International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Volume 01, No. 03, July - September, 2019, pp.115-120

भारत में साइबर सुरक्षा: ई-कॉमर्स के विकास के लिए चुनौती
(Cyber Security in India: A Challenge to Growth of E-Commerce)

प्रियंका छपेरा*

सार

पिछले कुछ वर्षों से ई–कॉमर्स यानी कि इलेक्ट्रॉनिक कॉमर्स अधिक प्रचलन में है। ई–कॉमर्स के माध्यम से वस्तुएँ और सेवाएँ उपभोक्ता को सीधे प्राप्त होती है। इससे मध्यस्थों की भूमिका समाप्त होती ही है, साथ ही सामान भी सस्ता मिलता है। इससे बाजार में भी प्रतिस्पर्द्धा बनी रहती है और ग्राहक बाजार में उपलब्ध सामानों की तुलना भी कर पाता है जिसके कारण ग्राहकों को उच्च गुणवता वाला सामान मिल पाता है। ई–कॉमर्स के द्वारा परिवहन, मेडिकल, रिटेल, बैंकिंग, शिक्षा, मनोरंजन जैसी सुविधाएँ ऑनलाइन होने से लोगों की सुविधाएँ बढ़ी है। इसलिए व्यवसाय की दृष्टि से ई–कॉमर्स दिन–प्रतिदिन महत्वपूर्ण होता जा रहा है। ई–कॉमर्स में साइबर अपराध सामान्य कंप्यूटर कार्यों के रूकावट के लिए जिम्मेदार है और कई कंपनियों और व्यक्तिगत संस्थाओं के पतन का कारण माना जाता है। प्रौद्योगिकी के उपयोग और प्रगति ने विभिन्न प्रकार के अपराधों जैसे चोरी, साइबर अपराध और आतंकवाद को बढ़ाया है।

कुन्जी शब्दः– *ई–कॉमर्स, साइबर सुरक्षा, साइबर अपराध, वायरस, फायरवॉल।*

प्रस्तावना

ई–कॉमर्स या ई–व्यवसाय इंटरनेट के माध्यम से व्यापार का संचालन है, न केवल खरीदना और बेचना, बल्कि ग्राहकों के लिये सेवाएँ और व्यापार के भागीदारों के साथ सहयोग भी इसमें शामिल है। उपभोक्ता और मूल्य वर्धित प्रकार के व्यापारों के लिए इंटरनेट कई अवसर प्रदान करता है। वर्तमान में कंप्यूटर, दूरसंचार और केबल टेलीविजन व्यवसायों में बड़े पैमाने पर विश्वव्यापी परिवर्तन हो रहे हैं। सन् 1990 से वाणिज्यिक उद्यमों ने विज्ञापन, बिक्री और दुनिया भर में अपने उत्पादनों का समर्थन के लिये इंटरनेट को एक संभावित व्यवहार्य साधन के रूप में देखा है। ऑनलाइन शॉपिंग नेटवर्क वाणिज्यिक गतिविधियों का एक बढ़ता प्रतिशत बन गया है। इक्कीस् वीं सदी ने ऑनलाइन व्यापारों के लिए असीम अवसर एवं प्रतिस्पर्धा का वातावरण प्रदान किया है। अनेक ऑनलाइन व्यापारिक कंपनियों की स्थापना हुई है और अनेक मौजूदा कंपनियों ने ऑनलाइन शाखाएँ खोल रखी हैं।

प्रौद्योगिकी निश्चित रूप से अच्छी बात है क्योंकि इससे संचार और सूचनाओं तक पहुँच आसान हो गई है। इसने दुनिया को एक वैश्विक गाँव बना दिया है और उद्यमियों के लिए एक अद्भूत मंच बनाया है। ई–कॉमर्स आधुनिक दुनिया के लिए एक व्यवसाय मॉडल है और सही रणनीतियों को अपनाने के साथ–साथ यह एक छोटे व्यवसाय को एक साम्राज्य में बदल सकता है।

साहित्य का पुनरावलोकन (Review of Literature)

- गुप्ता (2014) ने अपने शोध–पत्र ''ई–कामर्स': ई–कॉमर्स की भूमिका आज के कारोबार में'' ई–कॉमर्स की व्यापक परिभाषा को ई–बिजनेस से अलग करते हुए प्रस्तुत किया है।

---

* (ई.ए.एफ.एम.) वाणिज्य विभाग, म.द.स. विश्वविद्यालय, अजमेर, राजस्थान।

- nkl vkj vkjk ¼2015½ ने अपने शोध पत्र ''ई–कॉमर्स के विकास'' में बताया कि विकसित देश ई–कॉमर्स के माध्यम से अपने बाजारों का विकास–विस्तार करते है और विदेशी निवेशकों को भारतीय बाजार में अत्यधिक संभावनाएँ नजर आती है। जिसके परिणामस्वरूप कई नवीन उद्योगों को उद्यम पूँजीपतियों से निवेश प्राप्त हुआ है।
- ''ई–कॉमर्स की संभावनाएँ और संभावनाएँ'' के माध्यम से j?kukFk vkj ikxk ¼2013½ ने अपने अध्ययन में ई–कॉमर्स का विश्लेषण करते हुए स्पष्ट किया है कि आधुनिक युग में विज्ञापन, आदेश, भुगतान आदि सभी व्यावसायिक गतिविधि को डिजिटल रूप में किया जा सकता है। ई–कॉमर्स ने आंतरिक व्यापार प्रबंधन को बढ़ावा देकर बेहतर ग्राहक संबंधों में भी वृद्वि की है।

'kks/k dk mn~ns'; **(Objective of the Study)**

वर्तमान अध्ययन के निम्नलिखित उद्देश्य हैं:–

- ई–कॉमर्स में साइबर सुरक्षा के उद्देश्य को समझना।
- साइबर सुरक्षा को प्रोत्साहित करने के लिए राष्ट्रीय साइबर सुरक्षा नीति 2013 की योजनाओं का अध्ययन करना।
- ई–कॉमर्स में साइबर सुरक्षा की चुनौतियों का अध्ययन करना।

'kks/k izfof/k **(Research Methodology)**

प्रस्तावित शोध पत्र के अध्ययन के उद्देश्य के लिए समंक संग्रहण तकनीक में द्वितीयक समंकों का प्रयोग किया गया है। शोध कार्य हेतु द्वितीयक आँकड़े विभिन्न शोध–पत्रों सरकारी दस्तावेज, साप्ताहिक, मासिक, वार्षिक पत्र–पत्रिकाओं के लेख समाचार–पत्रों तथा इंटरनेट के माध्यम से एकत्रित किये गए हैं।

- b&dkelZ D;k gS\

ई–कॉमर्स शब्द ''इलेक्ट्रॉनिक कॉमर्स'' का संक्षिप्त रूप है।

ई–कॉमर्स का तात्पर्य इंटरनेट पर चीजों को खरीदने और बेचने की गतिविधि से है। यह एक प्रक्रिया है जिसके द्वारा एक इलेक्ट्रॉनिक माध्यम से वस्तुओं और सेवाओं की खरीद–बिक्री की जाती है। यह ऐसे वाणिज्यिक लेनदेन को प्रदर्शित करता है जो ऑनलाइन आयोजित किए जाते है।मोबाइल कॉमर्स, इंटरनेट मार्केटिंग, ऑनलाइन ट्रांजेक्शन प्रोसेसिंग, इलेक्ट्रॉनिक फंड ट्रांसफर, सप्लाई चेन मैनेजमेंट, सिस्टम और ऑटोमेटेड डेटा कलेक्शन सिस्टम जैसी कई तकनीकों पर ई–कॉमर्स तैयार किया जा सकता है।

b&dkelZ dk bfrgkl

ई–कॉमर्स की शुरूआत 1960 के दशक से शुरू हुई थी, जब बिजनेस ने अन्य कंपनियों के साथ व्यावसायिक दस्तावेज को शेयर करने के लिए Electronic Data Interchange [EDI] का प्रयोग शुरू किया। 1979 में, अमेरिकन नेशनल स्टैंडर्ड इंस्टीट्यूट ने ASC X 12 को इलैक्ट्रॉनिक नेटवर्क के माध्यम से दस्तावेज को शेयर करने के व्यवसायों के लिए एक युनिवर्सल स्टैंडर्ड के रूप में विकसित किया था। ई–कॉमर्स के इतिहास को eBay और Amazon के बिना सोचना असंभव है जो इलैक्ट्रॉनिक टैन्सैक्शन को शुरू करने वाली पहली इंटरनेट कंपनियों में से थे। 1990 के दशक में eBay और Amazon के उदय से ई–कॉमर्स उद्योग में क्रांतिकारी बदलाव आया। उपयोगकर्ता अब ई–कॉमर्स के माध्यम से किसी भी चीज को खरीद सकते है।

lkbcj lqj{kk dk vFk

साइबर सुरक्षा, यह एक तरह की सुरक्षा है जो कि इंटरनेट से जुड़े हुए सिस्टम, नेटवर्क और प्रोग्राम के लिए होती है। इसमें हार्डवेयर, सॉफ्टवेयर और डाटा को साइबर अपराध से बचाने का भी काम किया जाता है। साइबर हमले मुख्यतः उपभोक्ता की संवेदनशील जानकारी तक पहुँचने, बदलने या नष्ट करने के उद्देश्य से होते है, जिनमे यूजर्स/उपयोगकर्ता से रूपया निकालना या सामान्य व्यावसायिक प्रक्रियाओं को बाधित करना प्रमुख होता है। साइबर सुरक्षा डाटा की सुरक्षा के लिए रखी जाती है जिससे कि किसी भी तरह से डाटा की चोरी न हो और सभी दस्तावेज और फाइल सुरक्षित रहे। बड़े–बड़े कम्प्यूटर विशेषज्ञ और आईटी प्रशिक्षित लोग इस प्रकार के काम करने में समर्थ होते है।

lkbcj vijk/k

ये ऐसे गैर–कानूनी कार्य हैं जिनमें कंप्यूटर एवं इंटरनेट नेटवर्क का प्रयोग एक साधन अथवा लक्ष्य अथवा दोनों के रूप में किया जाता है। ऐसे अपराधों में हैकिंग, चाइल्ड पॉर्नोग्राफी, साइबर स्टॉकिंग, सॉफ्टवेयर पाइरेसी, क्रेडिट कार्ड फ्रॉड, फिशिंग आदि को शामिल किया जाता हैं।

Hkkjr e! lkbcj vijk/k jkdu! d! fy, vf/kfu;e

साइबर सुरक्षा पर खतरों को ध्यान में रखते हुए 2 जुलाई, 2013 को केन्द्रीय संचार और सूचना प्रौद्योगिकी मंत्री श्री कपिल सिब्बल ने 'राष्ट्रीय साइबर सुरक्षा नीति, 2013' जारी की।

- भारत में 'सूचना प्रौद्योगिकी अधिनियम 2000' पारित किया गया, जिसके प्रावधानों के साथ–साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिए पर्याप्त है।
- इसके अंतर्गत 2 वर्ष से लेकर उम्रकैद तथा दंड अथवा जुर्माने का भी प्रावधान है।

bl&dkel! d! i!dkj

bl&dkel! e[;r% pkj i!dkj d! gk!r! g%

- **ch 2 lh ¼fctul V! dLT;wej½ %&** इस व्यवसाय में एक व्यवसायी इंटरनेट पर वस्तुओं या सेवाओं को सीधे कंज्यूमर या उपभोक्ता को बेचता है। इसके अन्तर्गत उपभोक्ता किसी कंपनी से सीधे सामान खरीदता है। उदाहरण के लिए अमेजन, फ्लिपकार्ट या अन्य किसी साइट से सामान खरीदना।
- **ch 2 ch ¼fctul V! fctul½%&** इसके अन्तर्गत एक कंपनी किसी कंपनी या फर्म को सामान बेचती है। इसके अन्तर्गत ऐसी कंपनियाँ या फर्म आते है जो स्वयं के प्रयोग के लिए सामान खरीदते है या फिर कच्चा माल खरीदकर उससे बिक्री योग्य सामान तैयार करते हैं।
- **ch 2 lh ¼dLT;wej V! dLT;wej½ %&** इसके अन्तर्गत जब कोई कंज्यूमर या उपभोक्ता अपने प्रॉडक्ट या वस्तु को किसी अन्य कंज्यूमर या उपभोक्ता को इंटरनेट पर बेचता है। इसमें कंज्यूमर सीधे कंज्यूमर से संपर्क करता है, कंपनियों की कोई भूमिका नही होती है।

  इसमें एक कंज्यूमर अपनी पुरानी बाइक,कार जैसी अपनी प्रॉपर्टी को अन्य कंज्यूमर को सीधे इंटरनेट के माध्यम से बेचता है। आम तौर पर, ये लेन–देन थर्ड पार्टी के माध्यम से किया जाता है, जो ऑनलाइन प्लेटफार्म प्रदान करते हैं। इसके लिए OLX जैसी कई कंपनियाँ सर्विस के लिए कन्ज्यूमर को चार्ज करती हैं या फ्री में सर्विस देती है।
- **lh 2 ch ¼dLT;wej V! fctul½ %&** ई–कॉमर्स के इस प्रकार में कंपनी सीधे उपभोक्ता से संपर्क करती है। इसी तरह बाजार में सामानों की बढ़ती माँग और उसकी आपूर्ति के लिए ई–कॉमर्स की ऑनलाइन शॉपिंग में दो प्रकार के मॉडल अधिक प्रचलित हो रहे हैं, जिनमें पहला है : मार्केट प्लेस मॉडल। इस मॉडल में ऑनलाइन कंपनियाँ केवल एक प्लेटफार्म उपलब्ध करा देती है, जहाँ से उपभोक्ता अपनी जरूरत के अनुसार सामान खरीद सकते है। जैसे कि अमेजन, स्नैपडील, फ्लिपकार्ट इत्यादि। इनमें अन्य ऑनलाइन कंपनियों की कोई भूमिका नही होती है।

इसी प्रकार दूसरा प्रचलित मॉडल है : इन्वेंटरी मॉडल। इसके अन्तर्गत ऑनलाइन कंपनी इस प्लेटफॉर्म पर अपनी कंपनी के द्वारा सामान बेचती है। इसमें अलीबाबा का नाम सबसे प्रमुख है।

bl&dkel! lqj{kk midj.k

सुरक्षा, इंटरनेट पर होने वाले किसी भी लेनदेन का एक अनिवार्य हिस्सा है। विभिन्न ई–कॉमर्स सुरक्षा उपकरण इस प्रकार हैः–

- फायरवॉल–सॉफ्टवेयर और हार्डवेयर
- सार्वजनिक कुंजी अवसंरचना
- एन्क्रिप्शन सॉफ्टवेयर
- डिजिटल प्रमाण–पत्र

- डिजिटल हस्ताक्षर
- बॉयोमैट्रिक्स–रेटिना स्कैन, उंगलियों के निशान, आवाज आदि।
- ताले और बार–नेटवर्क संचालन केन्द्र।

bi&dkelI ,lyhdi'ku e lij{kk enn

किसी भी ई–कॉमर्स एप्लिकेशन में निम्नलिखित प्रकार के सुरक्षा मुद्दे हैः–

- nHkkouki.k dkM
  - वायरसः उनके पास अन्य फाइलों को दोहराने और फैलाने की क्षमता है। अधिकांश किसी प्रकार का ''पेलोड'' भी देते है (विनाशकारी या सौम्य), जिनमें मैक्रो वायरस, फाइल संक्रमित वायरस और स्क्रिप्ट वायरस सम्मिलित है।
  - कीड़ेः वे कीड़े जिन्हे कंप्यूटर से कंप्यूटर तक फैलाने के लिए डिज़ाइन किया गया है।
  - ट्रोजन हॉर्सः वे सौम्य प्रतीत होते है, लेकिन फिर उम्मीद के अलावा कुछ करते है।
  - बॉट्सः इसे कंप्यूटर में गुप्त रूप से स्थापित किया जा सकता है, यह हमलावर द्वारा भेजे गये बाहरी आदेशों का जवाब देता है।

अवांछित कार्यक्रमः ये उपयोगकर्ता की सूचित सहमति के बिना स्थापित किये गये है। इसके निम्नलिखित प्रकार होते हैः–

- ब्राउजर परजीवीः यह उपयोगकर्ता के ब्राउज़र की सेटिंग और मॉनिटर को बदल सकता है।
- एडवेयरः यह अवांछित पॉप–अप विज्ञापनों के लिए कहता है।

फिशिंग और पहचान की चोरीः किसी भी भ्रामक, तीसरे पक्ष द्वारा वित्तीय लाभ के लिए गोपनीय जानकारी प्राप्त करने का ऑनलाइन प्रयास है।

सबसे लोकप्रिय प्रकार– ई–मेल घोटाला पत्रः यह ई–कॉमर्स अपराध के सबसे तेजी से बढ़ते रूपों में से एक है।

- हैकिंग और साइबर बर्बरताः
- हैकरः वह व्यक्ति जो कंप्यूटर सिस्टम में अनाधिकृत पँहुच प्राप्त करना चाहता है।
- क्रैकरः आपराधिक इरादे के साथ हैकर (दो शब्दों का अक्सर एक–दूसरे से इस्तेमाल किया जाता हैं।)
- साइबर बर्बरताः वेबसाइट को जानबूझकर बाधित करना, खराब करना या नष्ट करना।

bi&dkelI vuii;kx d fy, yUk&nu lij{kk

- ,fUØl'ku nf"Vdk.k

एन्क्रिप्शन सादा पाठ या डेटा को सिफर पाठ में बदलने की प्रक्रिया है जिसे प्रेषक और प्राप्तकर्ता के अतिरिक्त किसी और के द्वारा नहीं पढ़ा जा सकता है।

एन्क्रिप्शन का उद्देश्य हैः–

- संग्रहीत जानकारी और सुरक्षित करने के लिए।
- सूचना प्रसारण को सुरक्षित करने के लिए।

कई प्रकार के एन्क्रिप्शन हैं जो इसकी कार्यक्षमता के संदर्भ में भिन्न हैं।

सममित कुंजी एन्क्रिप्शन में, प्रेषक और प्राप्तकर्ता दोनों एन्क्रिप्ट और डिक्रिप्ट करने के लिए एक ही कुंजी का उपयोग करते है। जबकि सार्वजनिक कुंजी एन्क्रिप्शन में गणितीय रूप से संबंधित दो डिजिटल कुंजी, सार्वजनिक कुंजी और निजी कुंजी का उपयोग किया जाता है।

- ljf{kr lkdV y;j

टीसीपी/ आईपी के सिक्योर लेयर (एसएसएल) के माध्यम से सबसे सुरक्षित चैनल का सबसे सामान्य रूप है। एसएसएल प्रोटोकॉल डेटा एन्क्रिप्शन, सर्वर प्रमाणीकरण, वैकल्पिक क्लाइंट प्रमाणीकरण और संदेश

अखंडता प्रदान करता है। टीसीपी/ आईपी कनेक्शन, सिक्योर सर्किट लेयर (एसएसएल) एक सुरक्षा प्रोटोकॉल है, जिसे पहले नेटस्केप कम्युनिकेशन कॉरपोरेशन द्वारा विकसित किया गया था और अब ट्रांसपोर्ट लेयर सिक्योरिटी वर्किंग ग्रुप्स के हाथों में लिया गया है। प्रोटोकॉल के डिजाइन का लक्ष्य है जब दो संचार अनुप्रयोगों के बीच एक डेटा को इंटरनेट पर ले जाया जाता है, तब ईवसड्रापिंग, छेड़छाड़ या संदेश जालसाजी को रोकना है।

- ljf{kr gkbijVDLV VklQj ikVkdky (S-HTTP)

S-HTTP एक सुरक्षित संदेश–उन्मुख संचार प्रोटोकॉल है, जो HTTP के साथ संयोजन के रूप में उपयोग के लिए डिजाइन किया गया है। यह HTTP के साथ सह–अस्तित्व के लिए और HTTP अनुप्रयोगों के साथ आसानी से एकीकृत होने के लिए डिजाइन किया गया है। जबकि SSL को दो कंप्यूटरों के बीच एक सुरक्षित कनेक्शन स्थापित करने के लिए डिज़ाइन किया गया है। एस–एचटीटीपी का अलग–अलग संदेश सुरक्षित रूप से भेजने के लिए डिजाइन किया गया है। एस–एचटीटीपी को उपयोग करते हुए, किसी भी संदेश पर हस्ताक्षर किए जा सकते है, प्रमाणित किया जा सकता है, एन्क्रिप्ट किया जा सकता है। सामान्यतः एस–एचटीटीपी (S-HTTP) का प्रयास एचटीटीपी (HTTP) को अधिक सुरक्षित बनाने के लिए होता है।

- fMftVy gLrk{kj

डिजिटल हस्ताक्षर का मतलब किसी रिकॉर्ड को प्रमाणित करने के इरादे से किसी पार्टी द्वारा निष्पादित एक अद्वितीय डिजिटल तरीका है जो कि इसका उपयोग करने वाले व्यक्ति के सत्यापन में सक्षम है। यह डेटा से इस तरह से जुड़ा होता है कि यदि डेटा को बदल दिया जाता है तो इलेक्ट्रॉनिक हस्ताक्षर अमान्य है। एक डिजिटल हस्ताक्षर आम तौर पर सन्देश का एक हैश होता है जिसे मालिक की निजी कुंजी के साथ एन्क्रिप्टेड किया जाता है।

- ljf{kr byDVkfud yunu **(SET)**

ई–कॉमर्स में शामिल सभी की सुरक्षा के लिए क्रेडिट/भुगतान कार्ड लेनदेन के लिए सुरक्षित इलेक्ट्रॉनिक लेनदेन (SET) विनिर्देश आवश्यक है। यह तीन मुख्य उद्देश्यों को पूरा करने के लिए डिजाइन किया जाता है।

  - यह सभी शामिल प्रमाणित कार्ड के लिए भुगतान सुरक्षा प्रदान करता है।
  - डिजिटल कार्ड धारकों और व्यापारियों को भुगतान डेटा के लिए गोपनीयता प्रदान करता है।
  - प्रोटोकॉल और संभावित इलेक्ट्रॉनिक सुरक्षा सेवा प्रदाताओं को परिभाषित करते है।

यह विभिन्न विक्रेताओं द्वारा विकसित अनुप्रयोगों के बीच अंतर को भी सक्षम करेगा और विभिन्न ऑपरेटिंग सिस्टम और प्लेटफॉर्म के बीच अंतर को सक्षम करेगा।

- fMftVy iek.k i=

डिजिटल प्रमाण–पत्र एक ऐसा साधन है जिसके द्वारा उपभोक्ता और व्यवसाय सार्वजनिक कुंजी अवसंरचना (PKI) के सुरक्षा अनुप्रयोगों का उपयोग कर सकते है। सार्वजनिक कुंजी अवसंरचना (PKI) में सुरक्षित ई–कॉमर्स और इंटरनेट आधारित संचार को सक्षम करने के लिए प्रौद्योगिकी शामिल है।

fu"d"k

सूचना प्रौद्योगिकी के क्षेत्र में की जा रही प्रगति के बावजूद ई–कॉमर्स में साइबर सुरक्षा हमेशा एक चुनौती के रूप में उजागर हुआ है। आम ई–कॉमर्स उपयोगकर्ता साइबर अपराधों से अनजान हो सकते है। जब से तकनीक तीव्र गति से विकसित हो रही है, कई निर्दोष व्यक्ति दुनिया भर में ई–कॉमर्स के दौरान साइबर अपराधों के शिकार होते है। इस आधुनिक युग में ई–कॉमर्स में साइबर अपराध का शिकार होने से बचना लगभग असंभव है, प्रौद्योगिकी में प्रगति साइबर अपराध करने के विभिन्न तरीकों को सुगम बनाती है। साइबर अपराध का शिकार बनने से बचने के लिए विभिन्न स्तरों पर जागरूक होने की जरूरत है। संभावित साइबर अपराधों से बचने के लिए आवश्यक सावधानी रखना भी अति आवश्यक है। कुछ समय तक भारतीय उपभोक्ता की छवि एक पांरपरिक ढंग से बंधी थी, परन्तु ई–कॉमर्स की सुविधा के आगमन के साथ ही गत कुछ वर्षों से

भारतीय उपभोक्ता एक नई दिशा की ओर अग्रसर हुआ है। विशेषज्ञों का मानना है कि आने वाले वर्षों में भारत के कई क्षेत्रों में ऑनलाइन रिटेलिंग पारंपरिक रिटेल आउटलेट्स को पीछे छोड़ देगी जो कि भारतीय प्रौद्योगिकी के विकास की ओर इंगित करता है।

lUnHk xUFk lph **(Refrences)**

- ई–वाणिज्य–विकिपीडिया
- भारत में ई–कामर्स का विकास–विकिपीडिया
- साइबर सुरक्षा बढ़ाए ई–कॉमर्स
- ई–कॉमर्स सुरक्षा प्रणाली
- राष्ट्रीय साइबर सुरक्षा नीति–2013
- Security Threats of E-Commerce
- साइबर सुरक्षा की चुनौतियाँ–प्रभात खबर–पवन दुग्गल
- E-Commerce Security Tools
- Cyber crime
- देबेन्द्र शॉ, ''भारत में साइबर अपराध ई–कॉमर्स के लिए एक चुनौती'' इंटरनेशनल जर्नल ऑफ मल्टीडिसिप्लिनरी स्टडीज, E-ISSN : 2456-3064 वाल्यूम I , नंबर 2 अक्टूबर 2016, पीपी 75–83।
- मधुरिमा खोसला / हरीश कुमार ''भारत में ई–कॉमर्स का विकासः एक विश्लेषणात्मक समीक्षा'' IOSR जर्नल ऑफ बिजनेस एंड मैनेजमेंट (IOSR- JBM) E-ISSN:2278-487X-पी-ISSN:2319-7668/ वॉल्यूम 19, अंक 6, वेर / I (जून,2017) पीपी 91–95
- www.iosrjournals.org
- दास गुप्ता, पी /और सेनगुप्ता, के । 2002 । ''भारतीय बीमा उद्योग में ई–कॉमर्स : संभावनाएँ और भविष्य'' इलेक्ट्रॉनिक कॉमर्स रिसर्च, 2–43–60। क्रॉसरफ गूगल स्कॉलर
- Santosh Kumar Maurya, Nagendra Pratap Bharti, "Cyber security : Issue and Challenges in E-commerce " IJOR (Indian Journal of Researc) PARIPEX E-ISSN-2250-1991,Volume-5। Issue : 1 । January 2016 । PP 191-193
- प्रज्ञा बी राणे$_1$ डॉ बीबीमश्रम$_2$, ''ई–कॉमर्स अनुप्रयोग के लिए लेनदेन सुरक्षा'' इंटरनेशनल जर्नल ऑफ इलेक्ट्रानिक एंड कंप्यूटर सांइस इंजीनियरिंग, ijecse ISSN-2277-1956।
- https://hi.m.wikipedia.org
- https://hi.m.wikipedia.org
- https://naidunia.jagran.com
- https://www.tutorialspoint.com
- https://www.javapoint.com
- https://www.cgbank.in
- https://www.prabhatkhabar-com.edu.ampproject.org
- www.google.com
- www.wikipedia.com
- www.shodhgangotri.inflibnet.ac.in
- www.ssgcp.com
- www.simplynotes.in

❖◆❖