर्चा की थी। वेब पेज हाइपरटेक्स्ट मार्कअप लैंग्वेज (एच.टी.एम.एल.) में विकृत होते हैं जिनमें यू.आर.एल. युक्त हाइपरलिंक होते हैं जो उपयोगकर्ताओं को अन्य वेब संसाधनों पर नेविगेट करने में मदद करते हैं। वेब पेज वेब ब्राउजर में प्रदर्शित होते हैं और उनमें टेक्स्ट, चित्र, वीडियो, ऑडियो और सॉफ्टवेयर घटकों के संदर्भ होते हैं।

यदि किसी सामान्य विषय या डोमेन नाम का उपयोग करने वाले कई वेब संसाधन हैं, तो उन्हें उन वेबसाइटों के रूप में कहा जाता है, जो एक वेब सर्वर नामक प्रोग्राम चलाने वाले कंप्यूटरों में संग्रहीत हैं। यह हर अनुरोध का जवाब देता है जो वेब ब्राउजर से इंटरनेट पर उपयोगकर्ताओं द्वारा बनाए जाते हैं। इन वेबसाइटों की सामग्री प्रकाशक के आधार पर भिन्न हो सकती है जो सामग्री के लिए जिम्मेदार हैं। उपयोगकर्ताओं की आवश्यकताओं के आधार पर विभिन्न वेबसाइटों को अलग-अलग ऑडियंस के लिए लक्षित किया जाता है। सूचना के इस युग में, जिसमें हम रह रहे हैं, विभिन्न वेबसाइटों के माध्यम से सूचनाओं तक पहुँचने के लिए दुनिया भर में अरबों लोग डब्ल्यू. डब्ल्यू. डब्ल्यू का उपयोग करते हैं, इंटरनेट इसके विकास का केंद्र है।

7.7 यू. आर. एल. (URL) (यूनिफॉर्म रिसोर्स लोकेटर)

जैसा कि वेब संसाधनों के ऊपर चर्चा की गई है, यू.आर.एल. द्वारा पहचाने जाते हैं। तकनीकी रूप से URL या वेब पता इंटरनेट पर किसी विशेष संसाधन का एक पता है।



Source: www.ignou.ac.in

चित्र 7.3: इग्नू का यू.आर. एल

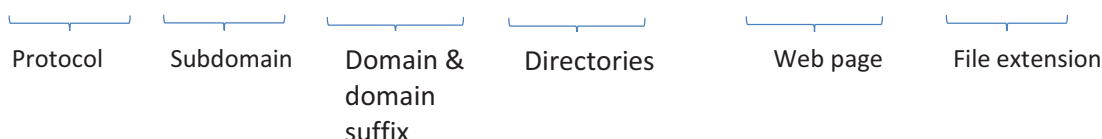
अब हमारा पिछला उदाहरण लेते हैं: [//www.ignou.ac.in](http://www.ignou.ac.in), इग्नू द्वारा जनता के लिए उपलब्ध संसाधनों तक पहुँचने के लिए एक यू.आर.एल है। यू.आर.एल. में तीन तत्व हैं:

- प्रोटोकॉल बनाना

- सर्वर नाम या होस्ट नाम
- निर्देशिका या फाइल के लिए पथ

आइए कुछ संशोधन के साथ हमारे उपरोक्त उदाहरण को लेते हैं, यदि आप नीचे दिए गए URL <http://www.ignou.ac.in/userfiles/ContactUs&2019-pdf> पर क्लिक करेंगे, तो यह आपको इग्नू के महत्वपूर्ण संपर्क विवरणों तक ले जाएगा, जो एक पीडीएफ फाइल है। आइए अधिक स्पष्टता के लिए यू.आर.एल. को क्लिक करें।

<http://www.ignou.ac.in/userfiles/ContactUs-2019.pdf>



चित्र 7.4: वेबसाइट सब पेज

आइए एक-एक करके प्रत्येक तत्व पर चर्चा करें।

- <http://> - "Http" हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल के लिए है, जो सूचना को एक्सेस करने के लिए ब्राउजर द्वारा उपयोग किए जाने वाले प्रोटोकॉल को बताता है। यदि प्रेषित जानकारी एन्क्रिप्ट और सुरक्षित है, तो इसे "https" कहा जाता है, जहां S का अर्थ Secure सुरक्षित है। हमें बृहदान्त्र (:) और दो फॉरवर्ड स्लैश (//) डालने की आवश्यकता है जो कि URL के शेष भाग से प्रोटोकॉल को अलग करते हैं।
- इसके बाद, "डब्ल्यू डब्ल्यू डब्ल्यू" का मतलब वर्ल्ड वाइड वेब है, जिसके बारे में हमने पहले ही उपरोक्त खंड में विस्तार से चर्चा की है। यह भाग वैकल्पिक है और इसे छोड़ा जा सकता है। ऊपर दिए गए उदाहरण में <http://ignou.ac.in> टाइप करना आपको इग्नू की वेबसाइट पर ले जाएगा।
- "Ignou.ac.in" वेबसाइट का डोमेन नाम है। डोमेन के अनुगामी भाग को डोमेन प्रत्यय भी कहा जाता है। यह वेबसाइट के प्रकार या स्थान की पहचान करने में मदद करता है। उदाहरण के लिए, ac.in डोमेन भारत के शैक्षिक संगठन द्वारा उपयोग किया जाता है, ".com" वाणिज्यिक के लिए है, ".org" एक संगठन के लिए है, और ".co.uk" यूनाइटेड किंगडम के लिए है। हम अंतिम खंड में विस्तार से डोमेन के बारे में पढ़ेंगे।
- ["/ userfiles"](http://userfiles/) उपरोक्त URL का यह भाग निर्देशिकाएं हैं, जहां वेबपेज सर्वर पर स्थित है। वेब पेज दो या अधिक निर्देशिकाओं से घिरे हो सकते हैं। हमारे उदाहरण में, यह एक गहरा स्तर है।
- ["/ContactUs-2019.pdf"](http://ContactUs-2019.pdf) अंत में यह दिए गए डोमेन पर वास्तविक वेब पेज है, जिसे हम देख रहे हैं। ट्रेलिंग .pdf फाइल एक्सटेंशन है जो इंगित करता है कि वेब पेज फाइल एक पीडीएफ फाइल है। कई अन्य एक्सटेंशन हैं जैसे कि .jpg, .gif, .php, .xml, .html आदि।

7.8 डोमेन नाम

डोमेन नाम यू.आर.एल (URL) का हिस्सा हैं, जो विशिष्ट वेब पृष्ठों की पहचान करने में मदद करता है। जैसा कि हमारे उदाहरण में चर्चा की गई है “ignou.ac.in” डोमेन नाम था। डोमेन नाम के अनिवार्य रूप से दो भाग हैं:

- वेबसाइट का नाम – हमारे मामले में इग्नू वेबसाइट का नाम है। अगर हम “facebook.com” का उपयोग कर रहे हैं, तो फेसबुक वेबसाइट का नाम है।
- डोमेन प्रत्यय – डोमेन के अनुगामी भाग या विस्तार को डोमेन प्रत्यय कहा जाता है, जो कि जिस वेबसाइट को हम देख रहे हैं उसके लिए पहचानकर्ता की तरह है, संगठन के प्रकार या संगठन के स्थान की पहचान करने में मदद करता है। यह इंगित करता है कि वे किस टी.एल.डी. (TLD) (टॉप-डोमेन) से संबंधित हैं।

डोमेन नाम का उपयोग उस सर्वर के शॉर्टकट के रूप में किया जाता है, जो वेबसाइट को होस्ट कर रहा है। एक डोमेन नाम की अनुपस्थिति में, हमें पूर्ण भौतिक पता दर्ज करना होगा जिसे वेबसाइट के लिए आईपी पता भी कहा जाता है, जिस पर हम काम कर रहे हैं। आईपी पते के साथ समस्या यह है कि उन्हें याद रखना मुश्किल है। Ignou-ac-in के हमारे उदाहरण में, बता दें कि यह एक आईपी एड्रेस 192.90.80.70 की ओर इशारा करता है। अन्य वेबसाइटों के लिए समान आईपी पते होंगे और जैसा कि आप देख सकते हैं कि यह समय लेने वाली और भ्रमित करने वाली हो सकती है। इसलिए, इग्नू सहित अधिकांश वेबसाइट के मालिक एक सेवा का उपयोग करने का विकल्प चुनते हैं जो वेब होस्टिंग पैकेज के साथ बंडल डोमेन नाम प्रदान करता है। हर वेब सर्वर को डोमेन नेम को आईपी एड्रेस में ट्रांसलेट करने के लिए एक डोमेन नेम सिस्टम (डीएनएस) सर्वर की आवश्यकता होती है, क्योंकि इंटरनेट आईपी एड्रेस पर आधारित होता है।

विभिन्न प्रकार के डोमेन

सबसे सामान्य प्रकार का डोमेन टी.एल.डी. है। शीर्ष स्तर का डोमेन इंटरनेट के डोमेन नाम के शीर्ष स्तर पर है।

- सी.सी.टी.एल.डी. (ccTLD) – देश कोड शीर्ष स्तर डोमेन देश के लिए कोड का उपयोग करता है। कोड देश के आधार पर दो अक्षर हैं, जैसे संयुक्त राज्य के लिए .uk, भारत के लिए .in, संयुक्त राज्य अमेरिका के लिए .us। वे उपयोगकर्ताओं को उन क्षेत्रों की पहचान करने में मदद करते हैं जिनमें वेबसाइट संचालित हो रही है।
- जी.टी.एल.डी. (gTLD) – एक सामान्य शीर्ष स्तर डोमेन डोमेन का प्रकार है जो विशिष्ट उपयोग के मामले के लिए अभिप्रेत है और किसी भी देश कोड पर निर्भर नहीं करता है। वहाँ हजार से अधिक जीटीएलडी (gTLD) उपलब्ध हैं, लेकिन व्यावसायिक व्यवसाय के लिए .com, संगठनों के लिए .org, नेटवर्क के लिए .net और शैक्षिक संस्थानों के लिए .edu सबसे आम हैं।

टी.एल.डी. के ठीक नीचे स्थित डोमेन दूसरे स्तर के डोमेन हैं। .Com.पद के बजाय .com.पद का उपयोग करने वाली भारतीय कंपनियाँ .ac.in का उपयोग कर रही हैं, ये दूसरे स्तर के डोमेन के आदर्श उदाहरण हैं।

बोध प्रश्न ख

1) यू.आर.एल. के विभिन्न भाग क्या हैं?

.....

.....

.....

.....

2) वर्ल्ड वाइड वेब क्या है?

.....

.....

.....

.....

3) रिक्त स्थान भरें:

- i) वर्ल्ड वाइड वेब द्वारा बनाया गया था।
- ii) प्रत्येक वेब सर्वर को आईपी पते में डोमेन नाम का अनुवाद करने के लिए
..... सर्वर की आवश्यकता होती है।
- iii) यदि एक सामान्य विषय या डोमेन नाम का उपयोग करते हुए कई वेब संसाधन हैं, तो उन्हें के रूप में कहा जाता है।
- iv) वेब संसाधनों की पहचान से होती है।

7.9 सारांश

इंटरनेट सूचना के आदान-प्रदान के लिए भौतिक रूप से जुड़े उपकरणों का वैश्विक नेटवर्क है। इसे 'नेटवर्कों के नेटवर्क' के रूप में संदर्भित किया जा सकता है, जिसमें नेटवर्किंग तकनीक से जुड़े लाखों इंटरकनेक्टेड डिवाइस शामिल हैं। इंटरनेट से संचार, मे आसानी, ई-कॉमर्स, चौबीसों घंटे उपलब्धता आदि लाभ हैं।

ई-मेल (इलेक्ट्रॉनिक मेल) इंटरनेट द्वारा प्रदान की जाने वाली सबसे लोकप्रिय सेवा है। ई-मेल मूल रूप से दुनिया भर के लोगों के बीच इलेक्ट्रॉनिक संदेश संचार है। आई.एम.ए.पी. (IMAP) का उपयोग केवल ईमेल प्राप्त करते समय किया जाता है और उनका उपयोग ईमेल भेजने के लिए नहीं किया जा सकता है। ईमेल सर्वर में मौजूद होंगे और उपयोगकर्ता के डिवाइस पर डाउनलोड नहीं किए जाएंगे और उन्हें संपादित किया जा सकता है, जैसे कि वे उपयोगकर्ता के डिवाइस पर हैं। जबकि, आई.एम.ए.पी. (IMAP) के विपरीत; POP पूरे ईमेल को स्थानीय उपयोगकर्ता डिवाइस में डाउनलोड करता है। उपयोगकर्ता सिस्टम पर मेल डाउनलोड हो जाने के बाद, यह सर्वर पर डेटा को हटा देगा जो Less free memory वाले सर्वर में काफी मददगार होता है।

वेब ब्राउजर एक के कंप्यूटर में स्थापित कंप्यूटर सॉफ्टवेयर एप्लीकेशन है, जिसका उपयोग इंटरनेट पर वेब पेज देखने के लिए किया जाता है। लोकप्रिय वेब ब्राउजर में से कुछ गूगल क्रोम, ओपेरा मिनी, ऐप्पल सफारी, मोजिला, फायरफॉक्स आदि हैं।

वर्ल्ड वाइड वेब केवल इंटरनेट पर कंप्यूटर के बीच सूचना के आदान-प्रदान का एक तरीका है। जानकारी अनिवार्य रूप से दस्तावेज और अन्य वेब संसाधन हैं जो हाइपरटेक्स्ट के माध्यम से जुड़े हुए हैं और यू.आर.एल. (URL) (यूनिफॉर्म रिसोर्स लोकेटर) द्वारा पहचाने जाते हैं। यू.आर.एल. (URL) या वेब एड्रेस इंटरनेट पर किसी विशेष संसाधन का एक पता है। सामान्य नाम यू.आर.एल. (URL) का हिस्सा है जो विशिष्ट वेब पेज की पहचान करने में मदद करता है। विशिष्ट वेब पेज डोमेन नाम का उपयोग उस सर्वर के शॉर्टकट के रूप में किया जाता है जो वेबसाइट को होस्ट कर रहा है। एक डोमेन नाम की अनुपस्थिति में, हमें पूर्ण भौतिक पता दर्ज करना होगा जिसे वेबसाइट के लिए आईपी पता भी कहा जाता है, जैसा कि हम देख रहे हैं।

7.10 शब्दावली

इंटरनेट (Internet) : इंटरनेट सूचना के आदान-प्रदान के लिए भौतिक रूप से जुड़े उपकरणों का वैश्विक नेटवर्क है। यह वैश्विक रूप से लाखों कंप्यूटरों को एक साथ जोड़ता है, एक ऐसा नेटवर्क बनाता है जिसमें कोई भी कंप्यूटर किसी भी अन्य कंप्यूटर के साथ संचार कर सकता है जब तक कि वे दोनों इंटरनेट से जुड़े हों।

प्रोटोकॉल (Protocol): एक प्रोटोकॉल नियमों का एक मानक समूह है जो इलेक्ट्रॉनिक उपकरणों को एक दूसरे के साथ संवाद करने की अनुमति देता है। इन नियमों में किस प्रकार के डेटा को प्रेषित किया जा सकता है, डेटा भेजने और प्राप्त करने के लिए कौन सी कमांड का उपयोग किया जाता है, और डेटा ट्रांसफर की पुष्टि कैसे की जाती है शामिल है।

ई-मेल या इलेक्ट्रॉनिक मेल (E-mail or electronic mail) : यह इंटरनेट द्वारा प्रदान की जाने वाली सबसे लोकप्रिय सेवाओं में से एक है जहाँ हम दुनिया में कहीं भी बैठे लोगों से इंटरनेट पर सेकंड में संदेश भेज सकते हैं या प्राप्त कर सकते हैं।

वेब ब्राउजर (Web browsers) : वेब ब्राउजर वर्ल्ड वाइड वेब पर सूचना तक पहुंचने के लिए एक सॉफ्टवेयर एप्लीकेशन है। जब कोई उपयोगकर्ता किसी विशेष वेबसाइट का अनुरोध करता है, तो वेब ब्राउजर वेब सर्वर से आवश्यक सामग्री प्राप्त करता है और फिर उपयोगकर्ता के डिवाइस पर परिणामी वेब पेज प्रदर्शित करता है।

यूआरएल या वेब पता (URL or web address) : एक समान संसाधन लोकेटर यू.आर.एल. (URL) इंटरनेट पर एक संसाधन का पता है। एक यू.आर.एल. (URL) संसाधन के स्थान के साथ-साथ उस तक पहुंचने के लिए उपयोग किए गए प्रोटोकॉल को भी इंगित करता है। यह इंटरनेट पर किसी विशेष संसाधन का एक पता है

डोमेन नाम (Domain Name) : डोमेन नाम यू.आर.एल. (URL) का हिस्सा है जो विशिष्ट वेब पृष्ठों की पहचान करने में मदद करता है। डोमेन नाम का उपयोग उस सर्वर के शॉर्टकट के रूप में किया जाता है जो वेबसाइट को होस्ट कर रहा है।

7.11 बोध प्रश्नों के उत्तर

बोध प्रश्न क

उत्तर: 3

- i) चैट रूम
- ii) पैकेट रूटिंग नेटवर्क
- iii) फाइल ट्रांसफर प्रोटोकॉल (एफ.टी.पी.)
- iv) इंटरनेट

बोध प्रश्न ख

- i) सफारी
- ii) एफ.टी.पी.
- iii) गूगल क्रोम
- iv) पोस्ट ऑफिस प्रोटोकॉल

बोध प्रश्न ग

- i) टिमोथी बर्नर्स ली
- ii) डोमेन नेम सिस्टम (DNS)
- iii) वेबसाइट्स
- iv) यू.आर.एल.

7.12 स्वपरख प्रश्न

- 1) निम्नलिखित पर संक्षिप्त नोट लिखें:
 - i) वर्ल्ड वाइड वेब
 - ii) डोमेन नाम
 - iii) यू.आर.एल. (यूनिफॉर्म रिसोर्स लोकेटर)
 - iv) वेब ब्राउजर्स
- 2) निम्नलिखित में अंतर करें:
 - i) आई.एम.ए.पी. और पी.ओ.पी. (POP3)
 - ii) ccTLD और gLTD
- 3) यू.आर.एल. के विभिन्न घटकों का अर्थ स्पष्ट करें।
- 4) इंटरनेट इस्तेमाल करने के फायदे बताएं।
- 5) क्या आपको आई.एम.ए.पी. और पी.ओ.पी. (POP3) का उपयोग करना चाहिए?

नोट: ये प्रश्न आपके अभ्यास के लिए हैं। इनके उत्तर लिखने का अभ्यास करें किंतु उत्तरों को विश्वविद्यालय में मूल्यांकन के लिए न भेजें। प्रश्नों के उत्तर लिखकर आप स्वयं अपनी प्रगति की जाँच कर सकते हैं।

इकाई 8 प्लास्टिक मुद्रा, ई-वॉलेट और ऑनलाइन भुगतान

इकाई की रूपरेखा

- 8.0 उद्देश्य
- 8.1 प्रस्तावना
- 8.2 प्लास्टिक मुद्रा की उत्पत्ति
- 8.3 प्लास्टिक मुद्रा का उपयोग
- 8.4 ई-वॉलेट
- 8.5 ई-वॉलेट प्रणाली का विकास
- 8.6 वाणिज्य में ई-भुगतान प्रणाली
- 8.7 मोबाइल वॉलेट— भुगतान और कार्ड नेटवर्क
- 8.8 मोबाइल वॉलेट में उपभोक्ता का अधिग्रहण
- 8.9 डिजिटल भुगतान पर विमुद्रीकरण के प्रभाव
- 8.10 वॉलेट की सफलता की कहानी, गूगल पे
- 8.11 सारांश
- 8.12 शब्दावली
- 8.13 बोध प्रश्नों के उत्तर
- 8.14 स्वपरख प्रश्न

8.0 उद्देश्य

इस इकाई को पढ़ने के बाद आप इस योग्य हो सकेंगे कि;

- वाणिज्यिक गतिविधियों में उपयोग किए जाने वाले आभासी भुगतान के विभिन्न तरीकों को पहचान सकें;
- डिजिटल भुगतान प्रणाली का विकास समझ सकें;
- वाणिज्यिक लेनदेन में प्रयुक्त विभिन्न प्रकार के ई-भुगतान प्रणाली को समझ सकें; और
- समझ सकें कि भारत में डिमोनेटाइजेशन ने डिजिटल भुगतान प्रणाली को कैसे प्रभावित किया है।

8.1 प्रस्तावना

पिछली इकाई में, हमने व्यापार में आईटी सुरक्षा उपायों की अवधारणा और अनुप्रयोग पर चर्चा की है। इन आईटी सुरक्षा उपायों ने ऑनलाइन लेनदेन को पहले की तुलना में कहीं अधिक सुरक्षित बना दिया है, जिसके परिणामस्वरूप उपभोक्ता विश्वास में सुधार हुआ है। इसके कारण डिजिटल भुगतान प्रणाली को बढ़ाया गया है। यह इकाई डिजिटल भुगतान प्रणाली के विविध पहलुओं को कवर करेगी।

सूचना प्रौद्योगिकी के विकास और तकनीकी नवाचारों के उभार ने धन का विकास किया है। पहला, पेपर मुद्रा से लेकर प्लास्टिक मुद्रा तक। प्लास्टिक मुद्रा में क्रेडिट कार्ड, डेबिट कार्ड, एटीएम, प्रीपेड कार्ड आदि शामिल हैं और हाल ही में इलेक्ट्रॉनिक या डिजिटल रूप में। दोनों ने पैसे के आवश्यक रूपों को तैयार किया जिससे नकदी को संभालने का जोखिम कम हो गया। वे लेनदेन को आसान और सस्ता बनाने वाली अर्थव्यवस्था में नकदी की भूमिका को चुनौती दे रहे हैं। इसी समय, वे एक अर्थव्यवस्था की मुद्रा आपूर्ति को भी प्रभावित करते हैं और इस प्रकार देश के केंद्रीय बैंकों के लिए कई नीतिगत मुद्दे उठाते हैं।

यह इकाई प्लास्टिक मुद्रा और डिजिटल वॉलेट की उत्पत्ति, अर्थव्यवस्था में उनके उपयोग और भूमिका को समझने में मदद करेगी – विशेष रूप से भारतीय अर्थव्यवस्था के संदर्भ में। हम भुगतान के विचलन, विमुद्रीकरण और डिजिटल वॉलेट पर विमुद्रीकरण के प्रभावों पर सरकार की भूमिका को भी समझने की कोशिश करेंगे।

8.2 प्लास्टिक मुद्रा की उत्पत्ति

प्लास्टिक मुद्रा ने इसका नाम “प्लास्टिक” रखा, जिसका उपयोग कागज और धातु की मुद्रा के विपरीत कार्ड के निर्माण में किया जाता है। भारत में प्लास्टिक कार्ड का बाजार, जिसमें क्रेडिट कार्ड, स्मार्ट कार्ड, डेबिट कार्ड, चार्ज कार्ड, संग्रहीत मूल्य कार्ड और अन्य शामिल हैं, केवल पिछले दशक में ही अधिक से अधिक लोकप्रिय हो गए हैं। कई भारतीय बैंकों ने पिछले कुछ वर्षों के दौरान प्लास्टिक कार्ड व्यवसाय में प्रवेश किया है; प्रीमियर बैंक राहित स्टेट बैंक ऑफ इंडिया।

व्यापार की उत्पत्ति मानव समाज के विकास के लिए दिनांकित की जा सकती है। व्यापार वस्तुओं और सेवाओं के प्रत्यक्ष आदान-प्रदान के साथ किया जाता था जिसे लोकप्रिय रूप से “वस्तु विनिमय प्रणाली” के रूप में जाना जाता था। बार्टर प्रणाली कई बाधाओं से ग्रस्त था, जिसमें सबसे महत्वपूर्ण था इसमें शामिल पक्षों के साथ वांछित वस्तुओं की अनुपलब्धता। समय बीतने के साथ, वस्तु विनिमय प्रणाली में आई ये असुविधाएँ गंभीर और असहनीय हो गईं। वस्तु विनिमय समस्या के समाधान की खोज करने से मुद्रा का विकास होता है। पैसा मानव जाति का सबसे महत्वपूर्ण और उपयोगी निर्माण (रचना) में से एक है, मानव जाति जिसने सामाजिक अर्थव्यवस्था के विकास में महत्वपूर्ण भूमिका निभाई। यह ठीक ही कहा गया है कि पैसा वह है जो पैसा करता है (वॉकर)। कुछ भी जो पैसे के कार्यों को करता है, वह पैसा है। यह आर्थिक प्रणाली में एक महत्वपूर्ण भूमिका निभाता है।

ऐसा कहा जाता है कि प्राचीन मेसोपोटामिया में, मंदिरों और शाही महलों में अनाज और अन्य वस्तुओं को सुरक्षित रखने के लिए सुरक्षित स्थान थे, जिससे बैंकिंग प्रणाली की उत्पत्ति हुई। जैसे-जैसे समाज सभ्यता के पैमाने पर बढ़ता गया, आर्थिक प्रणालियों के विकास के साथ बैंकिंग में विकास भी अनिवार्य होता गया। बैंकिंग प्रणाली बढ़ने के साथ, मुद्रा की भूमिका लगभग 17 वीं शताब्दी में कागजी धन के विकास के साथ और अधिक महत्वपूर्ण हो गई, जिसके बाद 19 वीं शताब्दी के अंत में चेक आए। 1920 के दशक में, यूएसए में “अभी खरीदें, बाद में भुगतान करें” एक शॉपर्स प्लेट द्वारा पेश किया गया था। इसे कार्ड पर स्ट्रिप्स के पहले उपयोग के रूप

में पहचाना जाता है। हालाँकि, ये कार्ड केवल जारी करने वाली दुकानों में उपयोग किए जा सकते हैं। प्लास्टिक मुद्रा की शुरुआत का पता 1946 से लगाया जा सकता है, जब जॉन बिगिन्स, ब्रुकलिन के प्लैटबश नेशनल बैंक के एक अंतिम उपयोगकर्ता विशेषज्ञ, एनवाई ने “चार्ज-इट” क्रेडिट योजना शुरू की। योजना में एक प्रकार का लाभांश था, जिसे स्थानीय व्यापारियों द्वारा छोटी खरीद के लिए स्वीकार किया गया था। बिक्री के पूरा होने के बाद व्यापारी को अपने बैंक खाते में राशि जमा करने की आवश्यकता होती है और ग्राहक को बैंक द्वारा कुल जारी किए गए लाभांश के लिए बिल भेजा जाता है। 1951 में न्यूयॉर्क में डिनर क्लब ने 200 ग्राहकों को चार्ज कार्ड जारी किए, जिनका उपयोग 27 निर्दिष्ट रेस्तरां में किया जा सकता था। यह तब तक जारी रखा गया था जब तक कि मैग्नेटिक स्ट्रिप्स के लिए मानकों को 1970 में स्थापित नहीं किया गया था। 1951 में, न्यूयॉर्क में फ्रैंकलिन नेशनल बैंक ने पहला आधुनिक प्लास्टिक मुद्रा जारी किया। इसे 1958 में अमेरिकन एक्सप्रेस द्वारा कार्ड लॉन्च करने के साथ 50 और 60 के दशक के दौरान कई बैंकों द्वारा कॉपी किया गया था। हालाँकि, उस समय तक सभी कार्डधारक केवल अपने भौगोलिक क्षेत्र में खरीदारी कर सकते थे। केवल व्यापारी अपने बैंक के साथ साइन अप करने में सक्षम थे। बैंक ऑफ अमेरिका द्वारा इस समस्या को हल किया गया, जब बैंक ऑफ अमेरिका ने अन्य बैंकों के साथ लाइसेंसिंग समझौता करना शुरू किया। बैंक अमेरिकन्स जारी किया गया था, जिसने 1965 में भाग लेने वाले बैंकों के बीच लेन-देन के आदान-प्रदान की सुविधा प्रदान की, जिसने 1976 में अपना नाम बदलकर वीजा (VISA) कर लिया। 1966 में, बैंक अमेरिका कार्यक्रम के साथ प्रतिस्पर्धा करने के लिए, चार कैलिफोर्निया बैंकिंग संस्थानों ने “वेस्टर्न स्टेट्स बैंककार्ड एसोसिएशन” का गठन किया और लाए। मास्टर चार्ज कार्यक्रम, जो अंततः 1979 में मास्टर कार्ड में बदल गया। ये दो अंतर्राष्ट्रीय कार्ड बहुत लोकप्रिय हैं और दुनिया भर में स्वीकार किए जाते हैं और सम्मानित किए जाते हैं। 1989 में, वीजा द्वारा डेबिट कार्ड पेश किए गए, जहाँ कार्ड ग्राहकों के खातों से जुड़े थे। आज, प्लास्टिक मुद्रा लेनदेन तेजी से नकद लेनदेन की जगह ले रहा है और दुनिया भर में व्यापक रूप से उपयोग किया जाता है।

8.3 प्लास्टिक मुद्रा का उपयोग

पिछले भाग में हमने चर्चा की है कि प्लास्टिक मुद्रा कैसे अस्तित्व में आई। अब हम इसके उपयोग पर गहराई से विचार करेंगे। क्रेडिट कार्ड और डेबिट कार्ड दुनिया भर में लोगों द्वारा उपयोग किए जाने वाले प्लास्टिक मुद्रा के दो सबसे लोकप्रिय रूप हैं। कुछ अन्य लोकप्रिय प्लास्टिक कार्ड्स – स्टोर वैल्यू कार्ड, एटीएम कार्ड, स्मार्ट कार्ड, प्री-पेड कार्ड, कृषि कार्ड आदि। भंडारण में सुरक्षा, सुरक्षा के साथ-साथ हर जगह इसका उपयोग करने से प्लास्टिक मुद्रा की लोकप्रियता में वृद्धि होती है।

- ऐसे कई स्थान हैं जहाँ कोई भी प्लास्टिक मुद्रा का उपयोग कर सकता है।
- किराने की दुकानों पर किराने का सामान खरीदने के लिए नकदी ले जाने की जरूरत नहीं। भारत में लगभग हर जगह किराने के सामान की दुकानों पर प्लास्टिक मुद्रा स्वीकार की जाती है।

- ईंधन स्टेशन पर, हम आपके वाहनों को ईंधन देने के लिए क्रेडिट या डेबिट कार्ड का उपयोग कर सकते हैं।
- रेस्तरां, होटल में भुगतान के लिए।
- हम अपने डेबिट या क्रेडिट कार्ड का उपयोग करके बस, ट्रेन, फ्लाइट टिकट बुक कर सकते हैं।
- हमारे गैस, मोबाइल, लैंडलाइन, बिजली के बिलों का भुगतान करने के लिए।
- डेबिट कम एटीएम कार्ड का उपयोग एटीएम से पैसे निकालने के लिए किया जा सकता है।
- ई-कॉमर्स वेबसाइटों में वृद्धि के साथ, हम अपनी ऑनलाइन खरीदारी के लिए क्रेडिट, डेबिट का उपयोग कर सकते हैं।
- स्मार्ट कार्ड का उपयोग प्लास्टिक मुद्रा के रूप में किया जा रहा है, जिसका उपयोग बस किराया, मेट्रो किराया जैसी छोटी खरीद के लिए किया जाता है। सबसे लोकप्रिय उदाहरण दिल्ली मेट्रो स्मार्ट कार्ड होगा।
- किसान कृषि कार्ड का उपयोग करते हैं – उदाहरण के लिए भारत में किसान क्रेडिट कार्ड, कृषि और संबद्ध गतिविधियों के तहत उनके ऋण प्रवाह में सुधार के लिए।

हम सैकड़ों उदाहरण रख सकते हैं जहां हम प्लास्टिक मुद्रा का उपयोग करते हैं। अनिवार्य रूप से, यह हमारी अर्थव्यवस्था के हर क्षेत्र में प्रवेश कर चुका है, और इसे सरल बनाने के लिए, नकद द्वारा किए जा सकने वाले सभी लेनदेन प्लास्टिक मुद्रा का उपयोग करके भी किया जा सकता है।

बोध प्रश्न क

1) बड़े पैमाने पर प्लास्टिक मुद्रा को अपनाने में किन कारकों का योगदान है?

2) प्लास्टिक मुद्रा के किसी भी चार उपयोग को सूचीबद्ध करें।

3) रिक्त स्थान भरें:

- i) ने कहा, “पैसा वही है जो पैसा करता है”।
- ii) वस्तुओं और सेवाओं का सीधा आदान-प्रदान प्रणाली में होता है।
- iii) प्लास्टिक मुद्रा की शुरुआत का पता इस वर्ष से लगाया जा सकता है
- iv) बैंकिंग प्रणाली की उत्पत्ति का पता प्राचीन से लगाया जा सकता है।

8.4 ई-वॉलेट

आज की दुनिया में लगभग सभी के पर्स में कैश, क्रेडिट और डेबिट कार्ड और बहुत कुछ होता है। इन सभी वस्तुओं पर नजर रखना काफी बोझिल है। ई-वॉलेट या इलेक्ट्रॉनिक वॉलेट हमें कई कार्डों की जरूरत को खत्म करने में मदद कर सकते हैं, जो उन्हें ले जाने की परेशानियों के बिना नकदी और कार्ड के सभी लाभ प्रदान करते हैं। इसके अतिरिक्त, इसमें सिक्योरिटी फीचर्स भी दिए गए हैं जो नियमित वॉलेट्स के साथ उपलब्ध नहीं हैं।

ई-वॉलेट या इलेक्ट्रॉनिक वॉलेट एक प्रकार का इलेक्ट्रॉनिक कार्ड होता है, जिसमें व्यक्ति बचत खातों के समान पैसा स्टॉक कर सकता है (बिना ब्याज के पैसे बचाए जाते हैं) और जिसका उपयोग कंप्यूटर या स्मार्टफोन द्वारा डिजिटल लेनदेन को सक्षम बनाने के लिए किया जाता है। यह एक प्रीलोडेड सुविधा है और क्रेडिट या डेबिट कार्ड की तरह ही कार्यक्षमता प्रदान करता है। उपभोक्ता किराने से लेकर एयरलाइन टिकट तक कई उत्पाद खरीद सकते हैं।

ई-वॉलेट विशेष रूप से अक्सर ऑनलाइन दुकानदारों के लिए बहुत सुविधाजनक है; ऑनलाइन शॉपिंग के लिए एक सुरक्षित, सुविधाजनक और आसानी से सुलभ उपकरण प्रदान करना। वे व्यक्तिगत और वित्तीय जानकारी भी संग्रहीत करते हैं जैसे कार्ड विवरण, पासवर्ड, पिन आदि। भौतिक वॉलेट के समान, ई-वॉलेट कार्ड में सबसे महत्वपूर्ण व्यक्तिगत जानकारी रखता है। ई-वॉलेट हमारी उपयोगिता और मर्चेंट बिल से संबंधित जानकारी को भी सहेज सकता है, इस प्रकार ग्राहकों को विभिन्न भुगतानों का ट्रैक रखने की अनुमति देता है। भारतीय बाजार में ई-वॉलेट का एक लोकप्रिय उदाहरण पेटीएम है।

उपयोगकर्ताओं को ई-वॉलेट के लिए पंजीकरण करना होगा जो वेब आधारित या ऐप आधारित हो सकता है। उनमें से अधिकांश ऐप-आधारित प्रणाली में चले गए हैं, जिन्हें पहले सॉफ्टवेयर की स्थापना की आवश्यकता होती है। एक बार जब उपयोगकर्ता ई-वॉलेट खाता बना लेता है, तो वह ऑनलाइन ट्रांसफर या अपने डेबिट कार्ड/क्रेडिट कार्ड का उपयोग करके वॉलेट में पैसे ट्रांसफर कर सकता है। जब भी वह किसी समर्थित साइट पर वॉलेट का उपयोग करता है तो इस बैलेंस का उपयोग किया जा सकता है। भुगतान में गिरावट की लगभग कोई संभावना नहीं है क्योंकि यह एक प्रीपेड खाता है। उपयोगकर्ता द्वारा प्रदान किए गए भुगतान विवरण जिसमें आमतौर पर उनका नाम, भुगतान विधि, डेबिट या क्रेडिट कार्ड विवरण शामिल होते हैं, अगली बार जल्दी स्थानांतरण के लिए भी बचाया जा सकता है। यह सुविधा

वैकल्पिक है और यदि वह इस जानकारी को संग्रहीत करना चाहता है, तो उपयोगकर्ता पर निर्भर करता है। अगले भाग में हम ई-वॉलेट प्रणाली के विकास के बारे में अधिक जानकारी प्राप्त करेंगे।

8.5 ई-वॉलेट प्रणाली का विकास

पुराने समय से ही वॉलेट का उपयोग किया जाता रहा है। तब से, उन्होंने कई रूप ले लिए हैं लेकिन दो चीजें स्थिर बनी हुई हैं: वे पोर्टेबल हैं और वे हमें मूल्य की वस्तुओं को संग्रहीत करने में मदद करते हैं। शुरुआती दिनों में, वे जानवरों की खाल से बने होते थे, जिन्हें बाद में कपड़े से बदल दिया जाता था, जिन्हें बाद में कई ब्रांडों के विविध आकार और आकारों के आधुनिक पर्स से बदल दिया जाता था। बटुए हमें आसानी से सिक्कों, धन, कार्ड और अन्य कीमती सामानों को रखने और ले जाने में सक्षम बनाते हैं। सूचना और संचार की प्रगति के साथ, प्रौद्योगिकी ने हमारे पर्स को बदलने में बहुत मदद की, जिसमें मुद्रा नोटों को धीरे-धीरे प्लास्टिक के पैसे से बदल दिया गया। एटीएम में लंबी लाइनें, से प्लास्टिक मुद्रा पारंपरिक धन पर एक सुधार था क्योंकि इसने पारंपरिक धन को चारों ओर ले जाने के खतरों को बहुत कम कर दिया था। फिर भी, यह सभी समस्याओं का अंत नहीं था, एटीएम की अनुपलब्धता, सही ढंग से उपयोग न हो पाने के कारण कार्ड की गुणवत्ता में कमी प्लास्टिक मुद्रा से होने वाली समस्याएं हैं। कुछ समस्याएं प्लास्टिक मुद्रा से ग्रस्त हैं। इसलिए, अगला उचित कदम प्लास्टिक मुद्रा की भौतिक उपस्थिति से स्वतंत्रता प्राप्त करना था। इससे ई-वॉलेट्स का विकास हुआ। इंटरनेट ने इन समस्याओं से बाहर निकलने का एक तरीका प्रदान किया, अब पैसा भौतिक दुनिया के प्रतिबंध के बिना पृथ्वी के चेहरे पर किसी भी स्थान पर हमारे साथ यात्रा कर सकता है। इन इलेक्ट्रॉनिक वॉलेट का विवरण विश्वसनीय सुरक्षित सर्वर में रहता है और इसे किसी भी इंटरनेट सक्षम डिवाइस से एक्सेस किया जा सकता है।

1996 में, डिजिटल वॉलेट के संस्थापक सैम पित्रोदा ने कहा, "एक डिजिटल वॉलेट में एक लिक्विड क्रिस्टल डिस्प्ले शामिल होगा जो एक नियमित प्लास्टिक बैंक कार्ड की तुलना में बहुत बड़ा नहीं होता है, जो अधिमानतः एक स्पर्श-संवेदनशील स्क्रीन और सरल उपयोगकर्ता इंटरफ़ेस है जो उपयोगकर्ता को उसी तरह से डिजिटल वॉलेट के माध्यम से फिलप करता है जिस तरह वह लैडर वॉलेट से फिलप करता है तब से, ई-वॉलेट्स के लिए पीछे मुड़कर नहीं देखा गया है। आज, ई-वॉलेट ई-कॉमर्स के इंजन हैं। व्यापक इंटरनेट एक्सेस, बेहतर बैंड-चौड़ाई और उच्च-प्रदर्शन वाले आईटी सक्षम उपकरणों के साथ, ई-वॉलेट तेजी से ग्राहकों द्वारा अपनाए और स्वीकार किए जा रहे हैं। इसका उपयोग निम्नलिखित में से किसी भी या सभी गतिविधियों के लिए किया जा सकता है:

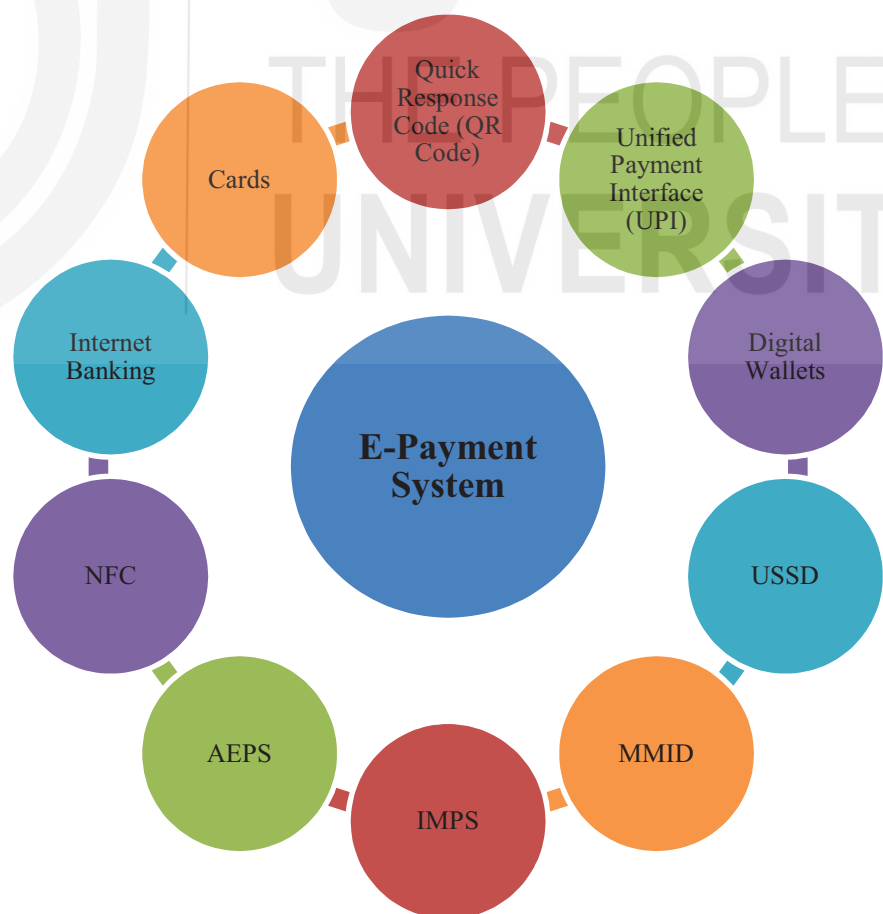
- ऑनलाइन व्यापारी भुगतान
- उपयोगिता भुगतान
- फ्लाइट टिकट खरीद और होटल बुकिंग
- मोबाइल रिचार्ज

- मूवी टिकट बुकिंग आदि।

8.6 वाणिज्य में ई-भुगतान प्रणाली

भुगतान प्रणाली व्यापार और वाणिज्य के समर्थक हैं। इलेक्ट्रॉनिक भुगतान या ई-भुगतान प्रणाली, नकदी या चेक के उपयोग को शामिल किए बिना इलेक्ट्रॉनिक माध्यम से वस्तुओं और सेवाओं के लिए भुगतान को सक्षम करके वाणिज्यिक लेनदेन की सुविधा प्रदान करती है। ई-कॉमर्स और इंटरनेट-बैंकिंग प्रणाली में वृद्धि के साथ, ई-भुगतान प्रणाली पिछले एक दशक में तेजी से बढ़ी है। इस वृद्धि को हाल ही में तकनीकी प्रगति द्वारा समर्थित किया गया है, जिसने न केवल उपयोग में आसानी में सुधार किया, बल्कि हमारी सुरक्षा चिंताओं को दूर करने में भी मदद की।

ई-भुगतान प्रणाली तेजी से पारंपरिक भुगतान प्रणाली की जगह ले रही है। उदाहरण के लिए, यदि हम अपनी खरीद के लिए नकद भुगतान कर रहे हैं; फिर हमें अपने खाते से नकदी निकालनी होगी, इस नकदी का उपयोग करके भुगतान करना होगा, जो कि दिन के अंत में दुकानदार द्वारा उसके खाते में जमा किया जाएगा। इस समय लेने वाली प्रक्रिया को ई-भुगतान प्रणाली के साथ सरल बनाया गया है, जिसमें भुगतान की जाने वाली राशि को सीधे दुकानदार के खाते में स्थानांतरित किया जा सकता है। ई-भुगतान प्रणाली में कई अलग-अलग प्रौद्योगिकियां शामिल हैं। यह खंड उन प्रौद्योगिकियों का अवलोकन प्रदान करता है:



चित्र 8.1 : ई-पेमेंट प्रणाली

- **क्विक रिस्पांस कोड (क्यू.आर. कोड):** एक क्यू.आर. कोड में एन्कोडेड जानकारी होती है, जिसे कोड रीडर / कैमरा के साथ किसी भी डिवाइस के साथ केवल 2 डी मैट्रिक्स बारकोड को स्कैन करके डीकोड किया जा सकता है। जानकारी व्यक्ति को वेबसाइट, ऐप आदि के लिए ले जाती है, जिसके लिए भुगतान करना पड़ता है।
- **यूनिफाइड पेमेंट इंटरफेस (यू.पी.आई.):** UPI मुद्रा ट्रांसफर के लिए वर्चुअल एड्रेस बनाने में सक्षम बनाता है। उपयोगकर्ता को पैसे भेजने या प्राप्त करने के लिए खाता संख्या का खुलासा करने की आवश्यकता नहीं है। सभी बैंकिंग एप्लिकेशन वास्तविक समय पैसे हस्तांतरण को सक्षम करने के लिए यूपीआई (UPI) सुविधा प्रदान करते हैं।
- **डिजिटल वॉलेट:** डिजिटल वॉलेट वर्चुअल वॉलेट हैं, जो ग्राहक को डिजिटल रूप से धन लोड करने में सक्षम बनाते हैं। उपयोगकर्ता अपने क्रेडिट / डेबिट कार्ड का उपयोग करके इन वॉलेट्स में पैसा लोड कर सकता है और इस पैसे का उपयोग व्यापारी को भुगतान करने के लिए किया जा सकता है या किसी अन्य व्यक्ति को हस्तांतरित किया जा सकता है। डिजिटल वॉलेट्स के मामले में एकमात्र बाधा यह है कि फंड को केवल एक ही वॉलेट में स्थानांतरित किया जा सकता है। उदाहरण के लिए, पैसे केवल एक पेटीएम वॉलेट से दूसरे पेटीएम वॉलेट में स्थानांतरित किए जा सकते हैं।
- **अनस्ट्रक्चर्ड सप्लीमेंट्री सर्विस डेटा (यू.एस.एस.डी.):** यूएसएसडी कोड उपयोगकर्ता को स्मार्टफोन या मोबाइल डेटा सुविधा के बिना भी भुगतान करने में सक्षम बनाता है। अपने मूल फोन का उपयोग करके, उपयोगकर्ता * 99 # (सभी दूरसंचार सेवा प्रदाताओं में सामान्य) डायल कर सकते हैं और अपने मोबाइल स्क्रीन पर प्रदर्शित इंटरैक्टिव मेनू का उपयोग कर सकते हैं। इसका उपयोग बैलेंस पूछताछ, फंड ट्रांसफर, मुद्रा स्टेटमेंट आदि जैसी सेवाओं के लिए किया जा सकता है।
- **मोबाइल मुद्रा आइडेंटिफायर (एम.एम.आई.डी.): एमएमआईडी (MMID)** ग्राहकों को बैंकों द्वारा प्रदान किया गया एक अनूठा सात-अंकीय नंबर है, जिन्होंने बैंक के साथ अपना मोबाइल नंबर पंजीकृत किया है। दोनों, उपयोगकर्ता और प्रेषक को (MMID) को उनके बैंकों द्वारा एमएमआईडी (MMID) के माध्यम से लेनदेन के लिए जारी करने की आवश्यकता है। MMID का उपयोग केवल INR 10,000 तक की राशि के हस्तांतरण के लिए किया जा सकता है।
- **आधार सक्षम भुगतान प्रणाली (ए.ई.पी.एस.):** AEPS आधार कार्ड रखने वाले व्यक्तियों की यूनिक आइडेंटिफिकेशन नंबर (UID) पर आधारित है। उपयोगकर्ता PoS या माइक्रो एटीएम में अपने आधार नंबर का उपयोग करके भुगतान कर सकते हैं। यह वित्तीय समावेशन की दिशा में एक महत्वपूर्ण कदम है, क्योंकि इसका उपयोग ग्रामीण क्षेत्रों में भी भुगतान और लेनदेन के लिए किया जा सकता है।

- **नियर फील्ड कम्यूनिकेशन(एनएफसी):** एन.एफ.सी. उपकरणों को बिना संपर्क के संचार करने में सक्षम बनाता है। उपयोगकर्ता केवल पी.ओ.एस. डिवाइस के पास अपना स्मार्टफोन/टैबलेट हिलाकर पेमेंट कर सकता है।
- **बैंकिंग कार्ड:** बैंकिंग कार्ड के कई प्रकार उपलब्ध हैं, अर्थात् डेबिट कार्ड, क्रेडिट कार्ड, प्रीपेड कार्ड, यात्रा कार्ड इत्यादि उपयोगकर्ता इन कार्डों का उपयोग ऑनलाइन और ऑफलाइन भुगतान करने के लिए कर सकते हैं। सुरक्षित भुगतान के लिए, ये कार्ड सुरक्षित पिन या ओटीपी का उपयोग करते हैं। उदाहरण: RuPay, Visa, इत्यादि।
- **इंटरनेट बैंकिंग:** इंटरनेट बैंकिंग एक इलेक्ट्रॉनिक भुगतान प्रणाली है जो उपयोगकर्ताओं को बैंक की वेबसाइट के माध्यम से वित्तीय लेनदेन करने में सक्षम बनाती है। इंटरनेट बैंकिंग लेनदेन के कई अलग-अलग प्रकार हैं:

नैशनल इलेक्ट्रॉनिक फंड ट्रांसफर (एन.ई.एफ.टी.)	रियल टाइम ग्रॉस सेटलमेंट (आर.टी.जी.एस.)	इमीडियेट पेमेंट सर्विस (आई.एम.पी.एस.)
यह किसी भी बैंक के साथ बैंक खाते वाले व्यक्तियों / व्यवसायों को इलेक्ट्रॉनिक रूप से एक से एक फंड ट्रांसफर में सक्षम बनाता है।	आरटीजीएस का उपयोग मुख्य रूप से बड़े मूल्य के लेनदेन (न्यूनतम। INR 2 लाख) के लिए किया जाता है और आरटीजीएस लेनदेन पर कोई ऊपरी कैप नहीं है।	IMPS चौबीसों घंटे इलेक्ट्रॉनिक पैसे के लेनदेन को सक्षम बनाता है। IMPS का उपयोग करके, देश भर में किसी भी बैंक खाते में तुरंत धनराशि स्थानांतरित की जा सकती है।

बोध प्रश्न ख

- 1) ई-वॉलेट की तीन सबसे महत्वपूर्ण विशेषताएं क्या हैं?

.....

.....

.....

.....

- 2) चार ई-भुगतान विधियों की सूची बनाएं।

.....

.....

.....

.....

3) बताएं कि निम्नलिखित कथन सही हैं या गलत।

- i) ई-पर्स के मामले में भुगतान में गिरावट की बहुत अधिक संभावना है।
- ii) एनएफसी उपयोग के लिए, यह अनिवार्य है कि दोनों डिवाइस संपर्क में हों।
- iii) USSD का इस्तेमाल बेसिक फोन पर भी किया जा सकता है।
- iv) IMPS चौबीसों घंटे धन हस्तांतरण में सक्षम बनाता है।
- v) RTGS लेनदेन पर ऊपरी कैप है।

8.7 मोबाइल वॉलेट – भुगतान और कार्ड नेटवर्क

मोबाइल वॉलेट भुगतान सेवाएं प्रदान करते हैं जो कि मोबाइल फोन, टैबलेट, व्यक्तिगत डिजिटल सहायक आदि के माध्यम से किए जा सकते हैं। मोबाइल वॉलेट का विकास और इस अपनाना मोबाइल संचार, मोबाइल इंटरनेट सेवाओं और वायरलेस नेटवर्क सेवाओं में बड़े पैमाने पर विकास का परिणाम है। मोबाइल वॉलेट एक मोबाइल डिवाइस के माध्यम से संचालित होने वाले इलेक्ट्रॉनिक खाते हैं। मोबाइल वॉलेट आर्किटेक्चर में तीन अलग-अलग घटक होते हैं:

- **भुगतान घटक:** भुगतान प्रमाणीकरण और सुरक्षित लेनदेन के लिए
- **यूजर इंटरफेस:** भुगतान सेवाओं के लिए सुविधाजनक पहुँच प्रदान करने के लिए
- **अम्ब्रेला यूआई घटक:** वॉलेट जारी करने वाली कंपनी द्वारा प्रदान किया जाता है, यह मोबाइल उपकरणों पर भुगतान सेवाओं के पोर्टफोलियो का प्रबंधन करता है

जारीकर्ता कंपनी के लिए राजस्व का स्रोत होने के बजाय, मोबाइल वॉलेट व्यावसायिक गतिविधियों के प्रति उत्साही हैं। खुदरा वित्तीय संस्थान अक्सर उच्च स्थान हासिल करने के लिए एक दूसरे के साथ प्रतिस्पर्धा करते हैं ताकि उनके कार्ड का उपयोग पैसे जोड़ने और मोबाइल वॉलेट्स के माध्यम से लेनदेन करने के लिए सबसे अधिक उपयोग किया जाए। वॉलेट जारी करने वाली कंपनी अक्सर वित्तीय संस्थानों से वॉलेट के माध्यम से की गई बिक्री पर कमीशन वसूल कर राजस्व अर्जित करती है। वॉलेट सेवा प्रदाता में से कुछ वित्तीय संस्थानों से कमीशन के साथ बाजार में प्रवेश करने की अनुमति के लिए अग्रिम शुल्क लेते हैं, जबकि कुछ अपने प्लेटफॉर्म पर विज्ञापनों की अनुमति देकर पैसे कमाते हैं।

भारत में दूरसंचार के तेजी से विकास ने उपयोगकर्ताओं को सशक्त बनाया है और संचार लागतों में भारी कमी करके अर्थव्यवस्था की उत्पादकता में सुधार किया है। सस्ते इंटरनेट कनेक्शन और बेहतर गति के साथ घटते सेट के साथ, स्मार्टफोन उपयोगकर्ताओं के दैनिक जीवन को आकार देने के लिए प्राथमिक उपकरण बन रहे हैं, जिससे वे प्रभावित होते हैं कि वे वस्तुओं की खोज कैसे करते हैं, और वे विभिन्न वस्तुओं और सेवाओं के लिए कैसे खरीद और भुगतान करते हैं।

मोबाइल वॉलेट ने डिजिटल भुगतान को अंतिम ग्राहकों के हाथों में ले जाकर डिजिटल भुगतान में बहुत योगदान दिया है। मोबाइल वॉलेट को तीन प्रमुखों के अंतर्गत वर्गीकृत किया जा सकता है, जो वॉलेट संचालित करने, उपलब्ध लेनदेन सीमा और वॉलेट के समग्र उद्देश्य पर निर्भर करता है।

ओपन वॉलेट्स – ये वॉलेट्स बैंकिंग संस्थानों के समर्थन के साथ मौजूद हैं और वे उपयोगकर्ताओं को सीधे वॉलेट से सामान और सेवाओं के लिए भुगतान करने की अनुमति देते हैं। वे उपयोगकर्ताओं को नकदी निकालने की अनुमति भी देते हैं और इसलिए सबसे अधिक लचीले होते हैं। इन वॉलेट्स की सीमा INR 10,000 प्रति माह है। उदाहरण: गूगल पे, गूगल द्वारा पेजेप (PayZapp), एच.डी.एफ.सी. (HDFC) बैंक द्वारा आइ.सी.आई.सी. (ICICI) द्वारा चलान में लाया गया है।

सेमी क्लोज्ड वॉलेट (Semi Closed Wallets) : इन वॉलेट का उपयोग चुनिंदा व्यापारियों को भुगतान करने के लिए किया जा सकता है, लेकिन वे ग्राहकों को नकदी निकालने की अनुमति नहीं देते हैं। इन वॉलेट में से कुछ अपने उपयोगकर्ताओं को सीधे दूसरे वॉलेट में राशि स्थानांतरित करने की अनुमति देते हैं। इन वॉलेट्स की सीमा प्रति माह INR 10,000 है और पूरे वर्ष के लिए 100,000 से अधिक नहीं हो सकती है। उदाहरण: अमेजन पे, पेटीएम, ओला मुद्रा।

क्लोज्ड वॉलेट्स (Closed Wallets) : इस तरह के वॉलेट्स मर्चेन्ट स्पेसिफिक वॉलेट्स होते हैं और इन्हें जारी करने वाले मर्चेन्ट साइट्स पर विशेष रूप से लेनदेन के लिए इस्तेमाल किया जा सकता है। इन वॉलेट में रखी जाने वाली राशि की सीमा INR 10,000 है। क्लोज्ड वॉलेट का उदाहरण मेक माई ट्रिप द्वारा जारी किए गये माई वॉलेट है, 'बिग बास्केट का बिग बास्केट वॉलेट है।

8.8 मोबाइल वॉलेट में उपभोक्ता का अधिग्रहण

जब भी कोई नया उत्पाद बाजार में लॉन्च किया जाता है, तो उत्पाद का दत्तक चक्र उसको अपनाने और स्वीकृति को दर्शाता है। मोबाइल वॉलेट के अपनाने और स्वीकृति में इसके आसानी से इस्तेमाल और लचीलेपन का बहुत योगदान है। अपनाने के चरणों को “रोजर्स के प्रसार के नवाचार” प्रक्रिया की मदद से समझाया जा सकता है। एम. रोजर्स ने एक अभिनव उत्पाद या सेवा को अपनाने के लिए अपनी तत्परता के आधार पर उपयोगकर्ताओं की पांच अलग-अलग श्रेणियों की पहचान की। यही सिद्धांत मोबाइल वॉलेट पर भी लागू होता है जो तेजी से उपभोक्ताओं के दिन प्रतिदिन के जीवन में अपनी जगह बना रहा है।

इनोवेटर्स (Innovators) : वे परिवर्तन और नवाचार के लिए नेता हैं। ऐसे व्यक्ति जो पहले विचारों की कल्पना करते हैं। मुख्य रूप से आयु वर्ग 18–30 में महानगरों में रहने वाली युवा पीढ़ी मोबाइल वॉलेट के मामले में नवप्रवर्तक हैं। वे कैब, डीटीएच, फोन बिल, व्यापारियों को भुगतान आदि जैसी सेवाओं के लिए भुगतान करने के लिए मोबाइल वॉलेट का उपयोग करते हैं। कम्पनियां अपने मोबाइल वॉलेट सेवाओं को निरंतर नये सेवाये प्रदान कर रही है ताकि वे उपभोक्ताओं जोकि नई नई सेवाओं के इंतजार में रहते है उनको बनाये रखने वे दूसरो को और उत्पाद को अपनाने के लिए प्रोत्साहित कर सकते है।

अर्ली एडॉप्टरे (Early Adopters) : ये जिज्ञासु व्यक्ति हैं जो नवीनतम रुझानों के लिए निरंतर खोज पर हैं। वे समान आयु वर्ग के इनोवेटर के रूप में हैं और फीडबैक के आधार पर वे नए उत्पादों की कोशिश करते हैं, यदि उन्हें लगता है कि यह उनके जीवन को आसान बना देगा और पैसा वसूल होगा। वे अन्य डिजिटल भुगतान मोड

और मोबाइल बैंकिंग सेवाओं से भी परिचित हैं। ज्यादातर वे मेट्रो और टियर 2 शहरों से संबंधित हैं। वे केवल तभी आकर्षित होते हैं जब उन्हें लगता है कि ये मोबाइल वॉलेट उपयोग के लिए सुरक्षित हैं और उन्हें अच्छा रिटर्न प्रदान करेंगे।

अर्ली मेजोरिटी (Early Majority) : वे अधिक व्यावहारिक उपयोगकर्ता हैं जो प्रौद्योगिकी में तब तक इंतजार करते हैं जब तक वे गोता लगाने से पहले खुद को साबित नहीं करते हैं। मोबाइल वॉलेट जैसे नए उत्पादों को अपनाते हुए, ये उपयोगकर्ता ऑफर की खोज करते हैं और बहुत ही चुनिंदा सेवाओं पर उनका उपयोग करते हैं। उनकी आदतों के कारण उनके नियमित भुगतान के तरीकों की तुलना में उनका उपयोग बहुत कम होगा। वे अक्सर मोबाइल वॉलेट कंपनियों द्वारा परिचयात्मक प्रचार प्रस्तावों से आकर्षित होते हैं।

लेट मेजोरिटी (Late Majority) : ये ऐसे व्यक्ति हैं जो तकनीक को तभी अपनाएंगे जब यह एक मानक बन जाएगा और इसे टाला नहीं जा सकता। मोबाइल वॉलेट के मामले में, ये उपयोगकर्ता 40–55 वर्ष की आयु वर्ग में हैं। इनमें से अधिकांश उपयोगकर्ता अभी भी मोबाइल वॉलेट से ज्यादा परिचित नहीं हैं और डेबिट कार्ड या ऑनलाइन ट्रांसफर पसंद करते हैं। मोबाइल वॉलेट कंपनियों को इन ग्राहकों को उनके सेवाओं और लाभों के बारे में शिक्षित करने के लिए पारंपरिक तरीकों पर काम करना होगा ताकि उन पर एस्ट्रो का विश्वास बढ़े।

लैगार्ड्स (Leggards) : वे आम तौर पर पुरानी पीढ़ी को अपनाने के लिए होते हैं, जो कभी भी एक नई तकनीक को जानबूझकर नहीं अपनाते हैं। इसमें 55 वर्ष से अधिक आय वाले लोग और जो स्मार्टफोन के इस्तेमाल करने में सहज नहीं हैं शामिल हैं। यह संभव नहीं है कि वे मोबाइल वॉलेट का उपयोग करेंगे क्योंकि उनका पसंदीदा भुगतान नकद है।

भारतीय उपभोक्ता अब केवल मोबाइल वॉलेट के विचार की तरह नहीं हैं बल्कि इसका उपयोग करने में वास्तविक लाभ देखते हैं। बाजार में 39% की मजबूत पैठ के साथ – अकेले पेटीएम के पास 200 मिलियन से अधिक ग्राहक और 5 मिलियन व्यापारी हैं। मूल्य वर्धित सेवाओं जैसे उपयोगिता बिल भुगतान, कैशबैक ऑफर, टिकट बुकिंग आदि के साथ अपने मुख्य उत्पाद की पेशकश को आगे बढ़ाने से अपनाने में मदद मिलती है। एक उत्पाद के रूप में मोबाइल वॉलेट पहले ही खुद को स्थापित कर चुका है और “अर्ली मेजोरिटी” चरण में है। यह देखना आसान है कि मोबाइल वॉलेट अब “अर्ली मेजोरिटी” चरण में हैं। लोग अब मोबाइल वॉलेट के “विचार” की तरह नहीं हैं, लेकिन इसका उपयोग करने में वास्तविक लाभ देखें और इसे तेजी से अपना रहे हैं। मोबाइल वॉलेट अपनाने में मदद करने वाले महत्वपूर्ण कारकों में से एक सरकार की नीति है। ऐसी नीति में से एक विमुद्रीकरण था जिसे हम विवरण में अगले खंड में अध्ययन करेंगे।

8.9 डिजिटल भुगतान पर विमुद्रीकरण के प्रभाव

विमुद्रीकरण “एक कानूनी निविदा के रूप में अपनी स्थिति की मुद्रा इकाई को अलग करने का कार्य” है। दूसरे शब्दों में, यह प्रचलन में मुद्रा के विशेष रूप को वापस लेने

की प्रक्रिया है। भारत सरकार ने निर्भीक रूप से 8 नवंबर, 2016 को नोटबंदी की घोषणा की। किसी भी प्रकार के तरल लेनदेन के लिए ₹ 500 और 1000 के नोटों के प्रचलन पर मध्यरात्रि 9 नवंबर, 2016 से प्रतिबंध लगा दिया गया था। एटीएम निकासी की सीमा ₹ 2500 निर्धारित की गई थी।

विमुद्रीकरण की अप्रत्याशित घोषणा और लंबे समय तक नकदी की कमी ने डिजिटल लेनदेन को बढ़ाने में मदद की। छोटी दुकान से लेकर बड़े मॉल तक की अर्थव्यवस्था के हर क्षेत्र में देश भर में डिजिटल लेनदेन में तेजी देखी गई। विमुद्रीकरण के बाद, कैशलेस भुगतान के तरीकों पर स्विच करना ग्रामीण और शहरी आबादी दोनों के लिए एक आवश्यकता बन जाता है। देश का प्रत्येक नागरिक, चाहे वह किसान हो, शिक्षक हो, सैनिक हो या फिर किसी बड़े ब्रांड का सीईओ हो, को कैशलेस लेनदेन करने के लिए उपलब्ध तरीकों के बारे में जानना होगा। वे मौजूदा सुविधाओं के बारे में अधिक जागरूक हो जाते हैं — कैसे वे इंटरनेट बैंकिंग के माध्यम से ऑनलाइन लेनदेन कर सकते हैं जैसे कि अकाउंट बैलेंस, बिल भुगतान, फंड ट्रांसफर आदि। इसके अलावा, ग्राहक की सुविधा के लिए 24 × 7 उपलब्ध है। छोटे विक्रेताओं ने अपने व्यवसाय को जारी रखने के लिए ई-वॉलेट के तरीकों — पेटीएम, मोबिक्विक आदि को भी शामिल किया है। सभी ने पूरे देश में डिजिटल लेनदेन को एक बड़ा धक्का दिया।

साथ ही, देश में अल्पकालिक नकदी-संकट वाले नागरिकों की मदद करने के लिए, भारत सरकार ने आक्रामक तरीके से बैंकिंग के डिजिटल साधनों को बढ़ावा दिया। कुछ भुगतान तरीकों पर लेनदेन शुल्क माफ कर दिया गया था। पिछले वित्त वर्ष की तुलना में 2016-17 में कुल इलेक्ट्रॉनिक और कार्ड भुगतान मूल्य में 46% और मात्रा में 65% की वृद्धि हुई है। यूनिकाइड पेमेंट्स इंटरफेस (UPI, सरकार की रियल-टाइम भुगतान प्रणाली) और आधार-आधारित भुगतान जैसे कुछ खंड बहुत कम आधार से सबसे तेजी से बढ़े हैं। ऑनलाइन बैंकिंग लेनदेन और डेबिट कार्ड से भुगतान सबसे अधिक हुआ। पेटीएम जैसी ई-वॉलेट कंपनियों ने विमुद्रीकरण के फैसले का स्वागत किया क्योंकि इससे उन्हें अपने ग्राहक आधार को बढ़ाने का मौका मिला। पे.टी.एम. वॉलेट 125 मिलियन वॉलेट ग्राहकों से विमुद्रीकरण से पहले 185 मिलियन तीन महीने बाद चला गया, और यह लगभग 300 मिलियन ग्राहक आधार के साथ बढ़ना जारी रहा है। निष्कर्ष में डिमोनेटाइजेशन ने डिजिटल भुगतान को जोर दिया, जिसके कारण जनता के बीच डिजिटल भुगतान की स्वीकार्यता में वृद्धि के साथ-साथ कई भुगतान वॉलेट कंपनियों को सफलता मिली।

8.10 वॉलेट की सफलता की कहानी, गूगल पे

पहले डिजिटल वॉलेट्स को केवल ई-कॉमर्स भुगतान टूल के रूप में देखा जाता था, लेकिन पोस्ट डिमोनेटाइजेशन जनता ने इसे दिन-प्रतिदिन के उपयोग के लेनदेन के लिए अपनाया। क्या यह किराने की दुकान, स्ट्रीट वेंडर, चाय की दुकान, पेट्रोल पंप और यहां तक कि कैब और ऑटो रिक्शा का भुगतान करने के लिए भी हो। पेटीएम (Paytm), मोबिक्विक (Mobiwik), फोन पे (PhonePay), गूगल (google) पे जैसे वॉलेट्स डिमोनेटाइजेशन की लहर के साथ चलते हैं।

हालांकि, डिजिटल भुगतान में क्रेडिट कार्ड और ऑनलाइन ट्रांसफर सबसे अधिक बाजार हिस्सेदारी रखते हैं। मोबाइल वॉलेट की वृद्धि की कहानी काफी आकर्षक है, विशेष रूप से पोस्ट डिमोनेटाइजेशन।

आजकल, मोबाइल वॉलेट एक मुख्यधारा भुगतान मोड के रूप में विकसित हुए हैं। Global Data द्वारा किए गए सर्वेक्षण में, इस तथ्य पर जोर दिया गया कि ई-कॉमर्स खरीद के लिए भुगतान के पसंदीदा मोड के रूप में कैश ऑन डिलीवरी की हिस्सेदारी 2013 में 31% से घटकर लगभग आधी हो गई है यानी वर्ष 2017 में 16%। इसके अलावा, भुगतान का हिस्सा इस अवधि के दौरान डिजिटल वॉलेट के माध्यम से मात्र 7% से 29% की वृद्धि हुई। साथ ही, इस अवधि में भुगतान करने के लिए कार्ड का उपयोग 38% से घटकर 32% हो गया।

इस तेजी से बढ़ते बाजार का उपयोग करने के लिए गूगल (Google) ने अगस्त, 2017 में तेज (Tez) 'नाम से अपनी मोबाइल भुगतान सेवा शुरू की। यह विशेष रूप से भारतीय ग्राहकों को लक्षित करता है। वास्तव में, 37 दिनों के थोड़े समय के भीतर, ऐप को 85 लाख से अधिक उपकरणों पर इंस्टॉल किया गया था। लगातार बढ़ते भारतीय भुगतान बाजार पर नजर रखने के साथ, गूगल (Google) ने अपने भुगतान ऐप, Google Tez को अगस्त 2018 में गूगल (Google) पे के रूप में फिर से लॉन्च किया, जो वैश्विक स्तर पर उपयोग की जाने वाली भुगतान सेवाओं के अनुरूप है। यह ऐप हिंदी, तेलुगु, मराठी आदि सहित भारत में बोली जाने वाली कई क्षेत्रीय भाषाओं का समर्थन करता है। ऐप यूपीआई आधारित प्लेटफॉर्म का उपयोग करता है और उपयोगकर्ता इसका उपयोग उपयोगिता और व्यापारी भुगतान के साथ-साथ धन हस्तांतरण के लिए भी कर सकते हैं। अब तक, यह 2,000 से अधिक ऐप्स और वेबसाइटों पर भुगतान का समर्थन करता है। गूगल (Google) का दावा है कि हर महीने लेनदेन के लिए 22 मिलियन से अधिक उपयोगकर्ता इस ऐप का उपयोग कर रहे हैं। तेज (Tez), जो एक बैंक लिंकड पेमेंट ऐप के रूप में शुरू हुआ था, ऑफलाइन रिटेल स्टोर्स के साथ-साथ बिग बाजार, ई-जोन आदि में उपलब्ध भुगतान सुविधाओं पर जोर दे रहा है। गूगल (Google) पे भी माइक्रो-लोन सेगमेंट में प्रवेश करने की योजना बना रहा है, जो सक्षम हो जाएगा उपयोगकर्ता को कागज के काम और फोन कॉल की परेशानी से बचने के लिए, यह एक क्लिक पर उनके बैंक खाते में उपलब्ध होगा।

बोध प्रश्न ग

1) मोबाइल वॉलेट के विभिन्न घटक क्या हैं?

.....

.....

.....

2) मोबाइल वॉलेट की तीन अलग-अलग श्रेणियां क्या हैं?

.....

.....

.....

3) रिक्त स्थान भरें:

- i) वॉलेट्स बैंकिंग संस्थानों के समर्थन के साथ मौजूद हैं और वे उपयोगकर्ताओं को सीधे वॉलेट से सामान और सेवाओं के लिए भुगतान करने की अनुमति देते हैं।
- ii) ऐसे व्यक्ति जो तकनीक को तभी अपनाएंगे जब यह एक आदर्श बन जाएगा और इसे टाला नहीं जा सकता।
- iii) नवाचार के प्रसार की प्रक्रिया के अनुसार, मोबाइल वॉलेट अब चरण में हैं।
- iv) “एक कानूनी निविदा के रूप में अपनी स्थिति की मुद्रा इकाई को अलग करने का कार्य”।
- v) Google ने वैश्विक रूप से उपयोग की जाने वाली अपनी भुगतान सेवाओं के अनुरूप Google भुगतान के रूप में अपने भुगतान ऐप, को फिर से लॉन्च किया।

8.11 सारांश

दुनिया कागज के पैसे या नकद से प्लास्टिक के पैसे – क्रेडिट कार्ड, डेबिट कार्ड से आगे बढ़ रही है। हाल ही में दूरसंचार क्रांति के साथ, लोगों को स्मार्टफोन और सस्ते इंटरनेट की सुविधा मिली। इसके कारण पारंपरिक इलेक्ट्रॉनिक भुगतान प्रणाली में ई-वॉलेट या मोबाइल वॉलेट प्रणाली का उत्तराधिकार हुआ है। सरकार के डिजिटल इंडिया कार्यक्रम को आगे बढ़ाने और जागरूकता बढ़ाने के साथ, विशेष रूप से ग्रामीण उपभोक्ताओं के बीच विश्वास का निर्माण किया जा रहा है। इलेक्ट्रॉनिक भुगतान को बढ़ावा देने वाली नीतियां, स्मार्टफोन के प्रवेश में वृद्धि (मोबाइल फोन सदस्यता 2016 में 100 करोड़ का आंकड़ा पार कर गई और अनुमानित 371 मिलियन उपयोगकर्ता अब मोबाइल इंटरनेट पर सब्सक्राइब हो गए हैं), टेलीकॉम और भुगतान बुनियादी ढांचे में सुधार और वॉलेट भुगतान ने प्रचार (promotion) करता है। डिजिटल वॉलेट उपयोगकर्ता के आधार का विस्तार और कायम बनाए रखने में मदद करती है।

8.12 शब्दावली

प्लास्टिक मुद्रा (Plastic Money) : प्लास्टिक या पॉलिमर से बना पैसा मुख्य रूप से सभी प्रकार के कार्डों— क्रेडिट कार्ड, डेबिट कार्ड, प्री-पेड कैश कार्ड और स्टोर कार्ड का उल्लेख करता है।

ई-वॉलेट (E-Wallet) : एक इलेक्ट्रॉनिक वॉलेट जिसका उपयोग इलेक्ट्रॉनिक रूप से या तो डिवाइस – स्मार्टफोन या ऑनलाइन सेवा के माध्यम से लेनदेन करने के लिए किया जाता है। इसे व्यक्ति के बैंक खाते से जोड़ना होगा।

ई-भुगतान प्रणाली (E-Payment System) : इलेक्ट्रॉनिक भुगतान या ई-भुगतान प्रणाली भुगतान की एक इलेक्ट्रॉनिक विधा है, जो नकदी या चेक के उपयोग को

शामिल किए बिना, इलेक्ट्रॉनिक रूप से वस्तुओं और सेवाओं के लिए भुगतान को सक्षम करके लेनदेन की सुविधा प्रदान करती है।

प्लास्टिक मुद्रा,
ई-वॉलेट और
ऑनलाइन भुगतान

मोबाइल वॉलेट (Mobile Wallet) : मोबाइल वॉलेट इलेक्ट्रॉनिक वॉलेट का एक रूप है, जो मोबाइल फोन, टैबलेट, पर्सनल असिस्टेंट आदि जैसे उपकरणों के माध्यम से भुगतान सेवाएं प्रदान करता है।

विमुद्रीकरण (Demonetization) : यह “कानूनी निविदा के रूप में अपनी स्थिति की एक मुद्रा इकाई को अलग करने का कार्य” को संदर्भित करता है। दूसरे शब्दों में, यह प्रचलन में मुद्रा के विशेष रूप को वापस ले रहा है।

8.13 बोध प्रश्नों के उत्तर

बोध प्रश्न क

- i) वॉकर
- ii) वस्तु-विनिमय
- iii) 1946
- iv) मेसोपोटामिया करे

बोध प्रश्न ख

- i) असत्य
- ii) असत्य
- iii) सत्य
- iv). सत्य
- v) असत्य

बोध प्रश्न ग

- i) ऑपन वाइलेट
- ii) देर से ही सही
- iii) प्रथम बहुमत
- iv) डेमोनेटाइजेशन
- v) तेज

8.14 स्वपरख प्रश्न

1) निम्नलिखित पर संक्षिप्त नोट लिखें:

- i) ए.ई.पी.एस. (AEPS)
- ii) क्यू.आर. कोड
- iii) एन.एफ.सी.
- iv) एम.एम.आई.डी.

- 2) निम्नलिखित में अंतर करें:
 - i) ओपन एंड क्लोज्ड वॉलेट
 - ii) एन.ई.एफ.टी और आर.टी.जी.एस
- 3) ई-वॉलेट का अर्थ समझाएं। भारत में ई-वॉलेट को अपनाने में योगदान देने वाले कारकों के बारे में संक्षेप में चर्चा करें।
- 4) ई-वॉलेट पर विमुद्रीकरण के प्रभाव को स्पष्ट करें।
- 5) पारंपरिक भुगतान प्रणाली की तुलना में ई-भुगतान प्रणाली कैसे बेहतर है?

नोट: ये प्रश्न आपके अभ्यास के लिए हैं। इनके उत्तर लिखने का अभ्यास करें किंतु उत्तरों को विश्वविद्यालय में मूल्यांकन के लिए न भेजें। प्रश्नों के उत्तर लिखकर आप स्वयं अपनी प्रगति की जाँच कर सकते हैं।

