ARYAVART SHODH VIKAS PATRIKA
RNI TITLED NO. UPBIL04292
RNI REG. NO. UPBIL/2014/66218 **PP. No.- 313-314**
I S S N NO. - 2347 – 2944 (Print)
e–I S S N NO.- 2582 – 2454 (Online)
Vol.-19, No.-I, Issues-35, YEAR-Jan-Mar. 2025

साइबर सुरक्षा और सामाजिक मीडिया

डॉ0 अनूप कुमार श्रीवास्तव
असिस्टेंट प्रोफेसर– रक्षा एवं स्त्रातजिक अध्ययन विभाग, महाविद्यालय भटवली बाजार, उनवल, गोरखपुर (उ0प्र0) भारत

Received-13.03.2025, Revised-23.03.2025 Accepted-29.03.2025 **E-mail : dranuplal79@gmail.com**

सारांशः ***आधुनिक युग को सूचना एवं प्रौद्योगिकी का युग कहा जाता है। इंटरनेट और सामाजिक मीडिया ने संचार, शिक्षा, व्यापार, मनोरंजन तथा सामाजिक संबंधों को नई दिशा प्रदान की है। आज विश्व की बड़ी जनसंख्या सामाजिक मीडिया प्लेटफॉर्म का उपयोग कर रही है। सामाजिक मीडिया ने सूचना के आदान–प्रदान को तीव्र, सरल और वैश्विक बना दिया है।***

किन्तु सामाजिक मीडिया के बढ़ते उपयोग के साथ साइबर अपराध, डेटा चोरी, ऑनलाइन धोखाधड़ी, फर्जी समाचार, साइबर बुलिंग तथा गोपनीयता संबंधी समस्याएँ भी बढ़ी हैं। यही कारण है कि साइबर सुरक्षा आज वैश्विक स्तर पर एक महत्वपूर्ण विषय बन चुकी है।

साइबर सुरक्षा का उद्देश्य इंटरनेट, डिजिटल नेटवर्क, कंप्यूटर प्रणाली तथा व्यक्तिगत डेटा को अनधिकृत पहुँच, साइबर हमलों और डिजिटल अपराधों से सुरक्षित रखना है। सामाजिक मीडिया प्लेटफॉर्म जैसेः Facebook,Instagram,WhatsApp,X, YouTube ने लोगों को जोड़ने का कार्य किया है, परन्तु इनके माध्यम से साइबर अपराधों में भी वृद्धि हुई है।

प्रस्तुत लेख में साइबर सुरक्षा की अवधारणा, सामाजिक मीडिया की भूमिका, साइबर अपराधों के प्रकार, उनके प्रभाव, सरकारी प्रयास, चुनौतियाँ तथा समाधान का विस्तृत विश्लेषण प्रस्तुत किया गया है।

कुंजीभूत शब्द– साइबर सुरक्षा, सामाजिक मीडिया, आधुनिक युग, सूचना एवं प्रौद्योगिकी युग, इंटरनेट, डिजिटल नेटवर्क, वैश्विक स्तर।

प्रस्तावना– 21वीं शताब्दी में डिजिटल तकनीक ने मानव जीवन को अत्यधिक प्रभावित किया है। इंटरनेट और स्मार्टफोन के प्रसार ने सामाजिक मीडिया को जीवन का अभिन्न अंग बना दिया है। आज लोग समाचार, शिक्षा, व्यापार, मनोरंजन तथा सामाजिक संपर्क के लिए सामाजिक मीडिया का उपयोग कर रहे हैं।

सामाजिक मीडिया ने लोकतंत्र, अभिव्यक्ति की स्वतंत्रता तथा वैश्विक संचार को सशक्त बनाया है। इसके माध्यम से लोग अपने विचार, अनुभव तथा जानकारी विश्वभर में साझा कर सकते हैं। किन्तु इसके साथ–साथ साइबर अपराधों की समस्या भी तेजी से बढ़ी है। हैकिंग, फिशिंग, डेटा चोरी, ऑनलाइन बैंकिंग धोखाधड़ी, साइबर बुलिंग तथा फर्जी पहचान जैसे अपराध सामाजिक मीडिया के माध्यम से बढ़ रहे हैं।

भारत में इंटरनेट उपयोगकर्ताओं की संख्या तेजी से बढ़ रही है। डिजिटल इंडिया अभियान, ऑनलाइन बैंकिंग तथा डिजिटल भुगतान प्रणाली के कारण साइबर सुरक्षा का महत्व और अधिक बढ़ गया है।

आज साइबर सुरक्षा केवल तकनीकी विषय नहीं रह गया है, बल्कि यह राष्ट्रीय सुरक्षा, आर्थिक विकास तथा सामाजिक स्थिरता से जुड़ा महत्वपूर्ण मुद्दा बन चुका है।

साइबर सुरक्षा की अवधारणा– साइबर सुरक्षा (Cyber Security) वह प्रक्रिया है, जिसके माध्यम से कंप्यूटर, मोबाइल, नेटवर्क, इंटरनेट तथा डिजिटल डेटा को साइबर हमलों और अनधिकृत पहुँच से सुरक्षित रखा जाता है।

इसका उद्देश्य– डेटा की सुरक्षा, गोपनीयता की रक्षा, साइबर अपराधों की रोकथाम, डिजिटल नेटवर्क की सुरक्षा, ऑनलाइन लेन–देन की सुरक्षा है।

सामाजिक मीडिया की अवधारणा– सामाजिक मीडिया ऐसे डिजिटल प्लेटफॉर्म हैं जिनके माध्यम से लोग जानकारी साझा करते हैं, संवाद करते हैं तथा ऑनलाइन समुदाय बनाते हैं।

सामाजिक मीडिया की प्रमुख विशेषताएँ–

- त्वरित संचार,
- वैश्विक पहुँच,
- सूचना साझा करना,
- वीडियो एवं फोटो साझा करना,
- ऑनलाइन समुदाय निर्माण,

आज सामाजिक मीडिया राजनीति, शिक्षा, व्यापार तथा मनोरंजन का प्रमुख माध्यम बन चुका है।

साइबर अपराधों के प्रमुख प्रकार–

1. हैकिंगः हैकिंग वह प्रक्रिया है जिसमें कोई व्यक्ति अनधिकृत रूप से कंप्यूटर प्रणाली या खाते में प्रवेश करता है। सामाजिक मीडिया खातों की हैकिंग आज एक सामान्य समस्या बन चुकी है।

2. फिशिंग (Phishing): फिशिंग में अपराधी नकली वेबसाइट या संदेश के माध्यम से लोगों की व्यक्तिगत जानकारी प्राप्त करते हैं। बैंकिंग पासवर्ड, OTP तथा डेबिट कार्ड जानकारी चोरी करना इसके प्रमुख उदाहरण हैं।

3. साइबर बुलिंगः सामाजिक मीडिया पर किसी व्यक्ति को धमकाना, अपमानित करना या मानसिक रूप से परेशान करना साइबर बुलिंग कहलाता है। यह समस्या विशेष रूप से किशोरों और युवाओं में अधिक देखी जाती है।

4. डेटा चोरीः सामाजिक मीडिया प्लेटफॉर्म पर उपयोगकर्ताओं की व्यक्तिगत जानकारी चोरी होने की घटनाएँ बढ़ रही हैं। डेटा चोरी से गोपनीयता और आर्थिक सुरक्षा दोनों प्रभावित होती हैं।

5. फर्जी समाचार (Fake News): सामाजिक मीडिया पर गलत एवं भ्रामक सूचनाओं का तेजी से प्रसार होता है। फर्जी समाचार सामाजिक तनाव, हिंसा तथा राजनीतिक अस्थिरता का कारण बन सकते हैं।

6. ऑनलाइन वित्तीय धोखाधड़ीः डिजिटल भुगतान और ऑनलाइन बैंकिंग के बढ़ते उपयोग के कारण साइबर ठगी की घटनाएँ बढ़ी हैं। UPI धोखाधड़ी, नकली लिंक तथा QR कोड स्कैम इसके प्रमुख उदाहरण हैं।

सामाजिक मीडिया का सकारात्मक प्रभाव–

I S S N NO. - 2347 – 2944 (Print)
e–I S S N NO.- 2582 – 2454 (Online)
Vol.-19, No.-I, Issues-35, YEAR-Jan-Mar. 2025

1. सूचना का तीव्र प्रसारः सामाजिक मीडिया के माध्यम से समाचार एवं जानकारी तुरंत विश्वभर में पहुँच जाती है।

2. शिक्षा में योगदानः ऑनलाइन शिक्षा, वेबिनार तथा डिजिटल सामग्री ने शिक्षा को अधिक सुलभ बनाया है।

3. व्यापार एवं रोजगारः सामाजिक मीडिया डिजिटल मार्केटिंग एवं ई–कॉमर्स का प्रमुख माध्यम बन चुका है। छोटे व्यवसायों को भी वैश्विक बाजार तक पहुँच प्राप्त हुई है।

4. सामाजिक जागरूकताः सामाजिक मीडिया ने सामाजिक आंदोलनों, पर्यावरण संरक्षण तथा मानवाधिकार जागरूकता को बढ़ावा दिया है।

सामाजिक मीडिया के नकारात्मक प्रभाव–

1. मानसिक स्वास्थ्य पर प्रभावः सामाजिक मीडिया की अत्यधिक निर्भरता तनाव, चिंता तथा अवसाद जैसी समस्याओं को बढ़ा सकती है।

2. गोपनीयता की समस्याः उपयोगकर्ताओं की व्यक्तिगत जानकारी का दुरुपयोग किया जा सकता है।

3. सामाजिक विभाजनः फर्जी समाचार एवं घृणास्पद सामग्री सामाजिक तनाव को बढ़ा सकती है।

4. समय की बर्बादीः सामाजिक मीडिया का अत्यधिक उपयोग उत्पादकता को प्रभावित करता है।

भारत में साइबर सुरक्षा की स्थिति– भारत विश्व के सबसे बड़े इंटरनेट उपयोगकर्ता देशों में शामिल है। डिजिटल भुगतान, ऑनलाइन शिक्षा तथा ई–गवर्नेंस के विस्तार के कारण साइबर सुरक्षा की आवश्यकता और बढ़ गई है। भारत में साइबर अपराधों की संख्या लगातार बढ़ रही है। बैंकिंग धोखाधड़ी, सोशल मीडिया हैकिंग तथा ऑनलाइन ठगी प्रमुख समस्याएँ हैं।

भारतीय सरकार के प्रयास– भारत सरकार ने साइबर सुरक्षा को मजबूत बनाने हेतु अनेक कदम उठाए हैंकृ

1. डिजिटल इंडिया अभियानः इस अभियान का उद्देश्य डिजिटल सेवाओं का विस्तार करना है।

2. साइबर अपराध पोर्टलः सरकार ने ऑनलाइन साइबर अपराध शिकायत पोर्टल प्रारंभ किया है।

3. CERT&In की स्थापनाः Indian Computer Emergency Response Team साइबर सुरक्षा घटनाओं की निगरानी एवं समाधान के लिए कार्य करती है।

4. डेटा संरक्षण कानूनः व्यक्तिगत डेटा की सुरक्षा हेतु सरकार ने डिजिटल डेटा संरक्षण संबंधी नीतियाँ विकसित की हैं।

5. साइबर जागरूकता अभियानः सरकार एवं शैक्षणिक संस्थाएँ साइबर सुरक्षा जागरूकता कार्यक्रम चला रही हैं।

साइबर सुरक्षा की चुनौतियाँ–

1. तकनीकी विकास की तीव्र गतिः नई तकनीकों के विकास के साथ साइबर अपराध भी अधिक जटिल होते जा रहे हैं।

2. जागरूकता की कमीः ग्रामीण एवं कम शिक्षित क्षेत्रों में साइबर सुरक्षा संबंधी जागरूकता सीमित है।

3. विशेषज्ञों की कमीः भारत में प्रशिक्षित साइबर सुरक्षा विशेषज्ञों की आवश्यकता बढ़ रही है।

4. अंतरराष्ट्रीय साइबर अपराधः साइबर अपराध सीमाओं से परे होते हैं, इसलिए इनके नियंत्रण में अंतरराष्ट्रीय सहयोग आवश्यक है।

साइबर सुरक्षा के समाधान–

1. मजबूत पासवर्ड का उपयोगः उपयोगकर्ताओं को जटिल एवं सुरक्षित पासवर्ड का उपयोग करना चाहिए।

2. दो–स्तरीय प्रमाणीकरण (Two&Factor Authentication): यह खातों की सुरक्षा को और मजबूत बनाता है।

3. साइबर जागरूकताः स्कूलों, कॉलेजों एवं समाज में साइबर सुरक्षा शिक्षा को बढ़ावा देना आवश्यक है।

4. सुरक्षित इंटरनेट उपयोगः अज्ञात लिंक, नकली वेबसाइट एवं संदिग्ध संदेशों से बचना चाहिए।

5. कानूनी व्यवस्था को मजबूत करनाः साइबर अपराधों के लिए कठोर कानून एवं त्वरित कार्रवाई आवश्यक है।

भविष्य की संभावनाएँ– भविष्य में कृत्रिम बुद्धिमत्ता (AI), ब्लॉकचेन तथा क्लाउड कंप्यूटिंग साइबर सुरक्षा को नई दिशा प्रदान करेंगे। भारत डिजिटल अर्थव्यवस्था के क्षेत्र में तेजी से आगे बढ़ रहा है। इसलिए साइबर सुरक्षा को राष्ट्रीय विकास का महत्वपूर्ण आधार बनाना आवश्यक है। यदि तकनीकी नवाचार, जागरूकता तथा मजबूत कानूनों पर बल दिया जाए, तो साइबर अपराधों को काफी हद तक नियंत्रित किया जा सकता है।

निष्कर्ष– साइबर सुरक्षा और सामाजिक मीडिया आधुनिक डिजिटल युग के दो महत्वपूर्ण पक्ष हैं। सामाजिक मीडिया ने संचार, शिक्षा, व्यापार तथा सामाजिक जागरूकता को नई दिशा प्रदान की है।

किन्तु इसके साथ साइबर अपराध, डेटा चोरी, फर्जी समाचार तथा गोपनीयता संबंधी समस्याएँ भी बढ़ी हैं। इसलिए साइबर सुरक्षा आज व्यक्तिगत, सामाजिक तथा राष्ट्रीय सुरक्षा का महत्वपूर्ण हिस्सा बन चुकी है।

भारत जैसे डिजिटल विकासशील देश के लिए साइबर सुरक्षा को मजबूत करना अत्यंत आवश्यक है। जागरूकता, तकनीकी विकास तथा प्रभावी कानूनों के माध्यम से साइबर अपराधों पर नियंत्रण पाया जा सकता है। सुरक्षित डिजिटल वातावरण ही भविष्य के सशक्त समाज एवं अर्थव्यवस्था की आधारशिला होगा।

संदर्भ ग्रंथ सूची

1. दत्त एवं सुंदरम – भारतीय अर्थव्यवस्था।
2. मिश्रा एवं पुरी – भारतीय अर्थव्यवस्था।
3. साइबर सुरक्षा एवं सूचना प्रौद्योगिकी – भारत सरकार प्रकाशन।
4. डिजिटल इंडिया रिपोर्ट।
5. योजना पत्रिका – डिजिटल भारत विशेषांक।
6. meity.gov.in
7. cybercrime.gov.in
8. विश्व बैंक रिपोर्ट।
9. अंतरराष्ट्रीय दूरसंचार संघ (ITU) रिपोर्ट।
10. भारतीय रिज़र्व बैंक वार्षिक रिपोर्ट।

*****