International Journal of Humanities and Social Science Research
www.socialsciencejournal.in
ISSN: 2455-2070
Received: 12-07-2025, Accepted: 11-08-2025, Published: 27-08-2025
Volume 11, Issue 4, 2025, Page No. 166-170

ए0आई0 के युग में साइबर सुरक्षा के समक्ष चुनौतियाँ

पंकज कुमार [1], आदित्य कुमार [2]
[1] प्रोफेसर, राजनीति विज्ञान विभाग, इलाहाबाद विश्वविद्यालय, प्रयागराज, उत्तर प्रदेश, भारत
[2] शोध छात्र, राजनीति विज्ञान विभाग, इलाहाबाद विश्वविद्यालय, प्रयागराज, उत्तर प्रदेश, भारत

सारांश
कृत्रिम बुद्धिमत्ता के उदय ने स्वास्थ्य सेवा, वित्त, मनोरंजन, सेना, कृषि, शिक्षा, यातायात आदि कई पहलुओं को अपने आप में समेटते हुए मानव जीवन में क्रांति सी ला दी है। हालांकि, यह प्रौद्योगिकीय उन्नति कई नई चुनौतियों को भी सामने लाती है जिसमें से एक महत्त्वपूर्ण क्षेत्र साइबर सुरक्षा का भी है। भारत का डिजिटल परिदृश्य तेजी से विकसित हो रहा है और 'इंटरनेट उपयोगकर्ताओं की संख्या 800 मिलियन से अधिक हो गई है' और सरकार सक्रिय रूप से आधार और डिजिटल इंडिया जैसी पहलों को बढ़ावा दे रही है। हालांकि इस विकास में दुर्भावनापूर्ण कार्य करने वाले भी पनप रहे हैं। केवल वर्ष 2023 में, भारत में एक अरब से अधिक साइबर हमले हुए जो मजबूत साइबर सुरक्षा उपायों की तत्काल आवश्यकता की तरफ ध्यान आकर्षित कर रहे हैं। न सिर्फ भारत बल्कि पूरी दुनिया एक बड़े डिजिटल क्रांति के दौर से गुजर रही है। क्रांति की इस धारा में कृत्रिम बुद्धिमत्ता प्रौद्योगिकी का बहाव सबसे तेज महसूस किया जा सकता है जो खतरा एवं अवसर दोनों एक साथ प्रस्तुत करती है। इसलिए आज ए0आई0 को सुरक्षित रूप से डिजाइन करना, तैनात करना एवं उपयोग करना बहुत महत्त्वपूर्ण होता जा रहा है ताकि आने वाली पीढ़ियाँ इस बदलाव को बिना कसी झिझक के अपना सके।

मूलशब्दः साइबर सुरक्षा, डिजिटल क्रांति, ए0आई0, डीपफेक, सोशल इंजीनियरिंग आदि।

साइबर सुरक्षा में ए0आई0 का एकीकरण अवसर और कठिनाइयां दोनों प्रदान करता है। एक ओर, ए0आई0 खतरे का पता लगा सकता है और प्रतिक्रिया को स्वचालित कर सकता है, विसंगतियों की पहचान करने के लिए बड़ी मात्रा में डाटा का विश्लेषण कर सकता है और यहाँ तक कि भविष्य के हमलों की भविष्यवाणी भी कर सकता है। हालांकि, 'ए0आई0 संचालित टूल का उपयोग हमलावरों द्वारा परिष्कृत साइबर हमले शुरू करने, सोशल इंजीनियरिंग के लिए डीपफेक बनाने और मैलवेयर विकास को स्वचालित करने के लिए किया जा सकता है।' हाल के वर्षों में भारत ने वैश्विक औसत को पार करते हुए साइबर हमलों में अभूतपूर्व वृद्धि का अनुभव किया है। मजबूत साइबर सुरक्षा उपायों की आवश्यकता महत्त्वपूर्ण है और ए0आई0 प्रौद्योगिकियां इन चुनौतियों का समाधान करने में महत्त्वपूर्ण भूमिका निभाती हैं। साइबर सुरक्षा में ए0आई0 का उदय निःसंदेह नैतिक चिंताओं को भी बढ़ाता है खासकर गोपनीयता के सम्बन्ध में। इसलिए, इस संदर्भ में विशेष रूप से ध्यान देने की आवश्यकता है क्योंकि न सिर्फ आज का समय बल्कि आने वाला भविष्य भी डिजिटलीकरण के ही साये में विकास करेगा तो ऐसे में लोगों के सारे डेटा, सारी जानकारियाँ, फोटो, वीडियो, फाइलें, डाक्यूमेंट्स सब कुछ ऑनलाइन रूप से संग्रहित किया जायेगा ऐसे में इनके वायरल सम्बन्धी समस्या का निराकरण आवश्यक है।

इस तरह देखा जाय तो कृत्रिम बुद्धिमत्ता की तीव्र प्रगति ने हमारे जीवन के विभिन्न पहलुओं को बदल दिया है जिससे मानव जीवन शैली में अभूतपूर्व सुविधा और दक्षता आई है। हालांकि ए0आई0 प्रौद्योगिकियों को अपनाने में वृद्धि के साथ नए साइबर खतरे सामने आए हैं। जैसे–जैसे ए0आई0 अधिक परिष्कृत होता जा रहा है, वैसे–वैसे साइबर अपराधियों द्वारा अपनाई जाने वाली तकनीकें भी बढ़ती जा रही हैं। यहाँ हम कुछ महत्त्वपूर्ण साइबर सुरक्षा खतरों की चर्चा करेंगें–

- **ए0आई0 संचालित मैलवेयर–** बड़ी चिंताओं में से एक परिष्कृत मैलवेयर और साइबर हमलों को विकसित करने में ए0आई0 का उपयोग है। ए0आई0 का उपयोग सिस्टम की कमजोरियों की पहचान करने, लक्षित हमलों को तैयार करने और पारम्परिक सुरक्षा उपायों से बचने के लिए किया जा सकता है। 'साइबर अपराधी मैलवेयर विकसित करने के लिए ए0आई0 एल्गोरिदम का लाभ उठा सकते हैं जो अपने वातावरण को अनुकूलित करके उपभोक्ता की पसंद–नापसंद का फायदा उठाकर इस डेटा का दुरूपयोग कर सकता है।'

ए0आई0 संचालित मैलवेयर से निपटने के लिए साइबर सुरक्षा पेशेवरो को ए0आई संचालित सुरक्षा को नियोजित करने की आवश्यकता है। एल्गोरिदम डेटा के बड़े सेट की जाँच कर सकते हैं और दुर्भावनापूर्ण गतिविधियों से जुड़े पैटर्न की पहचान कर सकते हैं। इसलिए ए0आई0 मॉडल को लगातार अद्यतन और प्रशिक्षित करके सम्भावित खतरों से निपटने के लिए मजबूत बनाये जाने की आवश्यकता है।

- **डीपफेक हमले–** डीपफेक तकनीक, जो ऑनलाइन सामग्री में हेरफेर या निर्माण करने के लिए ए0आई0 का उपयोग करती है, आजकल यह व्यक्तियों, संगठनों, राजनेताओं, बड़ी हस्तियों और यहाँ तक कि राष्ट्रीय सुरक्षा के लिए भी बहुत बड़ा खतरा एवं चुनौती बनती जा रही है। साइबर अपराधी व्यक्तियों को धोखा देने या जनता की राय में हेरफेर करने के लिए विश्वसनीय डीपफेक वीडियों, चित्र या ऑडियो रिकॉर्डिंग बना सकते हैं।

इन डीपफेक हमलों का उपयोग विभिन्न दुर्भावनापूर्ण उद्देश्यों के लिए किया जा सकता है जैसे गलत सूचना फैलाना, व्यक्तियों को ब्लैकमेल करना या वित्तीय लाभ के लिए प्रमुख व्यक्तियों का प्रतिरूपण करना। 'डीपफेक का पता लगाना तेजी से चुनौतीपूर्ण होता जा रहा है क्योंकि ए0आई0 एल्गोरिदम अत्यधिक यथार्थवादी सामग्री उपलब्ध करने के उनकी क्षमता में सुधार करते हैं।'

डीपफेक हमलों का मुकबला करने के लिए, शोधकर्ता ए0आई0 एल्गोरिदम विकसित कर रहे हैं जो हेरफेर की गई सामग्री की पहचान कर सकता है। ये एल्गोरिदम सूक्ष्म दृश्य या श्रव्य संकेतों का विश्लेषण करते हैं जो छेडछाड़ का संकेत देते हैं, जैसे चेहरे के भावों में विसंगतियां या अप्राकृतिक भाषा पैटर्न। इसके अलावा,

लोगों को डीपफेक के बारे में शिक्षित करना और मीडिया साक्षरता को बढ़ावा देना ऐसे हमलों के प्रभाव को कम करने के लिए महत्वपूर्ण है।

- **सोशल इंजीनियरिंग सम्बन्धित मुद्दे–** सोशल इंजीनियरिंग हमले लम्बे समय से साइबर अपराधियों के लिए मानवीय कमजोरियों का फायदा उठाने का एक पसंदीदा तरीका रहा है। ए0आई0 के साथ मिलकर सोशल इंजीनियरिंग हमलें और भी अधिक परिष्कृत हो जाते हैं। ए0आई0 एल्गोरिदम हमलों को तैयार करने के लिए सोशल मीडिया, ऑनलाइन प्रोफाइल और सार्वजनिक रिकार्ड से बड़ी मात्रा में डेटा एकत्र और अपने हित में व्याख्या कर सकता है।

'ए0आई0 संचालित चैटबॉट या वॉयस असिस्टेंट विश्वसनीय व्यक्तियों या संगठनों का प्रतिरूपण कर सकते हैं, जिससे पीड़ितों के लिए धोखाधड़ी वाली गतिविधियों की पहचान करना कठिन हो जाता है। संगठनों और व्यक्तियों को ए0आई0 सहायता प्राप्त सोशल इंजीनियरिंग से निपटने के लिए मजबूत सुरक्षा जागरूकता कार्यक्रम लागू करना चाहिए। शिक्षा और प्रशिक्षण लोगों को संवेदनशील जानकारी साझा करने से बचने व ऑनलाइन सुरक्षा के लिए सचेत करने में महत्वपूर्ण भूमिका निभा सकते हैं।

- **फिशिंग–** फिशिंग एक प्रकार की ऑनलाइन धोखाधड़ी है जिसमें पीड़ितों से क्रेडिट कार्ड नम्बर, पासवर्ड, खाता संख्या, ओ0टी0पी0 आदि जैसी गोपनीय व महत्वपूर्ण जानकारी गलत तरीके से प्राप्त करने के लिए विभिन्न प्रकार के अवैधानिक तरीके अपनाये जाते हैं। फिशिंग हमले आमतौर पर ई–मेल के माध्यम से किये जाते हैं हालांकि इन्हें सोशल मीडिया संदेश, टेक्स्ट संदेश आदि तरीकों से भी प्रसारित किया जा सकता है।

- **रैनसमवेयर–** रैनसमवेयर एक प्रकार का मैलवेयर है जो आपके कम्प्यूटर पर फाइलों को एन्क्रिप्ट या लॉक कर सकता है और उन्हें डिक्रिप्ट करने के लिए फिरौती की माँग कर सकता है। इस प्रकार का रैनसमवेयर हमला व्यवसायों के लिए विनाशकारी हो सकता है क्योंकि इसके द्वारा गोपनीय जानकारियाँ एकत्र कर चीजों का गलत इस्तेमाल कर लोगों को पैसा देने जैसे अनैतिक कार्यों के लिए मजबूर करके धोखाधड़ी की जा सकती है। आज कल खबरों में ऐसे हमलों के बारे में लगातार देखने–सुनने को मिलता है।

- **ब्लूजैकिंग व ब्लूस्नार्फिंग–** ब्लूजैकिंग एक ऐसी तकनीक है जिसमें ब्लूटूथ के माध्यम से मोबाइल फोन, कम्प्यूटर आदि ब्लूटूथ–सक्षम उपकरणों पर अनचाहे संदेश वीडियों, चित्र या ध्वनि किसी भी रूप में हो सकते हैं। इसके तहत व्यक्तिगत जानकारी में भी सेंध लगाकर सामने वाले उपयोगकर्ता से अपनी बातें मनवायी जा सकती है। जैसे–जैसे तकनीकी बढ़ती जा रही है एवं निरन्तर उन्नत होती जा रही है वैसे–वैसे हमलावर भी स्मार्ट तरीके लगातार ढूढ़ते जा रह हैं।

ब्लूस्नार्फिंग एक वायरलेस डिवाइस से जानकारी चुराने के लिए ब्लूटूथ कनेक्शन का उपयोग है जो विशेष रूप से स्मार्टफोन और लैपटॉप में आम हो गया है। 'प्रोगामिंग भाषाओं का उपयोग करके जो उन्हें लगातार चालू और 'डिस्कवरी' मोड में छोड़े गए ब्लूटूथ डिवाइसों को ढूढ़ने की अनुमति देती है, से साइबर अपराधी बिना कोई निशान छोड़े 300 फीट दूर तक डिवाइस पर हमला कर सकते हैं।'

- **साइबर आतंकवाद–** आमतौर पर आतंकवादी कृत्यों को अंजाम देने के लिए इंटरनेट या कम्प्यूटर प्रौद्योगिकी का उपयोग करके ऑनलाइन विनाश के बड़े कार्य किये जाते हैं, जैसे कि बुनियादी ढाँचे को नुकसान पहुँचाना, तकनीकी खराबी पैदा करना, सिस्टम हैंग या स्लो करना, गोपनीय जानकारी चुराना, राजनीतिक या सांस्कृतिक निहितार्थ में मनमानी सूचनाओं का प्रचार–प्रसार करना आदि। साइबर आतंकवाद के मामले तेजी से जटिल होते जा रहे हैं एवं कृत्रिम बुद्धिमत्ता में जितना ही विकास होता जा रहा, इस प्रकार के हमलें उतने ही बढ़ते जा रहे हैं।

- **ऑनलाइन उत्पीड़न–** सामान्यतया उत्पीड़न की अवधारणा भौतिक रूप से जुड़ी मानी जाती है लेकिन जैसे–जैसे समाज स्मार्ट एवं हाइटेक होता गया वैसे–वैसे सब–परम्परागत तरीकों में परिवर्तन आते चले गये। उसी तरह उत्पीड़न के संदर्भ में देखा जाय तो इसमें साइबरबुलिंग, साइबर स्टॉकिंग और किसी विशेष व्यक्ति को डराने, नुकसान पहुँचाने, क्रोधित करने, शर्मिंदा करने आदि इरादे से बार–बार की जाने वाली हरकतें शामिल हैं। आज ऑनलाइन उत्पीड़न सोशल मीडिया साइटों, डेटिंग एप्स आदि के माध्यम से सबसे अधिक प्रचलित है। ऑनलाइन उत्पीड़न के उदाहरणों में अनुचित और अनचाहे संदेश भेजना, स्पष्ट और जानबूझकर धमकी देना या किसी पीड़ित व्यक्ति की संवेदनशील तस्वीरें या वीडियों वायरल करना शामिल है।

- **डी0डी0ओ0एस0 हमले–** 'डिस्ट्रीब्यूटेड डिनायल ऑफ सर्विस अटैक या डी0डी0ओ0एस0 अटैक, किसी नेटवर्क या वेबसाइट को ट्रैफिक से अभिभूत करने के लिए प्रोग्राम किए जाते है', जिससे यह धीमा हो जाता है या पूरी तरह क्रैश हो जाता है। इस हमले के अन्तर्गत सरकारी और निजी संस्थाओं से सम्बन्धित कम्प्यूटर डेटा को हटाने या छेड़छाड़ करने सम्बन्धी कृत्य भी शामिल हैं।

- **मैन–इन–द–मिडिल (मिटएम) हमला–** कई नेटवर्क प्रोटोकॉल एन्क्रिप्शन द्वारा गुप्तचारों से सुरक्षित होते हैं, जिससे ट्रैफिक को पढ़ना असम्भव हो जाता है। मिटएम हमला एक कनेक्शन को दो टुकड़ों में तोड़कर इन सुरक्षाओं को दरकिनार कर देता है। क्लाइंट और सर्वर के साथ एक अलग एन्क्रिप्टेड कनेक्शन बनाकर, एक हमलावर कनेक्शन पर भेजे गए डेटा को पढ़ सकता है और इसे अपने गंतव्य पर अग्रेषित करने से पहले इच्छानुसार संशोधित कर सकता है। HTTPS प्रोटोकॉल का उपयोग करके सिस्टम हमलों पर अंकुश लगाया जा सकता है।

- **डिजिटल अरेस्ट–** यह साइबर अपराध का एक नया तरीका है। इसमें साइबर ठग लोगों को झूठे इल्जाम लगाकर ब्लैकमेल करते हैं। जब आप उनकी बातों में फंस जाते हैं तो वह पुलिस के बड़े अधिकारी से बात कराने का झांसा देकर अपने ही गिरोह के किसी से वीडियों कॉल पर बात करा देते हैं। इसके बाद शिकार बनाए गए व्यक्ति को इतना डरा धमका दिया जाता है कि वह घबरा जाए। साथ ही फंसने का डर दिखाकर किसी से सम्पर्क करने, कॉल करने या घर से बाहर निकलने से भी मना कर दिया जाता है।

वह बताता है कि आपका आधार, सिम कार्ड, बैंक अकाउंट किसी गैर–कानूनी काम के लिए इस्तेमाल हुआ है। साथ ही अगर उसकी बात नहीं मानी तो आप कानूनी कार्यवाही की जद में आ सकते हैं। इसके बाद वह रूपयों की मांग करता है। ए0आई0 तकनीकि आ जाने से कॉल पर आवाज बदलना या वीडियों कॉल पर चेहरा बदलना भी मुमकिन होने से इसके खतरे और बढ़ गये है।

- **व्हेल–फिशिंग–** इस पद्धति का उपयोग करने वाले हमलावर किसी संगठन में 'बड़ी मछली' प्रकार के लोगों को निशाना बनाते हैं इसीलिए इसे व्हेल नाम दिया गया है। 'व्हेल–फिशिंग लक्ष्यों में कम्पनियों के संस्थापक या सी0ई0ओ0 जैसे लोग शामिल किये जाते हैं।' यदि कोई व्हेल अनजाने में रैंसमवेयर डाउनलोड करता है तो इस बात की अधिक सम्भावना है कि वे मीडिया को सफल हमले की भनक लगने से रोकने के लिए फिरौती का भुगतान करेंगे और अपनी प्रतिष्ठा के साथ–साथ जिस कम्पनी के लिए वे काम करते हैं उसकी भी साख को बचाने के लिए कुछ भी करने को तैयार हो जायेंगे जो किसी भी तरीके से उचित नहीं है।

- **पासवर्ड अटैक–** हम सभी इस बात से सहज ही सहमत होंगे कि कठिन अनुमान लगाने योग्य पासवर्ड बनाना कितना महत्त्वपूर्ण है। QWERT, 12345, जन्मतिथि, नाम, स्थान आदि से सम्बन्धित पासवर्ड सुरक्षा के लिहाज से पर्याप्त नहीं है। 'हैकर्स पीड़ित के पासवर्ड का अनुमान लगाने के लिए उपयोगकर्ता के नाम और पासवर्ड जैसे विभिन्न चुराए गए क्रेडेंशियल्स का उपयोग करते हैं।' एक बार जब उनके पास आपका पासवर्ड आ जाता है तो वे सभी प्रकार की दुर्भावनापूर्ण कार्यवाही करने में सक्षम हो जाते हैं। दूसरी एक और बात यह है कि आजकल फोन पे, गूगल पे, इस्टाग्राम, फेसबुक, ए0टी0एम0, ट्विटर आदि इतने सोशल मीडिया प्लेटफार्मों के पासवर्ड याद रखना आसान नहीं है ऐसे में लोग कभी–कभी मोबाइल में लिखकर सेव कर लेते हैं एवं ए0आई0 आ जाने से आपकी पसन्द–ना–पसन्द सब पर नजर रखकर आपको हैक या ट्रैक करना आसान हो जाता हे जो कि आने वाले समय में और भी खतरनाक साबित हो सकता है क्योंकि बात सिर्फ पासवर्ड की नहीं है आजकल डिजीलॉकर जैसे एप्लीकेशन भी हैं जिसमें हमारे सारे दस्तावेज मौजूद रहते हैं यानि सारी चीजें ऑनलाइन रखना व्यक्ति की जरूरत एवं मजबूरी दोनों है। अतः इस पर विशेष रूप से ध्यान देने की जरूरत है।

- **डी0एन0एस0 स्पूफिंग–** डी0एन0एस0 का मतलब डोमेन नेम सिस्टम है। स्पूफिंग वह है जहाँ एक साइबर हमलावर 'स्पूफ्ड' वेबसाइट पर ट्रैफिक भेजने के लिए डी0एन0एस0 रिकार्ड को बदल देता है। डी0एन0एस0 स्पूफिंग का उपयोग एक नकली वेबसाइट बनाने के लिए भी किया जा सकता है जो किसी कम्पनी की वैध वेबसाइट के समान दिखती है लेकिन इसमें प्रतिष्ठा को धूमिल करने व नुकसान पहुँचाने के उद्देश्य से भड़काऊ सामग्री होती है। नकली वेबसाइट के झाँसे में आकर लोग अपनी वास्तविक जानकारी तक पहुँच प्रदान कर सकते हैं जिससे हैक होने की सम्भावना बढ़ जाती है।

- **ड्राइव–बाय डाउनलोड–** अधिकांश साइबर हमलों के लिए उपयोगकर्ता से सहभागिता की आवश्यकता होती है–जैसे किसी लिंक आदि पर क्लिक करना या अनुलग्नक डाउनलोड करना। ड्राइव–बाय डाउनलोड नहीं होते बल्कि वे दूषित वेबसाइटों को ब्राउज करते समय या भ्रामक पॉप–अप विंडो से जुड़ते समय बिना सोचे–समझे उपयोगकर्ताओं को संक्रमित कर सकते हैं।

- **एस0क्यू0एल0 इंजेक्शन हमले–** स्ट्रक्चर्ड क्वेरी लैंग्वेज (SQL) इंजेक्शन उन वेबसाइटों का लाभ उठाने का एक सामान्य तरीका है जो अपने उपयोकर्ताओं को सेवा देने के लिए डेटाबेस पर निर्भर है। क्लाइंट वे कम्प्यूटर होते हैं जो सर्वर से जानकारी प्राप्त करते हैं और एक एस0क्यू0एल0 हमला क्लाइंट से सर्वर पर डेटाबेस में भेजी गई एस0क्यू0एल0 क्वेरी का उपयोग करता है। 'कमांड को डेटा प्लेन में किसी अन्य चीज के स्थान पर डाला जाता है या 'इंजेक्ट' किया जाता है, जो सामान्य रूप से वहाँ होती है जैसे कि पासवर्ड या लॉगिन।' सर्वर जो डेटाबेस रखता है फिर कमांड चलाता है और सिस्टम में प्रवेश हो जाता है। यदि एस0क्यू0एल0 इंजेक्शन सफल होता है तो कई चीजें हो सकती है, जिसमें संवेदनशील डेटा जारी करना या महत्त्वपूर्ण डेटा को संशोधित करना या हटाना शामिल है।

- **वेब हमलें–** वेब हमलों से तात्पर्य उन खतरों से है जो वेब–आधारित अनुप्रयोगों में कमजोरियों को लक्षित करते हैं। हर बार जब आप किसी वेब एप्लिकेशन में जानकारी दर्ज करते हैं, तो आप एक कमांड शुरू कर रहे होते हैं जो एक प्रतिक्रिया उत्पन्न करता है। उदाहरण के लिए यदि आप ऑनलाइन बैंकिंग एप्लिकेशन का उपयोग करके किसी पैसे भेज रहे हैं, तो आपके द्वारा दर्ज किया गया डेटा एप्लिकेशन को आपके खाते में जाने, पैसे निकालने और किसी और के खाते में भेजने का निर्देश देता है हमलावर इस प्रकार के अनुरोधों के ढाँचे के भीतर काम करते हैं और अपने लाभ के लिए उनका उपयोग करते हैं। कृत्रिम बुद्धिमत्ता के गलत इस्तेमाल करके इसे और भी आसान बनाया जा सकता है जो किसी भी तरीके से मानवता के हित में नहीं है।

इस प्रकार देखा जाय तो अपराध पहले से ही व्याप्त रहे हैं जब से इस तकनीकि क्रान्ति की शुरूआत हुई एवं जैसे–जैसे तकनीके स्मार्ट होती गई चोरी एवं अपराध करने का तरीका भी स्मार्ट होता गया। कृत्रिम बुद्धिमत्ता एक कदम आगे की सोच रखने वाली तकनीकि है इसलिए आज के ए0आई0 युग में साइबर खतरों की प्रकृति एवं प्रवृत्ति तेजी से बदल एवं बढ़ रही है। इस पर अगर प्रभावी अंकुश नहीं लगाया गया तो आने वाले समय में यह और भी घातक सिद्ध हो सकती है।

जहाँ तक बात भारत की है तो भारत को अपने विशिष्ट सामाजिक–आर्थिक संदर्भ के कारण कई अन्य विशिष्ट साइबर चुनौतियों का सामना करना पड़ता है। भारत में व्याप्त डिजिटल विभाजन, खंडित साइबर सुरक्षा बुनियादी ढाँचा, डाटा गोपनीयता सम्बन्धी लचीली व्यवस्था, कौशल एवं प्रशिक्षण की कमी, कानूनों का प्रभावी रूप से लागू न हो पाना, अशिक्षा, गरीबी आदि बहुत सारे ऐसे कारण हैं जो भारत को इस दिशा में विशेष रूप से चिंतन करने के लिए विवश करते हैं।

उपरोक्त वर्णित समस्यायें एकाएक हल होने वाली नहीं है, चाहे कितना भी कठोर साइबर कानून बना दिया जाय साइबर हमलें एकदम से नहीं रूक सकते हैं। हाँ जनजागरूकता बढ़ाकर, डिजिटल साक्षरता पर काम करके एक मजबूत सुरक्षा तंत्र का विकास आदि कुछ निम्नलिखित वर्णित कदमों द्वारा साइबर हमलों को सफल होने से रोका जा सकता है या प्रभावी अंकुश लगाया जा सकता है। साइबर सुरक्षा चुनौतियों से सम्बन्धित प्रमुख समाधानों का वर्णन निम्नलिखित है–

- एक मजबूत साइबर सुरक्षा पारिस्थितिकी तंत्र का निर्माण इसमें सी0ई0आर0टी0 (इंडियन कम्प्यूटर इमरजेंसी रिस्पांस टीम–CERT-In) इन जैसी सरकारी योजनाओं को मजबूत बनाना, सार्वजनिक–निजी भागीदारी को बढ़ावा देना और हितधारकों के बीच सहयोग को बढ़ावा देना शामिल है।

- ए0आई0–संचालित साइबर सुरक्षा समाधानों में निवेश को बढ़ावा दिया जाना चाहिए क्योंकि जब एक ऐसी समय में जहाँ कृत्रिम बुद्धिमत्ता से सम्बन्धित तकनीकों का दुरूपयोग बढ़ता जा रहा है तो ऐसे में इसमें सक्रिय खतरों का पता लगाने और प्रतिक्रिया करने की भी अपार सम्भावनाएँ हैं। ऐसे में सुरक्षित ए0आई0 समाधानों के अनुसंधान और विकास में निवेश करना महत्त्वपूर्ण है।

- जहाँ भारत में पहले से इतनी अशिक्षा एवं गरीबी व्याप्त है ऐसे में डिजिटल साक्षरता और जागरूकता को बढ़ावा देना अपने आप में एक चुनौतीपूर्ण कदम है लेकिन एक लचीले डिजिटल समाज के निर्माण के लिए साइबर स्वच्छता, ऑनलाइन घोटालों और डाटा गोपनीयता प्रथाओं के बारे में जनता को शिक्षित करना आवश्यक है।

- भारत जैसे देश में एक मजबूत कानूनी ढाँचा विकसित करना अति आवश्यक है जिससे साइबर अपराध पर प्रभावी अंकुश लगाया जा सके। यहाँ दिन–प्रतिदिन अपराधों की तकनीकि और प्रवृत्ति बदलती एवं बढ़ती जा रही है एवं अपराध करने का तरीका लगातार स्मार्ट होता जा रहा है वहाँ महत्वपूर्ण बुनियादी ढाँचे की रक्षा करने और डाटा गोपनीयता सुनिश्चित करने के लिए मजबूत साइबर सुरक्षा कानूनों एवं विनियमों की आवश्यकता है।

- साइबर अपराध से सम्बन्धित कानून बना देना एवं उन्हें प्रभावी तरीके से लागू करवा देना यह साइबर सुरक्षा के लिहाज से तात्कालिक कदम पर्याप्त नहीं है। 'दीर्घकालिक समाधानों को ध्यान में रखते हुए साइबर सुरक्षा प्रशिक्षण और कौशल विकास में निवेश अति महत्वपूर्ण है।'' अच्छी बात यह है कि आजकल की युवा आबादी आई0टी0 सेक्टर की तरफ आकर्षित भी हो रही है।

- साइबर हमलों के प्रभाव एवं सम्भावना को कम करने के लिए घर, कार्यालय, व्यक्तिगत उपयोग आदि में आने वाले इलेक्ट्रॉनिक उपकरणों को हमेशा अद्यतन रखना चाहिए क्योंकि अपडेट पुराने संस्करणों की सुरक्षा खामियों को ठीक कर देते हैं। इसके अलावा हमें नवीनतम पीढ़ी के एंटीवायरस सॉफ्टवेयर भी समय–समय पर इंस्टॉल करते रहना चाहिए।

- हम दैनिक जीवन में पासवर्ड वाली जितनी भी चीजों का इस्तेमाल करते हैं उसमें पासवर्ड हमेशा लम्बे और जटिल रखना चाहिए जिसमें संख्याओं, प्रतीकों, बड़े एवं छोटे अक्षरों आदि का उपयोग करना चाहिए एवं इसको हमेशा गुप्त एवं सुरक्षित रखे तथा कोशिश करें कि हर जगह लिखकर रखने की आदत से बचें। एक बात का और ख्याल रखना चाहिए कि हमेशा एक ही पासवर्ड का उपयोग नहीं करना चाहिए इसे समय–समय पर बदलते रहना चाहिए।

- इलेक्ट्रॉनिक उपकरणों पर आने वाले लिंक, प्रोफाइल, वेबसाइट आदि की प्रमाणिकता जाँच कर ही उस तक पहुँच सुनिश्चित करें। फिशिंग, मैलवेयर दो सबसे आम साइबर हमले, संवेदनशील जानकारी तक पहुँचने के लिए धोखाधड़ी वाले लिंक का उपयोग करते हैं। सोशल नेटवर्क पर फर्जी प्रोफाइल मिलना आम बात है जिसका मकसद खुद को कम्पनी का बताकर डेटा एवं संवेदनशील जानकारियाँ चुराना होता है। इस संदर्भ में किसी भी स्थिति में व्यक्तिगत जानकारी साझा करने से बचना चाहिए चाहे सामने से कितनों लालच भरे ऑफर क्यों न दिये जाए।'

- जब भी आपको लगे कि आपने किसी संदिग्ध या अनुचित सामग्री वाली वेबसाइट या लिंक तक पहुँच प्राप्त कर ली है एवं अब यह आपके लिए जोखिम पैदा कर सकता है तो ऐसे में अधिकृत वेबसाइट से ही टोल फ्री नम्बर लेकर मदद माँगे एवं सक्षम अधिकारी को तुरन्त रिपोर्ट करें।

- फायरवॉल का उपयोग करना भी साइबर हमलों के बचाव का एक शुरूआती तरीका हो सकता है। 'फायरवॉल कम्प्यूटर एवं इंटरनेट के बीच पहली सुरक्षा सेतु के रूप में कार्य करता है।' ये लगातार चलने वाले नेटवर्क ट्रैफिक की निगरानी करते हैं और पूर्व निर्धारित नियमों के आधार पर यह निर्धारित कर सकते हैं कि किस ट्रैफिक को ब्लॉक करना है एवं किसको आगे जाने की अनुमति देना है।

- हैक होने की सम्भावना को कम करने के लिए मल्टीफैक्टर प्रमाणीकरण सक्षम करें एवं डेटा का हमेशा बैकअप रखें ताकि ऐसी आपातकालीन स्थिति में हैक के प्रभाव को जितना न्यूनतम किया जा सके बेहतर है जैसे एकाउंट ब्लाक या स्थिर (फ्रीज) करना आदि।

- कोई भी चीज सर्च करते समय या किसी भी वेबसाइट तक पहुँच सुनिश्चित करने के लिए हमेशा सुरक्षित वेब ब्राउजिंग का ही इस्तेमाल करें। यह सुनिश्चित करने के लिए कि सुरक्षित ब्राउजर कौन सा है, ब्राउजर के खोज बार में यू0आर0एल0 के बगल में एक लॉक पैडलॉक आइकन देखें। यह इंगित करता है कि वेबसाइट के पास वैध एस0एस0एल0 प्रमाण–पत्र और भ्ज्ज्ै प्रोटोकॉल है।

- जब भी सार्वजनिक वाई–फाई स्रोत का उपयोग किया जाए यहाँ तक कि अपना ईमेल भी जाँचा जाए तो डाटा सुरक्षा के लिए वी0पी0एन0 का उपयोग किया जाना चाहिए।

- सोशल मीडिया पर सब कुछ साझा करने (Over Sharing) से बचे। ऑनलाइन साझा की गई हर चीज उपयोगकर्ता के डिजिटल फुटप्रिंट का हिस्सा बन जाती है, जिसका उपयोग हैकर्स पासवर्ड और सुरक्षा प्रश्नों के सुराग का पता लगाने या सोशल इंजीनियरिंग हमले शुरू करने के लिए करेगें।

- सीमा–पार साइबर अपराधों से निपटने के लिए अंतर्राष्ट्रीय एजेंसियों और कानून प्रवर्तन के साथ सहयोग स्थापित किया जाना चाहिए।

- बच्चों को इंटरनेट के उपयोग के जोखिमों के बारे में शिक्षित करें और उनकी गतिविधियों पर नजर रखें क्योंकि इस मामले में बचे सॉफ्ट टारगेट होते हैं।

- भारत को सरकारी और निजी क्षेत्र के प्रतिभागियों के साथ एक साइबर सुरक्षा बोर्ड की स्थापना करनी चाहिए।

ए0आई0 के युग में साइबर सुरक्षा के लिए सामूहिक प्रयास की आवश्यकता है। सरकारी, निजी क्षेत्र, शिक्षा जगत और नागरिक समाज को एक मजबूत साइबर सुरक्षा पारिस्थितिकी तंत्र बनाने, जिम्मेदार ए0आई0 विकास को बढ़ावा देने और व्यक्तियों को डिजिटल दुनिया में सुरक्षित रूप से नेविगेट करने के लिए सशक्त बनाने के लिए एक साथ आना चाहिए।

जैसा कि भारत वैश्विक मंच पर एक डिजिटल नेतृत्वकर्ता बनने की आकांक्षा रखता है, अतः संवेदनशील जानकारी की सुरक्षा और मजबूत साइबर सुरक्षा उपायों को सुनिश्चित करना सर्वोपरि है। हाल के डेटा उल्लंघन के मामले सरकार के लिए तेजी से कार्य करने, व्यापक रणनीतियों को लागू करने और अपने नागरिकों को डिजिटल क्षेत्र में बढ़ते खतरों से बचाने के लिए सक्रिय संचार में शामिल होने की महत्त्वपूर्ण आवश्यकता पर जोर देते है। डिजिटल इंडिया लक्ष्य को प्राप्त करने के लिए साइबर सुरक्षा और डेटा सुरक्षा में वर्तमान कमियों को दूर करने के लिए एक ठोस प्रयास की आवश्यकता है।

इंटरनेट का उपयोग करने वाले लोगों की संख्या हर दिन बढ़ती जा रही है, दूसरी ओर साइबर स्पेस में अपराध भी तेजी से बढ़ रहे हैं। साइबर अपराध पर प्रभावी अंकुश लगाने के लिए सरकार, व्यवसायों, शैक्षणिक संस्थानों और व्यक्तियों सहित विभिन्न हितधारकों को ठोस प्रयास करने की आवश्यकता है। भारत में इन अपराधों से प्रभावी ढंग से निपटने के लिए साइबर सुरक्षा बुनियादी ढाँचे को मजबूत करना, जागरूकता बढ़ाना, प्रभावी साइबर सुरक्षा उपायों को लागू करना और सार्वजनिक और निजी क्षेत्रों के बीच सहयोग को बढ़ावा देना आवश्यक है।

निष्कर्ष

इस प्रकार हम कह सकते हैं कि विभिन्न रणनीतियों को लागू करके तथा एक सक्रिय और सहयोगात्मक दृष्टिकोण को अपनाकर, भारत ऑनलाइन अपराधों को काफी हद तक कम कर सकता है और अपने नागरिकों एवं व्यवसायों के लिए एक सुरक्षित डिजिटल वातावरण बना सकता है। अलग–अलग चुनौतियों का समाधान करके और ए0आई0 की क्षमता का लाभ उठाकर भारत अपने नागरिकों के लिए एक सुरक्षित और समृद्ध डिजिटल भविष्य सुनिश्चित कर सकता है। इस पर प्रभावी अंकुश लगाया जाना इसलिए भी जरूरी है क्योंकि यह व्यक्तिगत रूप से नागरिकों के साथ–साथ देश के लिए भी सुरक्षा सम्बन्धी खतरा खड़ा करता है। सरकार ने तो 2013 में ही राष्ट्रीय साइबर सुरक्षा नीति ला दी थी और लगातार इससे सम्बन्धित कानूनों में समय के हिसाब से बदलाव भी किया जा रहा है लेकिन जब तक प्रत्येक नागरिक व्यक्तिगत रूप से जागरूक व सतर्क होकर इससे बचने के उपाय नहीं अपनायेगा तब तक कितनी भी काननू ला दिये जाये साइबर अपराध पर प्रभावी अंकुश नहीं लगाया जा सकेगा।

संदर्भ ग्रन्थ सूची

1. Bhushan Mayank; Fundamental of Cyber Security, BPB Publication, 2021.
2. Dan, Patterson; Introduction to Artificial Intelligence and Expert System, Pearson Publication, 2015.
3. Joshi, Prachi; Artificial Intelligence: Building Intelligent Systems, PHI Learning Publication, New Delhi, 2023.
4. Khatana, Rohit; Introduction to Cyber Security, Notion Press Publication, 2021.
5. Kissinger, Henry; the Age of AI: And Our Human Future, John Murray Publication, 2022.
6. Malhotra, Rajiv; Artificial Intelligence and the future of Power, Rupa Publication, 2021.
7. Mishra, Jai Prakash; Cyber Vidhi-Ek Parichay, Central Law Publication, 2022.
8. Muralidharan, K.M.; Law of Cyber Crime in India, Asia Law House Publication, 2023.
9. Norving, Peter; Artificial Intelligence: A Modern Approach, Pearson Publication, 2022.
10. Pokhariyal, Purvi; Artificial Intelligence: Law and Policy Implication, Eastern Book Company Publication, 2022.
11. Sharma, Sunil Kumar; Artificial Intelligence: Ek Adhyayan, Vani Prakashan, 2024.
12. Singh, Tanigh; the Art of Artificial Intelligence, Blurose Publication, 2023.
13. Stuart, Russell; Human Compatible: AI and the Problem of Control, Penguin Publication, 2020.
14. Yojana Magazine.
15. Kurukshetra Magazine.
16. The Hindu.
17. Time of India.
18. Science Reporter Magazine.
19. Website-https://cisco.com
20. Website-https://www.itgovernance.co.uk.
21. Website-https://www.ncsc.gov.uk.
22. Website-https://www.ibm.com
23. Wesbite-https://www.nist.gov.