- एपिसोड 43 -

एआई और साइबर सुरक्षा : मेरे कंप्यूटर में अपराधी ?

स्क्रिप्ट : हेमंत लगवांकर

संकल्पना और समन्वय : डॉ. बी.के. त्यागी

आर्टिफिशियल इंटेलिजेंस (एआई) साइबर दुनिया में चर्चा का विषय है। ये प्रौद्योगिकी की चुनौतियों को दूर करने में महत्वपूर्ण भूमिका निभा सकता है। इन चुनौतियों में से एक है साइबर सुरक्षा... और बढ़ते साइबर अपराध प्रौद्योगिकी का काला पक्ष है... साइबर स्पेस में AI का भविष्य अनुप्रयोग हैकर्स पर अंकुश लगाना सुनिश्चित करेगा...

साइबर अपराध को लेकर लगभग हर रोज़ कोई न कोई ख़बर आ जाती है... ये सिर्फ एक देश की नहीं बल्कि पूरी दुनिया की समस्या है... हैकर्स द्वारा किए जाने वाले ऑनलाइन हमलों की वजह से सरकारों, बैंकों, बहुराष्ट्रीय कंपनियों के लिए साइबर अपराध बड़ा खतरा बन गया है। बहुत से व्यक्तिगत और संगठनात्मक डेटा का उपयोग हैकर्स द्वारा किया जाता है।

एआई और साइबर स्पेस के क्षेत्र में अनुसंधान को हाल के दिनों में ज़्यादा महत्व मिला है... और ये लंबे समय तक चलेगा क्योंकि ये मानव जीवन से जुड़ा एक गतिशील और संवेदनशील मुद्दा है।इस एपिसोड में बताया गया है कि साइबर तकनीकों में सुधार के लिए AI तकनीक किस तरह से मदद करती है।

किरदार :

हैकर : एक युवक (उम्र लगभग 25 वर्ष)

श्री पांडे : एक मध्यम आयु वर्ग का व्यक्ति (लगभग 45 वर्ष)

वर्णनकर्ता : एक महिला की आवाज़

पुलिस आयुक्त : आयु लगभग 57-58 वर्ष

श्रीमती मल्होत्रा : साइबर सेल यूनिट में पुलिस अधीक्षक (उम्र लगभग 45 वर्ष)

श्री आशीष दयाल : पुलिस विभाग के एक एआई विशेषज्ञ (उम्र लगभग 35 वर्ष)

(एक व्यक्ति जो हैकर है वह किसी अन्य व्यक्ति को एक नंबर डायल करता है। मोबाइल फोन की घंटी बजती है। रिंगटोन की आवाज सुनाई देती है। कॉल लिया जाता है और दो व्यक्तियों के बीच संवाद शुरू होता है।)

हैकर: हैलो...। गुड मॉर्निंग सर!

पांडे: हां...बोेलिए।

हैकर: क्या मैं मिस्टर चतुर्वेदी के साथ बात कर रहा हूं?

पांडे: नहीं, चतुर्वेदी नहीं...। मैं पांडे हूँ!

हैकर: ओह्ह...। माफ़ी चाहूंगा... मैं आपसे ही बात करना चाहता हूं... गलती से चतुर्वेदी जी का नाम बोल दिया...

पांडे: ठीक है... लेकिन आप कौन हैं?

हैकर: सर, मैं 'स्मार्ट पे' से बोल रहा हूं। मुझे आशा है कि आप नियमित रूप से हमारे ऐप का उपयोग कर रहे हैं!

पांडे: हां ... मैं अक्सर इसका इस्तेमाल करता हूं।

हैकर: जी सर! इसलिए मैंने आपको फ़ोन किया है।

पांडे: ठीक है।

हैकर: सर, क्या आप हमारी सेवा से संतुष्ट हैं? हमारे ऐप को इस्तेमाल करने में कोई दिक़्क़त तो नहीं आ रही है?

पांडे: नहीं, ऐसा तो कुछ नहीं है...

हैकर: तो सर, आप हमारे ऐप 'स्मार्ट पे' और हमारे द्वारा प्रदान की जाने वाली सेवा से संतुष्ट हैं ?

पांडे: हाँ...बिल्कुल...

हैकर: ठीक है, मिस्टर पांडे! आप हमारे मूल्यवान ग्राहक हैं। इसलिए हम आपको पिछले पांच लेन-देन के लिए एक सरप्राइज गिफ्ट देना चाहते हैं जो आपने इस महीने जीता है।

पांडे: ठीक है, लेकिन मैंने ऐप में ऐसा कोई ऑफर नहीं देखा।

हैकर: सर, मैंने आपसे कहा ना, हम आपको सरप्राइज देना चाहते हैं!

पांडे: ठीक है।

हैकर: सर, आपने हमारे ऐप के लिए यही फ़ोन नंबर पंजीकृत किया है... या फिर कोई और नंबर है ?

पांडे: यही नंबर है जिस पर हम बात कर रहे हैं...

हैकर: बहुत बढ़िया! तो फिर सर, हमारे ऐप में एक मेसेज आया होगा...उसे देखें ... अभी!

(मेसेज की घंटी बजती है। श्री पांडे को मेसेज मिल गया है)

पांडे: हाँ! मुझे मेसेज मिल गया है, लेकिन ये 18999.00 रुपये और भुगतान करने के लिए कह रहा है...

हैकर: बेशक सर! ये कह रहा है कि, आपको अपने वॉलेट से इस रक़म को भुगतान करने की आवश्यकता है। बस pay करने का विकल्प दबाएं और आपको अपने वॉलेट में राशि दिखाई देगी!

पांडे: ठीक है! मुझे ऐसा करने दो!

(फिर से मेसेज की घंटी बजती है। श्री पांडे ने एसएमएस प्राप्त किया है)

पांडे: ओह माय गॉड! हेलो...हेलो...। हे मिस्टर ..... हेलो...।

(फोन की व्यस्त ध्वनि केवल सुनाई देती है)

वर्णनकर्ता: (संगीत की एक उदास धुन पृष्ठभूमि पर है) तो दोस्तों, क्या आपने सुना ? क्या आप समझ गए हैं कि क्या हुआ है? श्री पांडेय को धोखा दिया गया। ये फोन कॉल एक धोखाधड़ी थी और श्री पांडे एक हैकर के इस कॉल का शिकार हो गए। उन्हें एक क्लिक में उन्नीस हजार रुपये देने के लिए मजबूर किया गया था। मुझे यकीन है कि, हम में से ज़्यादातर लोगों ने समाचारों में ऐसी घटनाओं को पढ़ा है, सुना है... और आप में से कुछ ने इस तरह के वित्तीय नुकसान का अनुभव भी किया होगा...।

(पार्श्व संगीत धीरे-धीरे बदलता है)

दोस्तों, ये तो बहुत छोटी सी घटना है... दुनिया तेज गति से डिजिटल हो रही है... और ये परिवर्तन और बढ़ने ही वाला है। डिजिटलाइजेशन का मतलब है सब कुछ बिजली की गति से बढ़ रहा है - व्यापार, मनोरंजन, रुझान, नए उत्पाद, आदि।

अधिक विडंबना ये है कि 2017 में किए गए अध्ययन के अनुसार, भारत साइबर खतरों के मामले में दुनिया का तीसरा सबसे कमजोर देश बन गया है, जैसे कि मैलवेयर, स्पैम फ़िशिंग, बॉट, नेटवर्क हमले, वेब हमले, रैनसमवेयर, और cryptominers।

अध्ययन में ये भी बताया गया है कि खतरे का परिदृश्य अधिक विविध होने के कारण, हमलावर हमले के नए रास्ते खोजने और ऐसा करते समय अपने ट्रैक को कवर करने के लिए कड़ी मेहनत कर रहे हैं।

(संगीत में बदलाव)

(पुलिस आयुक्त के केबिन का एक दृश्य। साइबर अपराधों और साइबर सुरक्षा के बढ़ते मुद्दों पर चर्चा के लिए आयुक्त द्वारा एक बैठक बुलाई जाती है। श्री दयाल के साथ पुलिस अधीक्षक श्रीमती मल्होत्रा भी वहाँ पहुंची हैं, जो पुलिस विभाग में AI विशेषज्ञ हैं।)

श्रीमती मल्होत्रा: (केबिन का दरवाजा खटखटाते हुए) क्या मैं अंदर आ सकती हूं?

पुलिस आयुक्त: हाँ, आइए...

श्रीमती मल्होत्रा: (कमिश्नर को सलाम! जमीन पर मारते हुए जूते की आवाज) पुलिस अधीक्षक, साइबर सुरक्षा सेल तनुजा मल्होत्रा, रिपोर्टिंग सर...

पुलिस आयुक्त: जय हिन्द!

श्रीमती मल्होत्रा: जय हिंद सर।

पुलिस आयुक्त: बैठिए श्रीमती मल्होत्रा!

श्रीमती मल्होत्रा: धन्यवाद सर। मैं आपको श्री दयाल के साथ रिपोर्ट कर रही हूं जो हमारे विभाग के एआई विशेषज्ञ हैं।

पुलिस आयुक्त: नमस्ते... बैठिए...

दयाल: जय हिंद सर!

पुलिस आयुक्त: जय हिंद...। तो श्रीमती मल्होत्रा, जैसा कि आप जानती हैं... मैंने इस बैठक को बहुत ही विशिष्ट एजेंडे के साथ बुलाया है।

श्रीमती मल्होत्रा: जी सर!

पुलिस आयुक्त: आप बहुत अच्छी तरह से जानते हैं कि, हाल ही में, हमने एक वेब नेटवर्क के माध्यम से लगभग 150 करोड़ के अनाधिकृत लेनदेन का अनुभव किया है। बेशक, सीबीआई इसकी देखरेख कर रही है। लेकिन, सूचना प्रौद्योगिकी, नेटवर्किंग, सोशल मीडिया, ऑनलाइन व्यापार आदि पर निर्भरता बढ़ने के साथ ही हम साइबर अपराध का सामना कर रहे हैं। हर दिन ये मामले बढ़ रहे हैं।

श्रीमती मल्होत्रा: मुझे जानकारी है सर!

पुलिस आयुक्त: इसके अलावा, श्रीमती मल्होत्रा ये केवल वित्तीय मुद्दों तक ही सीमित नहीं है, बल्कि ये राष्ट्रीय सुरक्षा के लिए भी खतरा बन गया है।

श्रीमती मल्होत्रा: जी सर! मैं समझ सकती हूँ!

पुलिस आयुक्त: तो, श्रीमती मल्होत्रा ... मैं जानना चाहता हूं कि इस ज्वलंत मुद्दे से निपटने के लिए हमारी क्या रणनीति हो सकती है। हमारी क्या तैयारी हो सकती है?

श्रीमती मल्होत्रा: हां, सर। हम निश्चित रूप से इसकी चर्चा करेंगे। इसीलिए मैंने श्री आशीष दयाल से इस मुद्दे पर काम करने के लिए कहा है क्योंकि उनके पास AI को लेकर विशेषज्ञता है और मुझे लगता है कि वो सही व्यक्ति हैं जो इस समस्या से निपटने के लिए कृत्रिम बुद्धिमत्ता का उपयोग करने के बारे में हमारा मार्गदर्शन कर सकते हैं।

पुलिस आयुक्त : ठीक है... तो आगे बढ़ते हैं...

श्रीमती मल्होत्रा: आशीष, आप बताइए ये कैसे किया जाएगा ?

दयाल: हाँ मैडम! कई कारण हैं जिसकी वजह से ये साइबर क्राइम हो रहे हैं।

श्रीमती मल्होत्रा: सही कहा...

दयाल: जब सब कुछ सुचारू रूप से चल रहा होता है, अचानक... आपको पता चलता है कि हैकर्स ने सिस्टम पर हमला किया है और फिरौती के रूप में एक पैर और एक हाथ की मांग कर रहे हैं। इस परिदृश्य में, आप न केवल पैसा खो देते हैं, बल्कि अपने ग्राहकों का भरोसा भी खो देते हैं। बाजार में जाने वाले नकारात्मक संदेश आपकी ब्रांड छवि को खराब कर देते हैं।

पुलिस आयुक्त: हम्म।

श्रीमती मल्होत्रा: इससे आम लोगों के मन में भी भय पैदा होता है... असुरक्षा का डर पैदा होता है...

दयाल: हाँ! हमारे अध्ययन से, हमें पता चला है कि, छोटे व्यवसाय या छोटे उद्यम पर किए जा रहे 43% हमलों के साथ ही ये निरंतर रडार पर हैं।

पुलिस आयुक्त: श्री दयाल, ये अध्ययन निश्चित रूप से इस मुद्दे को समझने और संभालने में हमारा नेतृत्व करेगा।

दयाल: हाँ सर! ये देखा गया है कि, हमारे लिए सबसे बड़ी चुनौती मैलवेयर प्रसार है। मैलवेयर एक दिन में एक लाख से ज़्यादा की तीव्र गति से बढ़ रहा है, जिसे नियंत्रित करना मुश्किल है।

श्रीमती मल्होत्रा: फिर क्या कृत्रिम बुद्धिमत्ता इस मुद्दे को हल करने में मदद कर सकती है?

दयाल: इस बात पर आता हूँ, मैडम। लेकिन, हमें पहले इस समस्या को विस्तार से देखना चाहिए जिससे कि हम इसके दायरे को समझ सके...

पुलिस आयुक्त: हाँ, बिल्कुल सही... तो आगे बताइए...

दयाल: साइबर हमले से लड़ने के लिए व्यवसाय पूरी कोशिश कर रहे हैं, लेकिन ये अनुमान लगाना कठिन है कि नए अभियान क्या बनेंगे और वे कैसे संचालित होंगे। अगला बड़ा मैलवेयर खतरा क्या होगा, ये समझ पाना और भी कठिन है।

पुलिस आयुक्त: आपके कहने का मतलब है, कि अज्ञात खतरों से बचाव करना मुश्किल है?

दयाल: हाँ सर, कुछ हद तक...

श्रीमती मल्होत्रा: और ये एक ऐसी चीज है जिसका साइबर अपराधी फायदा उठाते हैं।

दयाल: सर, Zeus trojan और Locky ransomware को कभी बड़े खतरे के रूप में माना जाता था, लेकिन अब Emotet botnet, the Trickbot trojan and Ryuk ransomware जैसी चीजों का ख़तरा बढ़ गया है।

श्रीमती मल्होत्रा: ये तो काफी भयानक है!

दयाल: भयानक हिस्सा ये है कि, Emotet सॉफ़्टवेयर आमतौर पर अन्य malicious payloads के लिए वितरण और पैकिंग सिस्टम के रूप में काम करता है, लेकिन कंप्यूटर सिस्टम को क्रूर बनाने, स्पैम ईमेल मेसेज बनाने, भेजने और वित्तीय डेटा चोरी करने में भी सक्षम है। Emotet ने बैंकिंग ट्रोजन के रूप में शुरूआत की, लेकिन एक Botnet के रूप में भी विकसित हुआ है... जिससे कि इसका इस्तेमाल अन्य आपराधिक गिरोह भी कर सकें, जो मशीनों से समझौता करने के लिए अपने स्वयं के मैलवेयर वितरित करना चाहते हैं। लगभग दो-तिहाई malicious payloads को फ़िशिंग हमलों के लिए Emotet द्वारा वितरित किया गया था।

पुलिस आयुक्त: लेकिन इस मामले में काम करने का तरीका क्या है?

दयाल: मैलवेयर को फ़िशिंग ईमेल के माध्यम से वितरित किया जाता है जिसमें एक malicious Microsoft Word दस्तावेज़ होता है। ईमेल का विषय आम तौर पर चालान, बैंक विवरण और अन्य वित्तीय विषयों पर आधारित होता है - यानी, लोगों का ध्यान आकर्षित करने के लिए सामान्य शब्द।

श्रीमती मल्होत्रा: और attachment में क्या होता है?

दयाल: ईमेल उपयोगकर्ता को दस्तावेज़ देखने के लिए 'enable content' का option देता है... और अगर ऐसा किया जाता है तो ये macros और URLs को उपयोगकर्ता के कंप्यूटर या मोबाइल पर Emotet डालने की अनुमति देता है।

श्रीमती मल्होत्रा: ओह्ह माय गॉड! ये एक जाल की तरह है!

दयाल: हाँ! ये उपयोगकर्ता के लिए एक जाल है और वे इस लुभावने दस्तावेज़ को खोलने के झांसे में आ जाते हैं। क्योंकि Emotet एक सफल botnet है... और ये malicious ईमेल किसी एक विशेष स्रोत से नहीं आता है, बल्कि दुनिया भर में संक्रमित विंडोज मशीनों से आता है।

पुलिस आयुक्त: इसका मतलब है कि ये महामारी की तरह फैलता है!

दयाल: बिल्कुल सर! अगर कोई मशीन Emotet का शिकार हो जाती है, तो ये न केवल मैलवेयर को सिस्टम में एक बैकडोर एंट्री करने देती है बल्कि हमलावरों को संवेदनशील जानकारी भी चुराने देती है... साथ ही ये हमलावरों को अतिरिक्त मैलवेयर फैलाने के लिए उसी मशीन का उपयोग करने की भी अनुमति देता है।

कमिश्नर: हम्म! ऐसा क्यों कहा जाता है कि, 'साइबर हमला मानव जाति के लिए सबसे बड़ा खतरा है, परमाणु हथियार से भी बड़ा खतरा!'

श्रीमती मल्होत्रा: ये सही है सर!

दयाल: महोदय, इस तरह के हमलों को न केवल वित्तीय सेवाओं में संगठनों पर निर्देशित किया गया है, बल्कि अब भोजन, मीडिया और परिवहन उद्योगों को भी निशाना बनाया गया है!

पुलिस आयुक्त: ठीक है... हमें वास्तविकता का सामना करना चाहिए और सोचना चाहिए कि इस चुनौती से कैसे निपटें...

दयाल: सर, पारंपरिक तकनीक पुराने आंकड़ों पर निर्भर करती है और इसे सुधारा नहीं जा सकता है। ये हैकर्स के नए तंत्र और चाल के साथ नहीं चल सकता है। आम लोगों को हर रोज़ अनगिनत साइबर खतरों का सामना करना पड़ता है। मैलवेयर एक दिन में 100,000 से अधिक की गति से बढ़ रहा है, जिसे मैन्युअल रूप से नियंत्रित करना मुश्किल हो जाता है।

श्रीमती मल्होत्रा: अगर लोग उचित सावधानी बरतें और अपना डेटा पासवर्ड सुरक्षित रखें तो?

दयाल: आप सही कह रहे हैं, लेकिन सुरक्षा की बात करते समय पासवर्ड का रोल बहुत नाजुक होता है। और वास्तविकता ये है कि, हम में से ज़्यादातर लोग अपना पासवर्ड बनाने में बहुत आलसी हैं... अक्सर कई खातों में एक ही पासवर्ड का इस्तेमाल करते हैं... वर्षों से एक ही पासवर्ड पर भरोसा करते हैं, उसे बदलते नहीं हैं... और तो और अपना पासवर्ड डिवाइस में लिखकर रखते हैं, आदि...

श्रीमती मल्होत्रा: और बायोमेट्रिक प्रमाणीकरण के बारे में क्या ?

दयाल: जैसा कि आपने कहा, बायोमेट्रिक प्रमाणीकरण को पासवर्ड के विकल्प के रूप में इस्तेमाल किया जाता है, लेकिन ये बहुत सुविधाजनक नहीं है... और हैकर्स भी इसे आसानी से दरकिनार कर सकते हैं। जैसे कि फेस रिकग्निशन सिस्टम आपको नए हेयर स्टाइल के कारण या टोपी पहनते समय पहचान नहीं सकता है। हमलावर फेसबुक या इंस्टाग्राम से आपकी छवियों का उपयोग करके भी इसके माध्यम से आपके बारे में जानकारी प्राप्त कर सकते हैं।

पुलिस आयुक्त: (कुछ चिड़चिड़े स्वर के साथ) श्री दयाल, मैं इसका समाधान पूछ रहा था। (विराम लेते हुए) अधिकारियों को देखें, मुझे इस मुद्दे में कोई नकारात्मकता नहीं चाहिए। हमें इस मुद्दे पर बहुत गंभीरता से विचार करने और तुरंत आवश्यक कार्यवाही करने की आवश्यकता है...।

श्रीमती मल्होत्रा: क्षमा करें सर ... हम आपकी भावनाओं को समझते हैं!

दयाल: सर, इस स्थिति में, कृत्रिम बुद्धिमत्ता ही एक संभव समाधान है... पूरी तरह से नहीं, लेकिन इसमें मैलवेयर के लिए मैन्युअल रूप से निर्मित एंटी-वायरस की आवश्यकता को समाप्त करके मैलवेयर प्रसार से निपटने की गुंजाइश है।

पुलिस आयुक्त: ठीक है!

दयाल: AI और machine learning की मदद से 'बुरे' को 'अच्छे' से अलग किया जा सकता है और हम alien मैलवेयर के हमले को भी हरा सकते हैं, जिसे पहले कभी नहीं देखा गया।

पुलिस आयुक्त: ये अच्छा है!

श्रीमती मल्होत्रा: मशीन लर्निंग इस मामले में कैसे मदद करती है ?

दयाल: असल में मैडम, मशीन लर्निंग के मुख्यधारा में आने से पहले, AI कार्यक्रमों का इस्तेमाल केवल व्यवसाय और उद्यमों में निम्न-स्तरीय कार्यों को स्वचालित करने के लिए किया गया था। मशीन लर्निंग मूल रूप से AI से अलग है, क्योंकि इसमें विकसित होने की क्षमता है। विभिन्न प्रोग्रामिंग तकनीकों का उपयोग करते हुए, मशीन लर्निंग algorithm बड़ी मात्रा में डेटा संसाधित करने और उपयोगी जानकारी निकालने में सक्षम है। इस तरह, वो मौजूदा डेटा से सीखकर अपने पिछली खामियों में सुधार कर सकते हैं।

श्रीमती मल्होत्रा: लेकिन AI का क्या ?

दयाल: हां, मैं उस पर ही आ रहा हूं! दरअसल, हम बड़े डेटा के बारे में बात किए बिना मशीन लर्निंग के बारे में बात नहीं कर सकते हैं... मशीन लर्निंग, algorithm के सबसे ज़रूरी पहलुओं में से एक है। किसी भी प्रकार का AI आमतौर पर अच्छे परिणामों के लिए अपने डेटासेट की गुणवत्ता पर निर्भर करता है, क्योंकि ये statistical methods का भारी उपयोग करता है। मशीन लर्निंग algorithm के साथ, AI सिर्फ प्रोग्राम किए गए कामों को करने से परे और चीज़ें विकसित करने की भी क्षमता रखता है।

पुलिस आयुक्त: इसलिए मशीन लर्निंग और आर्टिफिशियल इंटेलिजेंस दोनों साथ-साथ चलते हैं...

दयाल: बिल्कुल सर! आज की ऑनलाइन दुनिया में, कंपनियों की पहुँच अपने ग्राहकों के डेटा तक है और ये आमतौर पर लाखों में है... ये डेटा बहुत बड़ा है... और हर रोज़ बढ़ रहा है... इसे manually manage करना लगभग असंभव है।

श्रीमती मल्होत्रा: और इसमें AI मदद कर सकता है।

दयाल: बिल्कुल सही! AI की मदद से हम समझदारी से चीज़ों को मैनेज कर सकते हैं। इसकी मदद से किसी उल्लंघन या व्यवहार में परिवर्तन और

परिणामों को समझना आसान होगा और मौजूदा समय में इसे लेकर खुद को विकसित करना ज़रूरी भी है। AI, सॉफ्टवेयर में देखी गई कमजोरियों को कुशलता से संभाल सकता है और ये ज़्यादा जोखिम वाली स्थिति को प्राथमिकता दे सकता है, जिन पर तत्काल ध्यान देने की ज़रूरत है। साइबर सिक्योरिटी में मशीन लर्निंग और आर्टिफिशियल इंटेलिजेंस का एक महत्वपूर्ण लाभ ये भी है कि ये संभावित समस्याओं को लगभग तुरंत ही रोक देते हैं, जिससे संभावित कार्यों में आने वाली बाधा से बचा जा सके।

पुलिस आयुक्त: ये बहुत महत्वपूर्ण पहलू है!

दयाल: आर्टिफिशियल इंटेलिजेंस किसी भी खतरे का पता लगाने और उसका सामना करने के लिए सक्षम है, जिससे डेटा पहले से कहीं अधिक सुरक्षित रह सके। आर्टिफिशियल इंटेलिजेंस पूरी तरह से मशीनी भाषा में काम करता है, इसलिए बिना किसी गलती के साइबर सुरक्षा सेवाएँ दे सकता है। प्रौद्योगिकी में ये क्षमता है कि वो किसी भी हमले के शुरुआती चरणों का पता लगा सके... साथ ही किसी भी हमले के होने से पहले ही उसके बारे में जान जाए...

श्रीमती मल्होत्रा: ये बहुत अच्छा है!

दयाल: और जैसे हम ये भी सोचते हैं कि अपराधियों का अगला संभावित कदम क्या हो सकता है, तकनीक हमें ऐसा करने में मदद कर सकती है।

श्रीमती मल्होत्रा: वो कैसे?

दयाल: आर्टिफिशियल इंटेलिजेंस और मशीन लर्निंग 10,000 से अधिक सक्रिय फ़िशिंग स्रोतों का पता लगा सकता है और उन्हें ट्रैक कर सकता है... ये मनुष्यों की तुलना में बहुत तेज़ प्रतिक्रिया कर सकता है। जैसा कि हम जानते हैं, फ़िशिंग अभियानों का किसी भौगोलिक क्षेत्र से कोई सम्बन्ध नहीं होता है... लेकिन, आर्टिफिशियल इंटेलिजेंस और मशीन लर्निंग दुनिया भर से आ रही फिशिंग की धमकियों को स्कैन करती हैं... और आर्टिफिशियल इंटेलिजेंस ने नकली और असली वेबसाइट के बीच अंतर करना संभव बना दिया है।

पुलिस आयुक्त: इसका मतलब है कि AI लगातार बदलती, हाई-टेक हो रही दुनिया के हिसाब से काम करने की क्षमता रखती है। क्या मैं सही कह रहा हूँ?

दयाल: बिलकुल सर! मशीन लर्निंग और आर्टिफिशियल इंटेलिजेंस वास्तव में हैकर्स के फिशिंग पैटर्न का अध्ययन करते हैं। इसलिए आर्टिफिशियल इंटेलिजेंस की मदद से, फ़िशिंग गतिविधि को तुरंत पहचानना संभव है... इसके अलावा दुर्भावनापूर्ण घुसपैठ की संभावित क्षति को रोकना और लॉगिन क्रेडेंशियल्स को चोरी होने से बचाना, मैलवेयर को तैनात किया जाना या हमलावरों को नेटवर्क तक पहुंचने में सक्षम बनाना भी संभव हो गया है।

श्रीमती मल्होत्रा: लेकिन अगर हैकिंग के नए पैटर्न सामने आने लगे तो क्या होता है?

दयाल: बहुत अच्छा सवाल है, मैडम! आर्टिफिशियल इंटेलिजेंस की मदद से सुरक्षा देना इसकी व्यवहारिक विश्लेषण क्षमता से होता है।

श्रीमती मल्होत्रा: मतलब?

दयाल: इसका मतलब है कि मशीन लर्निंग algorithm सीख सकते हैं और अपने व्यवहार का एक पैटर्न बना सकते हैं, जिसका विश्लेषण करके आप आमतौर पर अपने डिवाइस और ऑनलाइन प्लेटफॉर्म का उपयोग कर सकते हैं। जिसमें आपके टाइपिंग और स्क्रॉलिंग पैटर्न, आपके सामान्य लॉगिन का समय और आईपी पते आदि से लेकर सब कुछ शामिल हो सकता है। अगर किसी भी समय, आर्टिफिशियल इंटेलिजेंस algorithm असामान्य गतिविधियों या किसी अलग तरह के व्यवहार को नोटिस करता है जो आपके मानक पैटर्न के बाहर होता है, जो कि एक संदिग्ध उपयोगकर्ता द्वारा किया जा सकता है तो ये उपयोगकर्ता को ब्लॉक कर सकता है। आर्टिफिशियल इंटेलिजेंस के algorithm से जुड़ी गतिविधियाँ कुछ भी हो सकती है जैसे कि कोई महँगी ख़रीदारी जिसे किसी आपके पते की जगह किसी अन्य पते पर भेजा जाता है... या फिर आपके फ़ोल्डर से अचानक बड़ी संख्या में दस्तावेज़ डाउनलोड होने लगे, या आपकी टाइपिंग की गति में अचानक कोई बदलाव आए।

पुलिस आयुक्त: मेरा एक मौलिक प्रश्न है यहां।

दयाल: हाँ सर... पूछिए न...

पुलिस आयुक्त: हैकर्स भी बुद्धिमान हैं। उनके पास भी वही तकनीक है जो हमारे पास है। तो क्या वे हमें सुपरसीड कर सकते हैं?

दयाल: सर, वास्तव में आर्टिफिशियल इंटेलिजेंस के क्षेत्र में ये सबसे बड़ी चुनौती है कि ये हैकर्स सहित सभी के लिए समान रूप से उपलब्ध है। हमले करने के लिए हैकर्स आर्टिफिशियल इंटेलिजेंस का भी इस्तेमाल कर रहे हैं। वे मालवेयर को म्यूट करने के लिए आर्टिफिशियल इंटेलिजेंस का इस्तेमाल कर रहे हैं। वे तकनीक के लिहाज़ से सबसे कमजोर लोगों का पता लगाने के लिए भी आर्टिफिशियल इंटेलिजेंस का इस्तेमाल कर रहे हैं जो उनके लिए आसान लक्ष्य हो सकते हैं।

पुलिस आयुक्त: एक तरह से देखा जाए तो हमलावरों और रक्षकों के बीच लगातार लड़ाई होती रहती है...

दयाल: हां सर, लेकिन अब ऐसे सिस्टम हैं जो तुरंत संदिग्ध गतिविधि की सूचना देते हैं। इसके लिए कुछ विशेष मशीन-लर्निंग signatures और मॉडल तैयार किए जा रहे हैं। AI-आधारित नेटवर्क-निगरानी उपकरण ये भी ट्रैक कर सकता है कि उपयोगकर्ता दैनिक आधार पर क्या करते हैं जिससे वो उपयोगकर्ता के व्यवहार की एक तस्वीर बना लेता है। इस जानकारी का विश्लेषण करके, AI प्रणाली विसंगतियों का पता लगा सकती है और उसके अनुसार काम कर सकती है।

पुलिस आयुक्त: ठीक है... ये बहुत अच्छा है! तो आपके कहने का मतलब है कि हम पूरी तरह से तकनीक से लैस हैं और आर्टिफिशियल इंटेलिजेंस का उपयोग कर ऐसे फ़िशिंग हमलों से बचा जा सकता है।

दयाल: हाँ सर! लेकिन, ये भी उतना ही महत्वपूर्ण है कि किसी भी ऑनलाइन गतिविधि को करते समय उपयोगकर्ताओं को सावधान रहना चाहिए, खासकर लेनदेन करते समय!

(संगीत पर बदलाव)

अनाउन्सार: तो दोस्तों, मशीन लर्निंग और आर्टिफिशियल इंटेलिजेंस दो मजबूत हथियार हैं जिन्हें हमें फ़िशिंग हमलों से बचाना है... लेकिन जैसा कि विशेषज्ञों का कहना है, कृत्रिम बुद्धिमत्ता के बारे में सब कुछ 'स्पष्ट' नहीं है... हमें व्यक्तिगत स्तर पर भी सावधान रहना चाहिए... क्योंकि ये आपके साथ भी हो सकता है... एक अध्ययन बताता है कि हर 130 ईमेल में से एक में एक मैलवेयर होता है... तो, सावधान रहें... नहीं तो कौन जानता है कि आपके कंप्यूटर में एक अपराधी भी हो सकता है...

(संगीत का अंश। एपिसोड समाप्त होता है)