

कृत्रिम बुद्धिमत्ता और साइबर जोखिम परिदृश्य

अवसरों, खतरों और जिम्मेदारियों को समझना

डॉ. संजय मदान
वैज्ञानिक 'ई'

व्यावहारिक कृत्रिम बुद्धि और विश्लेषिकी विभाग



प्रगत संगणन विकास केंद्र, मोहाली



ऐआई और साइबर जोखिम परिदृश्य

आइए मैं एक ऐसी असल स्थिति से शुरुआत करता हूँ जिससे हममें से कई लोग संबंधित हो सकते हैं...

“एक सुबह, एक भारतीय कंपनी में एक कर्मचारी को फ़ोन आता है। फ़ोन करने वाले की आवाज़ बिल्कुल कंपनी के वरिष्ठ अधिकारी जैसी थी - वही आवाज़, वही स्वर, वही अंदाज़।

कॉलर कहता है: ‘यह बहुत ज़रूरी है। एक गोपनीय भुगतान तुरंत जारी करना है। मैं एक सभा में हूँ। इसे अभी करो।’

आवाज़ पर भरोसा करके, कर्मचारी पैसों का भुगतान जारी कर देता है।

बाद में पता चला कि अधिकारी ने कभी कॉल किया ही नहीं। आवाज़ कृत्रिम बुद्धिमत्ता का इस्तेमाल करके बनाई गई थी।

यह कल्पित विज्ञान नहीं है। यह आज का साइबर जोखिम परिदृश्य है।”

कृत्रिम बुद्धिमत्ता हमारी ज़िंदगी को बदल रहा है – लेकिन यह साइबर खतरों को भी बदल रहा है।

आज हमें यह समझने की ज़रूरत है कि ऐआई साइबर रिस्क को कैसे बदलता है, वह भी सरल और व्यावहारिक तरीके से।

यह हमारे लिए क्यों मायने रखता है?

कई अहम कारणों से अब यह पहले से कहीं ज़्यादा मायने रखता है:

- भारत विभिन्न सेवाओं के साथ तेजी से डिजिटाइज़ हो रहा है:
 - डिजिटल भुगतान (यूपीआई) – भारत में रोज़ाना लाखों रुपये का लेनदेन यूपीआई ट्रांज़ैक्शन प्रोसेस होते हैं।
 - आधार-आधारित सेवाएं
 - ऑनलाइन शिक्षा, स्वास्थ्य सेवा, बैंकिंग
- बड़े पैमाने पर डेटा जनरेशन
- डिजिटल प्लेटफॉर्म पर बढ़ती निर्भरता

हम जितने ज़्यादा डिजिटल होते जाएंगे, साइबर जोखिमों का दायरा उतना ही बड़ा होता जाएगा। .

2025 में शीर्ष साइबर खतरे और चलन

- **ऐआई - सक्षम हमले:** 47 प्रतिशत से अधिक संगठन जेनरेटिव ऐआई को एक बड़ी चिंता मानते हैं, क्योंकि यह हमलावरों को ज़्यादा जटिल, मापनीय और निजीकृत फ़िशिंग अभियान बनाने की इजाज़त देता है।
- **रैंसमवेयर हमला और जबरन वसूली:** रैंसमवेयर हमला एक बड़ा खतरा बना हुआ है, जिसमें हमलावर डेटा चुराने और जबरन वसूली पर ध्यान दे रहे हैं।
- **आपूर्ति श्रृंखला शोषण:** हमलावर बड़े, ज़्यादा सुरक्षित नेटवर्क में संध लगाने के लिए सॉफ्टवेयर आपूर्ति श्रृंखला और थर्ड-पार्टी विक्रेताओं को तेज़ी से निशाना बना रहे हैं।
- **पहचान-आधारित हमले:** सूचना चोर मैलवेयर और चोरी हुए आवश्यक प्रमाण में भारी बढ़ोतरी (42 प्रतिशत की बढ़ोतरी), अनधिकृत प्रवेश को बढ़ावा दे रही है।
- **भू-राजनीतिक संघर्ष:** वैश्विक ताकतों से जुड़े लोग साइबर जासूसी को पैसे के मकसद के लिए भी साइबर खतरों को बढ़ावा दे रहे हैं।

कृत्रिम बुद्धिमत्ता क्या है?

कृत्रिम / बनावटी

यह किसी ऐसी चीज़ को बताता है जिसे इंसान ने बनाया या उत्पादित किया हो, न कि जो प्राकृतिक रूप से होती हो, खासकर किसी प्राकृतिक चीज़ की नकल के रूप में।

बुद्धिमत्ता

ज्ञान और कौशल हासिल करने और उन्हें लागू करने की क्षमता को संदर्भित करता है।

कृत्रिम बुद्धिमत्ता (ऐआई) का मतलब उन संगणक प्रणाली से है जो:

- ऐआई प्रणाली आधारित तथ्यों (डेटा) से सीखता है और बड़ी मात्रा में इसका विश्लेषण करता है।
- एकत्रित किये गए पुराने तथ्यों को सीखकर, स्वरूप की पहचान करना
- बिना स्पष्ट प्रोग्रामिंग के अनुमान लगाएं या निर्णय लें।



ऐआई की परिणाम गुणवत्ता निर्भर करती है – तथ्यों (डेटा) की गुणवत्ता और योजना डिज़ाइन की गुणवत्ता क्वालिटी पर

ऐआई के प्रकार

कृत्रिम बुद्धिमत्ता (ऐआई):

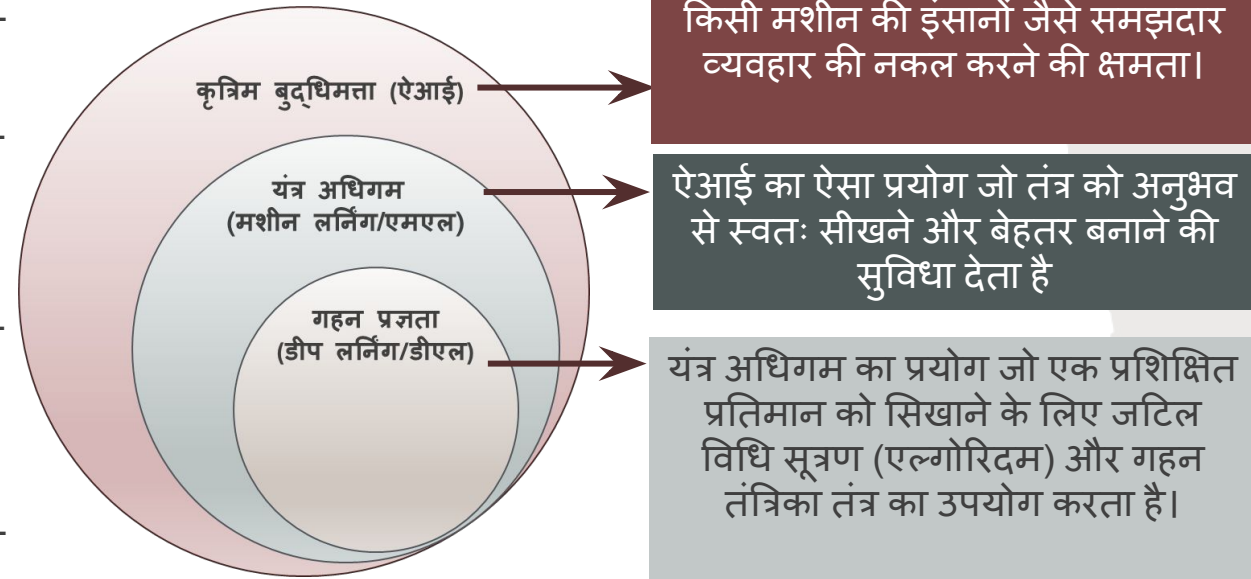
- ऐआई में ऐसी बुद्धिमान मशीनें बनाना शामिल है जो इंसानों जैसे काम करती हैं।
- ऐआई एक व्यापक शब्द है, एमएल और डीएल को इसमें शामिल माना जा सकता है।

यंत्र अधिगम (मशीन लर्निंग / एमएल):

- एमएल एक तरह का ऐआई है जो नियमों और गणितीय प्रतिरूप को इस्तेमाल करके संगणक तंत्र को तथ्यों से सीखने और परिणाम को बेहतर बनाने में मदद करता है।
- उदाहरण के लिए, एक अवांछित छानने का यन्त्र (स्पैम फ़िल्टर), जो यूज़र फ़ीडबैक के आधार पर अवांछित ईमेल की पहचान करना सीखता है।

गहन प्रज्ञता (डीप लर्निंग / डीएल):

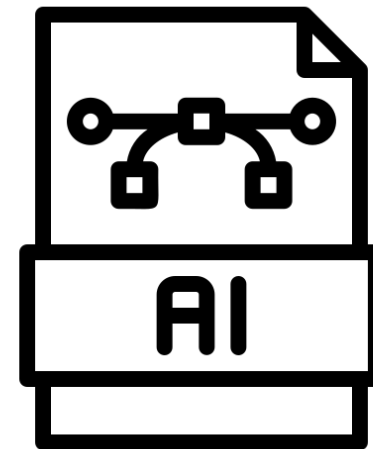
- डीएल एक तरह का एमएल है जो स्वरूप (पैटर्न) खोजने और बड़ी मात्रा में तथ्यों से अनुमान लगाने के लिए गहन तंत्रिका तंत्र (डीप न्यूरल नेटवर्क) का इस्तेमाल करता है।
- उदाहरण के लिए, स्व-चालित कारें, चीज़ों को पहचानने और फैसले लेने के लिए संगणक दृष्टि (कंप्यूटर विज़न) और गहन प्रज्ञता डीप लर्निंग का इस्तेमाल करती हैं।



ऐआई के प्रकार

जनरेटिव ऐआई

- जनरेटिव ऐआई एक तरह का कृत्रिम बुद्धिमत्ता है जो बड़े मौजूदा आंकड़ा समुच्चय (डेटासेट) से स्वरूप सीखकर मूलपाठ (टेक्स्ट), प्रतिकृति (इमेज), कोड, ध्वनि (ऑडियो) और चलचित्र (वीडियो) समेत नवीन प्रकरण बनाता है।
- उदाहरण के लिए, जनरेटिव ऐआई के साइबर सुरक्षा में कई प्रयोग हैं जैसे स्वचालित खतरे का पता लगाना, विसंगति की पहचान के लिए बड़े आंकड़ा समुच्चय का विश्लेषण करना, सुरक्षा घटना पर वास्तविक समय पर प्रतिक्रिया करना।



साइबर सुरक्षा क्या है?

“संगणक, इलेक्ट्रॉनिक संचार तंत्र, इलेक्ट्रॉनिक संचार सेवाएं, तार संचार और इलेक्ट्रॉनिक संचार को नुकसान से बचाना, उसकी सुरक्षा करना और उसे ठीक करना, जिसमें उसमें मौजूद जानकारी भी शामिल है, ताकि उसकी उपलब्धता, ईमानदारी, प्रमाणीकरण, गोपनीयता और गैर-अस्वीकृति सुनिश्चित हो सके।”



साइबर सुरक्षा में ऐआई क्षमताओं का लाभ उठाना

- प्रतिरूप अभिज्ञान, विसंगति की पहचान और पूर्वानुमानित विश्लेषण में बदलते खतरों से निपटने के लिए

साइबर सुरक्षा से जुड़े ऐआई के प्रकार

नियम-आधारित प्रणालियाँ

- पूर्व-निर्धारित नियमों का उपयोग करता है
- उदाहरण: फ़ायरवॉल नियम

यंत्र अधिगम

- सामान्य बनाम असामान्य व्यवहार सीखता है
- धोखाधड़ी का पता लगाना, घुसपैठ का पता लगाना, वगैरह के लिए इस्तेमाल होता है।

गहन अधिगम

- जटिल स्वरूप को सीखने के लिए उपयोग किया जाता है
- जैसे छवि पहचान, वाणी, डीपफेक वगैरह।

साइबर जोखिम क्या है?

परिभाषा

साइबर जोखिम का मतलब है किसी इन्फॉर्मेशन सिस्टम को खतरनाक लोगों या ऐसे हालात के सामने लाना जिनसे नुकसान या क्षति हो सकती है।

साइबर जोखिम के स्रोत

बाहरी हमलावर, वायरस कमजोर सुरक्षा वाले थर्ड-पार्टी वेंडर अप्रकाशित सॉफ्टवेयर

जोखिम घटक

तंत्र पर किसी बुरी घटना के असर की संभावना

धमकी
भेद्यता
प्रभाव

साइबर जोखिम का प्रभाव

अनधिकृत पहुंच
तथ्यों की चोरी
वित्तीय क्षति
सेवा व्यवधान
विश्वास की हानि

सामान्य साइबर खतरे

खतरे की श्रेणियाँ

- फ़िशिंग – उपयोगकर्ताओं को धोखा देना
- मैलवेयर - दुर्भावनापूर्ण सॉफ़्टवेयर
- रैनसमवेयर – तथ्यों का बंधक
- प्रत्यक्ष पत्र (क्रेडेंशियल) की चोरी – गलत इरादे वाले लोगों द्वारा बिना इजाज़त के प्रमाणित करने वाली जानकारी हासिल करना
- वेबसाइट को खराब करना – बिना इजाज़त के लोग वेबसाइट पर उपलब्ध जानकारी को बदलने के लिए वेब सर्वर में सेंध लगाते हैं

भारतीय संदर्भ में जोखिम :

- फर्जी बैंक एसएमएस
- फर्जी सरकारी पोर्टल
- व्हाट्सएप स्कैम मैसेज

मैलवेयर क्या है?

मैलवेयर एक निष्पादन योग्य फ़ाइल है जो प्रकृति से द्वेषपूर्ण होती है और कई तरह की दुर्भावनापूर्ण गतिविधियाँ करता है और साइबर संरचना को नुकसान पहुंचाता है।

- यह सबसे आम साइबर खतरों में से एक है।
- यह साइबर हमलावरों द्वारा बनाए गए किसी भी तरह के दुर्भावनापूर्ण सॉफ्टवेयर के लिए एक शब्द है, जिसे संगणन या संजाल पर तथ्यों को चुराने या उसे खत्म करने के इरादे से तैयार किया जाता है।
- यह आमतौर पर संजाल की कमज़ोरियों, डाउनलोड या ईमेल संलग्नक के माध्यम से फैलता है।

क्या एंटी-वायरस सॉफ्टवेयर हमारी सुरक्षा के लिए काफी हैं?

उपयोगकर्ताओं की जानकारी के बिना उनके बारे में जानकारी इकट्ठा करता है

संगणन कीबोर्ड पर टाइप किए गए कीस्टॉक्स को लेख्यांकित और निगरानी करता है।

स्पाइवेयर

संगणन पर नियंत्रण करके तथ्यों को एन्क्रिप्ट कर देते हैं, इस्तेमाल करने के लिए उपयोगकर्ताओं को फिरौती देनी होती है

कीलॉगर

रैंसमवेयर

हमला करने के लिए संगणन को दूर से अनाधिकृत इस्तेमाल करने की अनुमति देता है।

बैकडोर

सामान्य प्रकार के मैलवेयर

एडवेयर

तंत्र को खराब करने के लिए खराब लिंक वाले अनचाहे ऐड और पॉप-अप।

किसी दूसरी निष्पादन योग्य फ़ाइल के साथ जुड़ा हुआ खराब निष्पादित कोड, जो तथ्यों को बदलें या मिटा दे।

वायरस

वर्म्स

तंत्र पर खुद को अनुकृति करते हैं। आमतौर पर संजाल धीमा हो जाता है और संजाल पर बहुत तेज़ी से फैलता है

बॉट
और
बॉटनेट

ट्रोजन

बॉट एक मैलवेयर से संक्रमित संगणन है, जिसे हमलावर दूर से संचालित कर सकता है।

ऐसा दुर्भावनापूर्ण कार्यक्रम जो खेल जैसा लगता है लेकिन जानकारी चुरा लेता है या मिटा देता है।

किस-किस को खतरा है?

व्यक्तियों को

- बैंक धोखाधड़ी
- चोरी की पहचान
- सोशल मीडिया अपहरण

संगठनों को

- तथ्यों की चोरी
- वित्तीय क्षति
- प्रतिष्ठा को नुकसान

सरकार और बुनियादी ढांचे को

- बिजली आपूर्ति के जाल
- रेलवे सेवाओं को
- स्वास्थ्य सेवा प्रणालियाँ

साइबर जोखिम राष्ट्रीय स्थिरता को प्रभावित करता है

प्रमुख कमजोरियाँ

- **ज़रूरी आधारभूत संरचना**: ऊर्जा, स्वास्थ्य सेवाएं और सरकारी मुख्यालय मुख्य निशाना हैं।
- **क्लाउड और आईओटी**: बढ़ते डिजिटल फुटप्रिंट, जिसमें क्लाउड का गलत विन्यास और असुरक्षित आईओटी उपकरण शामिल हैं, जो बड़े हमले को बढ़ावा दे रहे हैं।
- **कौशल अंतर**: साइबर सुरक्षा के पेशेवरों की कमी से संगठनों की मुश्किल, स्वचालित हमलों से बचाव करने की क्षमता कमज़ोर हो जाती है।

पारंपरिक साइबर सुरक्षा – इसकी सीमाएँ

पारंपरिक सुरक्षा इस पर निर्भर करती है:

- ज्ञात आक्रमण हस्ताक्षर
- हाथ से किया हुआ विश्लेषण
- स्थिर नियम

सीमाएँ:

- नए हमलों का पता लगाने में सक्षम नहीं
- प्रतिक्रिया धीमी है
- उच्च झूठी चेतावनी

साइबर सुरक्षा में ऐआई की ज़रूरत क्यों है

- वास्तविक समय में खतरे का पता लगाना और प्रतिक्रिया
- उच्च मात्रा में तथ्यों का प्रबंधन
- सक्रिय रक्षा (पूर्वानुमानित विश्लेषण)
- स्वचालित नियमित कार्य
- अंदरूनी खतरों के लिए व्यवहार विश्लेषण
- परिष्कृत मैलवेयर का मुकाबला

अज्ञात हमले के स्वरूप को सीखता है

विशाल तथ्यों की मात्रा को संभालता है

निरंतर संचालित होता है

मानव कार्यभार कम करें

ऐआई का उपयोग धोखाधड़ी का पता लगाने के लिए

धोखाधड़ी का पता लगाने में ऐआई, वास्तविक समय में बड़े आंकड़ा समुच्चय के विश्लेषण करने के लिए यंत्र अधिगम और भविष्यसूचक विश्लेषण का इस्तेमाल करता है, और धोखाधड़ी से जुड़ी गतिविधियों का संकेत देने वाली गड़बड़ियों और वयावहारिक स्वरूप की पहचान करता है।

- ऐआई सामान्य व्यावहारिक गतिविधियाँ सीखता है, और विचलन को अंकित करता है, जैसे की:
 - असामान्य स्थान
 - असामान्य समय
 - असामान्य राशि
- बैंक, ऐआई का इस्तेमाल निगरानी करने के लिए करते हैं, जैसे की:
 - यूपीआई लेनदेन
 - क्रेडिट कार्ड
 - नेट बैंकिंग

अनुप्रयोग

ईमेल और संदेश सुरक्षा में ऐआई का इस्तेमाल

विश्लेषण :

- भाषा स्वरूप की पहचान
- यूआरएल की पहचान
- प्रेषक व्यवहार

खोजने में मदद करता है:

- फर्जी जीएसटी ईमेल
- फर्जी आयकर नोटिस
- नकली कूरियर संदेश

संजाल और संगणन की निगरानी में ऐआई का इस्तेमाल

निगरानी में:

- लॉगिन व्यवहार
- फ़ाइल को इस्तेमाल करने का तरीका
- संजाल का यातायात

पता लगाता है:

- अंदरूनी खतरे
- समझौता किए गए खाते
- मैलवेयर गतिविधि

ऐआई का इस्तेमाल हमलावर भी करते हैं

कृत्रिम बुद्धिमत्ता अपने आप में न तो अच्छा है और न ही बुरा। यह एक साधन है, और किसी भी दूसरे साधन की तरह इसका गलत इस्तेमाल किया जा सकता है।

ऐआई स्वरूप को सीखता है, हमलावर उसी सीखने की क्षमता का इस्तेमाल करते हैं:

- शिकार के व्यवहार का अध्ययन करता है
- कमजोरियों की पहचान करता है
- हमलों को स्वचालित रूप से अनुकूलित करता है

हमलावर ऐआई की तरफ क्यों आकर्षित होते हैं:

- कम कौशल की आवश्यकता होती है
- स्वचालित निष्पादन
- हजारों या लाखों लक्ष्य

ऐआई-संचालित हमले

फ़िशिंग हमला :

- उत्तम व्याकरण का उपयोग करता है
- वैयक्तिकृत सामग्री का इस्तेमाल करता है
- संदर्भ-जागरूक संदेश भेजता है

उदाहरण :

फ़िशिंग ईमेल में बताया गया:

- आधार
- पी ऐ ऍन
- बैंक केवाईसी
- छात्रवृत्ति या सब्सिडी

डीपफेक और स्वर की क्लोनिंग :

ऐआई से उत्पन्न :

- फर्जी चलचित्र
- नकली आवाज
- नकली चित्र

जोखिम :

- फर्जी राजनीतिक भाषण
- नकली प्रसिद्ध व्यक्ति का विज्ञापन
- फर्जी आधिकारिक निर्देश

उभरता हुआ साइबर जोखिम परिदृश्य

- हमले तेज़ होते हैं
- हमले ज़्यादा चतुराई से होते हैं
- हमलों का श्रेय देना कठिन है

उच्च जोखिम वाले क्षेत्र:

- बैंकिंग और वित्त
- स्वास्थ्य देखभाल
- शक्ति और ऊर्जा
- अत्याधुनिक शहर
- रक्षा और अंतरिक्ष



साइबर सुरक्षा में ऐआई की ज़रूरतें

- साइबर सुरक्षा में, ऐआई का मतलब है साइबर खतरों की छान-बीन करने, उनका पता लगाने और उन पर प्रतिक्रिया करने के लिए कम्प्यूटेशनल एल्गोरिदम और उन्नत यंत्र अधिगम तकनीक का इस्तेमाल करना।
- साइबर सुरक्षा में ऐआई का मतलब है ऐसे बुद्धिमान तंत्र को बनाना जो स्वायत्त रूप से या अर्ध स्वायत्त रूप से बहुत सारे आकड़ों में स्वरूप की पहचान कर सके, गड़बड़ियों और संभावित खतरों को भी पहचान सकें।

उन्नत खतरों की पहचान

- ऐआई एल्गोरिदम का इस्तेमाल वास्तविक समय में बहुत सारे आकड़ों के विश्लेषण करने के लिए किया जा सकता है ताकि स्वरूप को पहचान सकें, गड़बड़ियों और संभावित खतरों का पता लगाया जा सके जो पारंपरिक हस्ताक्षर आधारित पता लगाने वाली प्रणालियों से बच सकते हैं।
- इससे मुश्किल और पहले से अनजान खतरों की जल्दी पहचान हो पाती है।



व्यवहार विश्लेषण

- ऐआई आधारित तंत्र आम उपयोगकर्ता के व्यावहार, संजाल गतिविधियों और तंत्र संचालन को समझने के लिए व्यावहारिक विश्लेषण का इस्तेमाल करते हैं।
- वे इन नियमों में बदलाव का पता लगा सकते हैं, जिससे संभावित सुरक्षा उल्लंघन या गलत गतिविधियों का संकेत मिल सकता है।



स्वचालित घटना प्रतिक्रिया

- ऐआई सुरक्षा घटनाओं को तेज़ी से पहचानकर और कम करके स्वचालित घटना प्रतिक्रिया को मुमकिन बनाता है
- यह खतरों को रोकने, खराब तंत्र को अलग करने, या सुधार के उपाय लागू करने के लिए तुरंत कार्रवाई कर सकता है, जिससे प्रतिक्रिया समय कम हो जाता है और नुकसान कम से कम होता है।



भविष्यसूचक विश्लेषण

- ऐआई पुराने आकड़ो, रुझान और नए खतरे की जानकारी के आधार पर संभावित सुरक्षा जोखिम का अनुमान लगा सकता है।
- यह सक्रिय तरीका संस्थाओ को भविष्य के खतरों के खिलाफ पहले से ही अपने बचाव को मज़बूत करने में मदद करता है।



मानव निर्णय लेने की क्षमता को बढ़ाना

- ऐआई इंसानी विश्लेषण की जगह नहीं लेता, बल्कि उन्हें अंतर्दृष्टि, सिफारिशें और संदर्भ देकर मदद करता है।
- यह सुरक्षा पेशेवरों को तेज़ी से और ज़्यादा सही तरीके से सोच-समझकर फैसले लेने में मदद करता है।



शमन के लिए रणनीतियाँ

व्यक्ति क्या कर सकते हैं

- भरोसा करने से पहले पुष्टि करें
- अत्यावश्यक अनुरोधों से बचें
- मजबूत पासवर्ड का उपयोग करें
- दो-कारक प्रमाणीकरण सक्षम करें
- सूचित रहें

राष्ट्रीय -स्तरीय दृष्टिकोण

- बड़े पैमाने पर साइबर जागरूकता
- एआई गवर्नेंस फ्रेमवर्क
- कुशल साइबर सुरक्षा कार्यबल
- सार्वजनिक-निजी भागीदारी

संगठनों को क्या करना चाहिए

- ऐआई आधारित सुरक्षा समाधान तैनात करें
- कर्मचारी जागरूकता प्रशिक्षण
- घटना प्रतिक्रिया योजना
- मानव ऐआई सहयोग

कृत्रिम बुद्धिमत्ता (आर्टिफिशियल इंटेलिजेंस) के ज़माने में, साइबर सुरक्षा का मतलब सिर्फ़ तंत्र को बचाना नहीं है — यह लोगों, उनके भरोसे और देश को बचाना है।

धन्यवाद



प्रगत संगणन विकास केंद्र (सी-डैक),
ऐ-34, इंडस्ट्रियल एरिया, फेज-8, मोहाली-160071 (पंजाब).