International Journal of Sociology and Political Science
www.sociologyjournal.in
Online ISSN: 2664-7745, Print ISSN: 2664-7737
Received: 27-09-2025, Accepted: 26-10-2025, Published: 11-11-2025
Volume 7, Issue 4, 2025, Page No. 64-67

भारत की साइबर सुरक्षा में कृत्रिम बुद्धिमत्ता (एआई) की प्रासंगिकता

वीरेंद्र कुमार
शोध छात्र, रक्षा एवं स्त्रातेजिक अध्ययन विभाग, इलाहाबाद विश्वविद्यालय, श्यामा प्रसाद मुखर्जी डिग्री कॉलेज, प्रयागराज, उत्तर प्रदेश, भारत

सारांश
आज की तेजी से बदलते डिजिटल परिवेश में कृत्रिम बुद्धिमत्ता ने कई क्षेत्रों में क्रांति ला दी है साथ ही सूचना प्रौद्योगिकी के इस युग में साइबर सुरक्षा पर इसका प्रभाव गहरा रहा है। यह शोध पत्र आर्टिफिशियल इंटेलिजेंस में हुई प्रगति और साइबर सुरक्षा में एआई की भूमिका एवं उभरती चुनौतियों के समाधान का अन्वेषण करता है। यह एआई की उपयोग से मिलने वाले लाभ एवं उससे जुड़ी चिताओं को उजागर करता है। इसके अतिरिक्त यह पत्र साइबर सुरक्षा में एआई से जुड़े संभावित जोखिम और सरकारी प्रयासों और नीतियों पर भी चर्चा करता है। वर्तमान शोध प्राथमिक एवं द्वितीय स्रोतों के विश्लेषण एवं केस स्टडी के माध्यम से भारत की साइबर सुरक्षा एवं कृत्रिम बुद्धिमत्ता की प्रासंगिकता को उल्लेखित करता है।

मूल शब्दः साइबर सुरक्षा, कृत्रिम बुद्धिमत्ता, साइबर खतरे, मशीन लर्निंग

प्रस्तावना

आज डिजिटल युग का दौर है। जिसमें हमारे फोन, बैंक, दफ्तर स्कूल और सरकारी काम काज भी इंटरनेट से जुड़े हैं। लगभग सभी कार्य ऑनलाइन होने के कारण हमारी सुरक्षा चिंता और बढ़ गई है, जिससे कि साइबर अपराध, डाटा चोरी, हैकिंग और फेक न्यूज़ जैसे खतरे अब आम बात हो गए हैं। ऐसे समय में कृत्रिम बुद्धिमत्ता (एआई) एक नई उम्मीद बनकर सामने आई है। यह एक ऐसी तकनीकी है जो कंप्यूटर को इंसान की तरह सोचने और सीखने की क्षमता देती है। साइबर सुरक्षा में इसका इस्तेमाल खतरे को पहचानने, रोकने और जल्दी प्रतिक्रिया देने के लिए किया जा रहा है। साइबर सुरक्षा में एआई, मशीन लर्निंग एल्गोरिथम और व्यावहारिक विश्लेषण का लाभ उठाकर विशाल डाटा सेट में पैटर्न और विसंगतियों को उजागर कर सकता है। जिससे ज्ञात और पहले से अनदेखी दोनों तरह के खतरों की पहचान संभव हो पाती है। इसका सक्रिय दृष्टिकोण संगठनों को त्वरित और प्रभावी प्रतिक्रिया देने में सक्षम बनाता है। जिससे संभावित खतरों को गंभीर नुकसान पहुंचाने से पहले ही कम किया जा सकता है। [1]

साइबर हमलों के जवाब में एआई की क्षमता बड़े डेटा ऐतिहासिक घटनाओं और निरंतर सीख के साथ खतरों का पता लगाने और उनकी रोकथाम में मनुष्य से कहीं आगे निकल गई है। [2] कृत्रिम बुद्धिमत्ता (एआई) मशीनों में मानवीय बुद्धिमता का अनुकरण एवं व्यवहार शामिल है। जिसमें तर्क करने और इस तरह कार्य करने की क्षमता जो दिए गए उद्देश्यों तक पहुंचने की संभावना को अधिकतम करती है आई एक ऐसी तकनीक है जो डाटा पैटर्न देखकर समझती है, गलतियों से सिखाती है और खुद निर्णय लेती है। [3] इसके अलावा एआई की संभावनाओं में भेद्यता विश्लेषण भी शामिल है। एआई संचालित, स्वचालित स्कैनिंग और पेनिट्रेशन परीक्षण सिस्टम नेटवर्क और अनुप्रयोगों में खामियों का प्रभावी ढंग से पता लगा सकते हैं। पिछले कुछ वर्षों में एआई ने वैश्विक स्तर पर अपना गहरा प्रभाव बना लिया है, ऐसे में साइबर अपराधी भी लोगों को फंसाने के लिए अब एआई का इस्तेमाल कर रहे हैं। हाल ही में चेक प्वाइंट सॉफ्टवेयर टेक्नोलॉजी रिपोर्ट से यह पता चला है कि इस स्कैमर्स मजबूत मालवेयर बनाने के लिए एआई का इस्तेमाल कर रहे हैं जो कि साइबर सुरक्षा के लिए एक खतरा है। इस प्रकार एआई का एक दोहरा स्वरूप दिखाई पड़ता है। रक्षा के संदर्भ में एआई आधारित टूल्स से एनामली डिटेक्शन, ऑटोमेटेड इंसीडेंट रिस्पांस व क्लाउड और आईओटी सुरक्षा में भारी लाभ मिलता है। इसके विपरित साइबर अपराधी भी एआई की मदद से अत्यधिक फिशिंग मालवेयर और फ्रॉड हमलों को अंजाम दे रहे हैं जिससे पारंपरिक सुरक्षा उपाय कमजोर हो रहे हैं। [4]

भारत का साइबर सुरक्षा परिदृश्य एवं आर्टिफिशियल इंटेलिजेंस (एआई)

भारत में साइबर सुरक्षा एवं आर्टिफिशियल इंटेलिजेंस (एआई) का उपयोग तेजी से बढ़ रहा है। जिसमें न केवल साइबर अपराध से निपटने की क्षमता बढ़ी है बल्कि डिजिटल इंफ्रास्ट्रक्चर सुरक्षित करने में भी नई संभावनाएं खुल गई है। भारत में जिस गति से डिजिटल सेवाओं का दायरा बढ़ा है उसी गति से साइबर हमलों का जोखिम भी बढ़ा है। नेक्स्टजेन एग्जीबिशन की रिपोर्ट के अनुसार वर्ष 2024 में साइबर सुरक्षा की 23 लाख मामले सामने आए हैं जिसमें हमलों के कारण 1200 करोड़ की संपत्ति का नुकसान हुआ है। अमेरिका और रूस के बाद भारत दुनिया की तीसरा देश है जहां सर्वाधिक साइबर हमले होते हैं। [5]

साइबर अपराध के मामलों में एनसीआरबी की रिपोर्ट के अनुसार वर्ष 2024 में बैंकिंग धोखाधड़ी फिशिंग रेनसमवेयर हमले और डाटा चोरी की घटनाएं ज्यादा रही है। वर्ष 2024 में साइबर अपराध के लगभग 36.37 लाख मामले दर्ज हुए जो 2023 के 24. 42 मामलों की तुलना में काफी अधिक है। [6] इस वर्ष भारत ने साइबर अपराधों में लगभग 22,845 करोड़ का वित्तीय नुकसान उठाया है जो वर्ष 2023 में 7.465 करोड़ के मुकाबले लगभग 206 प्रतिशत की बढ़ोतरी है। साइबर अपराधों के मामलों में कर्नाटक 21889, तेलंगाना 18236, उत्तर प्रदेश 10794 शीर्ष राज्य शामिल है। इस रिपोर्ट के अनुसार 2024 में 1.91 लाख साइबर अपराध की शिकायतें दर्ज हुई जबकि 2023 में यह संख्या लगभग 1.5 लाख थी। एआई ड्रिवन साइबर क्राइम और डिजिटल अरेस्ट जैसी नई चुनौतियां सामने आई है जैसे कि अपराधी अब एआई का उपयोग करके फर्जी कॉल मैसेज भेजते हैं, पहचान छेड़छाड़ करते हैं और डिजिटल गिरफ्तारी की धमकी देकर आम जनता को फसाते हैं। [7]

एआई आधारित समाधानों को विकसित करने और बढ़ावा देने के लिए "इंडिया एआई साइबर गार्ड एआई" जैसी पहले शुरू की गई। जिनका उद्देश्य साइबर धोखाधड़ी और अपराधों को कम

करने के लिए उन्नत एआई प्रणाली विकसित करना है। एआई की मदद से साइबर अपराधों में तेजी से पहचान (एमटीटीडी) और प्रतिक्रिया (एमटीटीआर) क्षमता बढ़ाई जा रही है। जिससे हमलावरों को रोकने और हमलों का सामना करने में सफलता मिल रही है। [8] उदाहरण के रूप में आरबीआई का मिलहंटर एआई जैसे डीप लर्निंग मॉडल का उपयोग मल्टीलेयर्ड साइबर हमलों को रोकने के लिए किया जा रहा है। एआई संचालित सक्रिय खतरे की पहचान से ऐपीटी और जीरो डेज एक्सप्लोइट्स का प्रभावी रूप से नियंत्रित किया जा रहा है। [9]

भारत की राष्ट्रीय सुरक्षा परिषद सचिवालय (एनएससीएस) द्वारा आयोजित प्रमुख राष्ट्रव्यापी साइबर सुरक्षा अभ्यास "भारत एनसीएक्स नक्स 2025" का लक्ष्य वास्तविक दुनिया के जटिल साइबर अपराध हमलों को नकल कर सरकारी रक्षा और महत्वपूर्ण अवसंरचना की जवाबी क्षमताओं का मजबूत करना है। इसमें एआई संचालित मालवेयर डीपफेक और एपीआई सुरक्षा से जुड़े खतरों पर विशेष ध्यान दिया गया है। इस अभ्यास का उद्देश्य भारत की साइबर ऑपरेशन तैयारी को बढ़ाना और राष्ट्रीय डिजिटल संप्रभुता को सुनिश्चित करना है। [10]

साइबर सुरक्षा में आर्टिफिशियल इंटेलिजेंस (एआई) की भूमिका

वर्तमान समय में इंटरनेट हमारी जिंदगी का एक अहम हिस्सा बन चुका है। भारत डिजिटल बनने की दिशा में बहुत तेजी से आगे बढ़ रहा है जैसे डिजिटल इंडिया, यूपीआई, ई गवर्नेंस और ऑनलाइन शिक्षा जैसे पहलों ने लोगों को इंटरनेट से जोड़ दिया है। तकनीकी ने हमारे कार्यों को जितना आसान कर दिया है उतना खतरे भी बढ़ा दिया हैं। साइबर अपराधी अब पहले से ज्यादा स्मार्ट हो गए हैं और इसके आपराधिक गतिविधियां पहले की तुलना में कहीं अधिक जटिल हो गए हैं। ऐसे में पारंपरिक सुरक्षा उपाय जैसे पासवर्ड, एंटीवायरस, फायरवॉल अब प्रासंगिक नहीं रहे। अब हमें ऐसी तकनीकी चाहिए जो खुद सोचें खतरों को पहले से पहचाने और तुरंत जवाब दे सके। यही काम कृत्रिम बुद्धिमत्ता (एआई) कर रही है। एआई के एकीकरण से साइबर सुरक्षा में महत्वपूर्ण परिवर्तन आया है जो इस प्रकार है–

- **खतरे की पहचान और रोकथाम:** एआई संचालित सिस्टम किसी नेटवर्क या डिवाइस की हर गतिविधियों पर नजर रखते हैं जैसे ही कोई असामान्य व्यवहार होता है उदाहरण के रुप में अचानक बहुत ज्यादा डाटा ट्रांसफर होना, लॉगिन पैटर्न और सिस्टम फाइलों में छेड़छाड़ एआई तुरंत अलर्ट कर देता है। एआई आधारित साइबर सुरक्षा प्रणालियों में नेटवर्क ट्रेफिक सिस्टम लॉग्स उपयोगकर्ता व्यवहार, असामान्य पैटर्न और खतरें खोजने में सक्षम होता है। जैसे कोई फिशिंग ईमेल गलती से क्लिक हो जाता है तो एआई त्वरित रूप से व्यवहार में बदलाव को पहचान कर खतरे की सूचना देता है। एआई वास्तविक समय में घटनाओं का पता लगाने और बृहद डेटा विश्लेषण करने की क्षमता के कारण यह सुरक्षा उल्लंघन का शीघ्रता से पता लगा सकता है और उन पर कार्यवाही कर सकता है। [11]

- **पूर्वानुमान:** विश्लेषण पुरानी डाटा का अध्ययन करके एआई यह अनुमान लगा सकता है कि आगामी हमला किस प्रकार के हो सकते हैं। इससे सुरक्षा के लिए पहले से ही तैयार हो सकते हैं संभावित खतरों के पूर्वानुमान से उनसे होने वाले जोखिम को न्यूनीकरण करना संभव हो जाता है। [12]

- **फिशिंग और स्पैम ईमेल की पहचान:** अधिकतर साइबर हमले ईमेल या मैसेज के जरिए होते हैं एआई ईमेल आधारित लिंक को पढ़कर यह समझ लेता है की कौन सा ईमेल असली है और कौन सा नकली। यदि किसी ईमेल में टाइपिंग पैटर्न, लिंक स्ट्रक्चर या भाषा संदिग्ध है तो एआई उसे तुरंत स्पैम या फिशिंग के रूप में मार्क कर देता है। इसे देखकर यूजर उसे लिंक पर गलती से भी क्लिक नहीं करता है एआई मशीन लर्निंग एल्गोरिदम ईमेल सामग्री और संदर्भ को विश्लेषित कर फिशिंग प्रयासों की पहचान बहुत उच्च सटीकता के साथ करता है। कुछ मशीन लर्निंग तकनीक के 94% तक की पहचान डर के साथ फिशिंग ईमेल को वर्गीकृत कर सकती है। [13]

- **रैनसमवेयर हमले रोकना:** रैनसमवेयर का शाब्दिक अर्थ फिरौती मांगना अर्थात ऐसा वायरस जो आपकी सारी फाइलें लॉक कर देता है और उन्हें खोलने के बदले पैसा मांगता है। एआई सिस्टम फाइलों के व्यवहार को मॉनिटर करता है। यदि कोई फाइल अचानक इंक्रिप्ट होते या जल्दी–जल्दी कॉपी होते देखा है तो तुरंत उसे उसे प्रक्रिया को रोक देता है साथ ही सुरक्षा टीम की प्रक्रिया के लिए भारी संख्या में अलर्ट्स को विश्लेषण करने का बोझ कम करता है और मानव त्रुटि की संभावना घटना है जिससे हमले के प्रभाव को जल्दी और प्रभावी ढंग से नियंत्रित किया जा सकता है। [14]

- **उपयोगकर्ता व्यवहार विश्लेषण:** एआई उपयोगकर्ता और सिस्टम व्यवहार का विश्लेषण कर संभावित अंदरूनी खतरों की पहचान करता है। यह सिस्टम की नियमित गतिविधियों से हटकर व्यवहार को ट्रैक करता है और संदिग्ध गतिविधियों पर अलर्ट देता है। जिससे डेटा सुरक्षा बढ़ती है और इस प्रकार एआई न केवल बाहरी बल्कि आंतरिक खतरों से भी सुरक्षा प्रणाली को मजबूत बनाता है। [15]

- **एंड प्वाइंट सुरक्षा और ऑथेंटिकेशन:** एआई आधारित समाधान और एंड पॉइंट सुरक्षा को बेहतर बनाते हैं जो विशेष रूप से दूरस्थ कार्य के बढ़ने के संदर्भ में महत्वपूर्ण है। यह सिस्टम नियमित व्यवहार के बेसलाइन स्थापित कर डेविएशन को तुरंत पकड़ लेता है। जिससे जीरो डे हमलों और अंजन खतरों का पता चलता है साथ ही आई आधारित कैप्चा, फेस रिकॉग्निशन और फिंगरप्रिंट स्कैन जैसे उन्नत प्रमाणित कारण उपाय लोगों सुरक्षा को बेहतर बनाते हैं। [16]

साइबर सुरक्षा हेतु प्रमुख एआई उपकरण

एआई टूल्स का उपयोग साइबर खतरों का पता लगाने और रोकने के लिए उपयोग में लाया जाता है। एआई और मशीन लर्निंग के इस्तेमाल से नेटवर्क पैटर्न व्यवहार और खतरनाक गतिविधियों का विश्लेषण कर रियल टाइम में खतरों का पता लगते हैं। जिससे सुरक्षा एवं तेजी से बचाव में मदद मिलती है।[17] जो निम्नलिखित है–

1. **एक्यूक्नॉक एआई कोपायलट:** यह रियल टाइम निगरानी, खतरा जानकारी, कमजोरी की पहचान, स्वचालित सुरक्षा नीतियां बनाने और जीरो ट्रस्ट क्लाउड सुरक्षा प्रदान करता है यह कंफीग्रेशन त्रुटियां सुधारना और तीव्र प्रतिक्रिया देना ताकि सुरक्षा का ऑटोमेशन और उत्पादकता बढ़े। [18]

2. **डार्कट्रेस:** मशीन लर्निंग से स्वचालित नेटवर्क पर असामान्य व्यवहार और अनोमाली का पता लगता लगता है लगता है स्वयं प्रतिक्रिया देता है जिस तेजी से खतरों का मुकाबला किया जा सकता है। नेटवर्क और क्लाउड वातावरण में व्यापक सुरक्षा प्रदान करता है।

3. **वेक्ट्रा एआई:** यह नेटवर्क क्लाउड और पहचान अस्तर पर हमला करने वालों की गतिविधियों को जोड़कर उन्हें ट्रैक करता है।

4. **क्लाउड स्ट्राइक फाल्कन:** यह ए आधारित और पॉइंट और खतरा इंटेलिजेंस समाधान जो रियल टाइम में खतरों की पहचान करता है और एसओसी टीमों की रक्षात्मक क्षमता बढ़ाता है। यह क्लाउड और ऑन – प्रीमाइसेस दोनों के लिए उपयुक्त है। [19]

5. **प्लो अल्टो कार्टेक्स: एक्सडीआर:** नेटवर्क एंड प्वाइंट, क्लाउड डाटा को समेकित कर एआई आधारित गाइडेड जांच और खतरा प्रतिक्रिया प्रदान करता है सुरक्षा के साथ जोखिम प्रबंध प्रबंध करता है। [20]

6. **सेंटीनेल वन:** एआई और मशीन लर्निंग का उपयोग करके रियल टाइम डिटेक्शन, रिस्पांस और एंड पॉइंट सुरक्षा प्रदान करता है। क्लाउड वर्कलोड का सुरक्षा प्रबंध करता है।

7. **चेक पॉइंट पॉइंट इनफिनिटी:** नेटवर्क क्लाउड एंड पॉइंट मोबाइल समेत एकीकृत सुरक्षा प्लेटफार्म है। एआई से लैस खतरे पहचान, निवारण और उन्नत सुरक्षा नितियां प्रदान करता है। [21]

साइबर सुरक्षा में एआई की चुनौतियां

वर्तमान समय में खतरे के बढ़ते परिदृश्य को देखते हुए साइबर अपराधी भी एआई का इस्तेमाल करने लगे हैं। जिससे सुरक्षा चिंताएं और बढ़ गयी, इस प्रकार एआई एक दोधारी तलवार होने को दर्शाती है। जहां एक तरफ एआई सुरक्षा सुधारने में मदद करती है वहीं इसके दुरुपयोग से खतरे भी बढ़ जाते हैं। इस प्रकार एआई वर्तमान समय में एक चुनौती के रूप में उभर कर सामने आई है जो निम्नलिखित प्रकार के हैं–

1. **सिस्टम अपडेट की समस्या:** तेजी से विकसित होने वाले साइबर हमलों में एआई का इस्तेमाल करके साइबर अपराधी भी अपने हमलों को और अधिक परिष्कृत बना रहे हैं। जिससे पारंपरिक सुरक्षा उपाय इन हमलों का मुकाबला नहीं कर पाते हैं जैसे हैकर्स एआई का इस्तेमाल फिशिंग, ईमेल, डीपफेक, ऑटोमेटेड हैकिंग आदि।

2. **डाटा प्राइवेसी की समस्या:** एआई को सीखने के लिए बड़े डाटा सेट्स की जरूरत होती है। कई बार यह निजी एवं संवेदनशील डाटा होता है। जिससे प्राइवेसी और कानूनी नियमों का खतरा बढ़ जाता है। जिसे डाटा चोरी और निजी जानकारी के दुरुपयोग का खतरा रहता है।

3. **एआई सिस्टम पर हमले:** प्रशिक्षित साइबर अपराधी एआई मॉडल में बग निकालकर उसे गड़बड़ करने के लिए प्रशिक्षित डेटा में धोखा देते हैं। जिससे एआई गलत निर्णय लेता है और सुरक्षा कमजोर पड़ जाती है। इसे एडवर्सिमल हमला भी कहते हैं। इसमें जब कभी हैकर्स ऐसे इनपुट देते हैं जिससे आई को भ्रम हो जाए और वह गलत निर्णय ले अर्थात वह खतरे को सही रूप से पहचान ही ना पाए।

4. **एआई तकनीक का दुरुपयोग:** साइबर अपराधी सार्वजनिक रूप से उपलब्ध एआई टूल्स का उपयोग करके हानिकारक कोड और फेक संचार बना सकते हैं। जिससे साइबर अपराध आसान हो जाता है। [22]

5. **पारदर्शिता का अभाव:** एआई डाटा के भीतर पैटर्न रुझान और संबंधों की पहचान करने के लिए उपयुक्त है। एआई को प्रशिक्षित होने के बाद इन पैटर्न के आधार पर निर्णय लेना और पहचान करने में सक्षम होता है। जबकि आई प्रणालियों द्वारा उपयोग किए जाने वाले मॉडल पारदर्शी एवं व्याख्या योग्य नहीं होते हैं इससे निश्चित करना असंभव हो जाता है कि एआई मॉडल में पूर्वाग्रह या त्रुटियां हैं। [23]

6. **जागरूकता का अभाव:** जागरूकता के अभाव के कारण कई बार ऐसे प्रोफेशनल बहुत कम मिलते हैं। जिन्हें एआई और साइबर सिक्योरिटी द्वारा दोनों की गहरी समझ हो इसलिए इसे अपनाना चुनौती पूर्ण हो जाता है।

7. **ब्लैक बॉक्स समस्या:** एआई का निर्णय समझ न आना अर्थात कई बार एआई बिना कारण बताएं सिर्फ परिणाम देता है। जिससे साइबर एक्सपर्ट को समझ नहीं आता कि सिस्टम किस आधार पर निर्णय लिया है अर्थात स्रोत की स्रोत की सटीकता का सही पहचान न हो पाना।

सरकारी प्रयास और नीतियाँ

भारत सरकार ने आर्टिफिशियल इंटेलिजेंस और साइबर सुरक्षा से जुड़ी नीतियों को लेकर एक व्यापक योजना तैयार की है। जिसमें एआई को बढ़ावा देने के लिए "इंडिया एआई मिशन" शुरू किया है। जिसमें कई पहले शामिल है जैसे एआई स्टार्टअप को वित्तीय सहायता देना, एआई रिसर्च हब और एक्सीलेंस केंद्र स्थापित करना। एआई को जिम्मेदार व सुरक्षित उपयोगी नीति बनाना। [24] सरकार ने केंद्रीय बजट 2024 –25 के दौरान 1550 करोड रुपए साइबर सिक्योरिटी और एआई प्रोजेक्ट के लिए देने का ऐलान किया है। जिससे एक मजबूत साइबर सुरक्षा ढांचा तैयार कर यूजर्स के डाटा को सुरक्षित करेगी साथ ही एआई में रिसर्च को आगे बढ़ावा मिलेगा। [25]

- नीति आयोग ने नेशनल स्ट्रेटजी फॉर आर्टिफिशियल इंटेलिजेंस नमक दस्तावेज तैयार किया है। जिसमें एआई का समावेशी विकास नवाचार शिक्षा प्रशिक्षण डेटा अवसंरचना नैतिकता आदि आयामो से जोड़ा गया है। इस दस्तावेज में नैतिकता गोपनीयता सुरक्षा को एक विशिष्ट खंड दिया गया है। एआई को "एआई फॉर ऑल" के रूप में अपनाने की कल्पना है। अर्थात यह न केवल बड़े शहरों एवं उद्योगों के लिए हो बल्कि ग्रामीण एवं पिछड़े इलाकों तक भी पहुंचे हो। [26] भारत में अभी तक एआई को लेकर कोई विशेष कानून एवं वैधानिक नियम नहीं है। जो सीधे तौर पर एआई को नियंत्रित करता हो, परंतु एआई के नियमन को दिशा देने के लिए विभिन्न ढांचे तैयार किया जा रहे हैं।
- कृत्रिम बुद्धिमत्ता के लिए राष्ट्रीय रणनीति – जून 2018 – इसका उद्देश्य भारत में एआई के भविष्य को विनियमन के लिए एक मजबूत आधार स्थापित करना है।
- प्रिंसिपल फॉर रिस्पांसिबल एआई (उत्तरदायी एआई के सिद्धांत)– फरवरी 2021– यह विभिन्न क्षेत्रों में नैतिक उत्तरदायी एआई परिस्थितिकी तंत्र के निर्माण के लिए भारत की रोड मैप के रूप में कार्य करते हैं।
- उत्तरदायी एआई के लिए परिचालन सिद्धांत अगस्त 2021 –यह यह एआई के संबंध में नियामक और नीतिगत हस्तक्षेप क्षमता निर्माण और डिजाइन द्वारा नैतिकता को प्रोत्साहित करने की आवश्यकता पर जोर देता है। [27] सरकार ने प्रस्तावित किया कि भविष्य में "डिजिटल इंडिया एक्ट" को अपनाया जाए, जिससे 'एआई जोखिम' और 'हाई रिस्क' एआई सिस्टम को नियंत्रित करने का प्रावधान हो सकते हैं। [28] भारत सरकार का एआई स्टैंडर्ड एंड पॉलिसीज पोर्टल

रखती है जहां एआई संबंधी मानक दिशा निर्देश इत्यादि अपडेट होते रहते हैं।

- cybercrime.gov.in को एआई पोर्टल से जोड़ा गया है। जिस बैंक टेलीकॉम कंपनियों और पुलिस आपस में तालमेल कर सके नकली सिम कार्ड और डिवाइसेज को ब्लॉक करने जैसी पहल भी हुई है, साथ ही पुलिस कर्मियों को डिजिटल सबूत और साइबर अपराध पहचान में प्रशिक्षित करने के लिए "Cy Train" प्लेटफार्म लॉन्च किया गया है। इसके अलावा आईटी एक्ट और डिजिटल पर्सनल डाटा प्रोटक्शन एक्ट 2023 आदि ऑनलाइन प्लेटफॉर्म को जवाबदेही बढ़ाने में मदद करते हैं। [29]
- मार्च 2025 में भारत की पहली डीप फेक डिटेक्शन तकनीक "Vastav AI" लॉन्च की गई,जो एआई जनित वीडियो,चित्र और ऑडियो की पहचान 99% सटीकता से करती है। इसका उपयोग कानून प्रवर्तन और मीडिया संस्थानों द्वारा किया जा रहा है। इसके अलावा CERT-In ने एआई आधारित साइबर खतरा निगरानी और तंत्र विकसित किया है। जो महत्वपूर्ण डिजिटल संपत्तियों की सुरक्षा करता है। निजी क्षेत्र में कंपनियां जैसी रिलायंस जियो और एयरटेल एआई संचालित सिक्योरिटी ऑपरेशन केंद्र स्थापित कर रही है, जो नेटवर्क ट्रेफिक की निगरानी करती है। [30]

निष्कर्ष

भारत के डिजिटल भविष्य को सुरक्षित और मजबूत बनाने में आर्टिफिशियल इंटेलिजेंस एक अमूल्य साधन है। बढ़ते साइबर साइबर खतरों से निपटने के लिए एआई तकनीक की समुचित, नैतिक और सुनियोजित उपयोग से ही संभव है। सरकार उद्योग और शैक्षणिक संस्थाओं को मिलाकर एआई आधारित साइबर सुरक्षा तंत्र विकसित करना होगा। इसके साथ–साथ राष्ट्रीय एवं अंतर्राष्ट्रीय स्तर पर अन्य देशों के साथ रणनीतिक एवं सुरक्षा सहयोग स्थापित कर भारत को सुरक्षित एवं आत्मनिर्भर बनाने में महत्वपूर्ण भूमिका निभाएगी। इस प्रकार एआई के बढ़ते महत्व एवं उपयोगिता को देखते हुए यह राष्ट्रीय अवसंरचना की सुरक्षा में निर्णायक भूमिका निभा रही है। अतः यह कहा जा सकता है कि भारत की साइबर सुरक्षा रणनीति में एआई का समावेश अब विकल्प ही नहीं बल्कि अनिवार्य आवश्यकता है।

सन्दर्भ ग्रंथ–सूची

1. सिंह रोहित 2023 कृत्रिम बुद्धिमत्ता का प्रभाव साइबर सुरक्षा https://ijert.org
2. दास, राम मनोहर और राघव संधाने (2020) साइबर सुरक्षा में कृत्रिम बुद्धिमत्ता https://icacse.org
3. शर्मा, वंदना और दीपक दशरथ राव,(फरवरी 2024) कृत्रिम बुद्धिमत्ता से साइबर सुरक्षा खतरों का पता लगाना विश्लेषण दृष्टिकोण
4. https://hindi.news24online.com/gadgets/ai-powered-malware-emerging-as-threat-in-cyber-security-says-report/920370
5. https://www.livehindustan.com/ncr/new-delhi/story-india-must-invest-in-ai-for-cyber-and-border-security-survey-201753106554087
6. राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी) गृह मंत्रालय https://www.mha.gov.in/en/national-crime-records-bureau-ncrb
7. https://www.livehindustan.com/ncr/new-delhi/story-india-must-invest-in-ai-for-cybe.
8. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2068482
9. https://share.google/JjbwuSr30ODE9IX22r-and-border-security-survey-201753106554087
10. https://bharatncx.in/NCX25.aspx?utm_source=perplexity
11. https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow
12. https://www.geeksforgeeks.org/ethical-hacking/ai-in-cybersecurity
13. Ibid.
14. https://secureframe.com/blog/ai-in-cybersecurity
15. [1] Ibid.
16. [1] https://www.geeksforgeeks.org/ethical-hacking/ai-in-cybersecurity
17. [1] https://accuknox.com/blog/ai-cybersecurity-tools
18. [1] Ibid.
19. [1] Ibid.
20. [1] https://cybermagazine.com/top10/top-10-ai-powered-cybersecurity-solutions
21. [1] https://www.checkpoint.com/cyber-hub/tools-vendors/4-best-ai-cybersecurity-tools-in-2025
22. [1] https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security
23. [1] https://www.checkpoint.com/cyber-hub/tools-vendors/4-best-ai-cybersecurity-tools-in-2025
24. [1] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2178092
25. [1]https://www.tec.gov.in/pdf/Studypaper/AI%20Policies%20in%20India%20A%20status%20Paper%20final.pdf
26. [1] https://www.aajtak.in/technology/tech-news/story/budget-2024-govt-announces-rs-1550-crore-for-cybersecurity-and-ai-projects-ttec-1991539-2024-07-25 https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf
27. [1] https://www.whitecase.com/insight-our-thinking
28. [1] https://iapp.org/resources/article/global-ai-governance-india
29. [1] https://navbharattimes.indiatimes.com/tech/ai-news/india-ai-driven-cyber-fraud-detectionai-watch-global-regulatory-tracker
30. https://www.livehindustan.com/ncr/new-delhi/story-india-must-invest-in-ai-for-cyber-and-border-security-survey-201753106554087