Chapter 5- Security and Future of IoT Ecosystem

Need of security in IoT

आज के समय में जिस प्रकार हर छोटा बड़ा व्यापार साइबर आधारित है,जहाँ पर Internet, LAN थता दूसरे नेटवर्क Methods का उपयोग किया जा रहा है,ऐसे में साइबर खतरों से बचाव व कार्यों को सुचारु रूप से बनाए रखने थता महत्वपूर्ण **डाटा** की सुरक्षा के लिए **नेटवर्क सिक्योरिटी** का होना आवश्यक है।

इसके परिपालन द्वारा ही नेटवर्क में होने वाले किसी भी प्रकार के साइबर क्राइम जैसे Hacking**, Virus, Data Loss, Data Modification, Identity Theft, DDOS Attack** इत्यादि को रोका जाता है, और User को कार्य करने के लिए एक सुरक्षित प्लेटफार्म उपलब्ध कराया जाता है।

नेटवर्क सिक्योरिटी का अर्थ एक नेटवर्क को अनधिकृत (Unauthorized) Access Misuse और Risk से बचाना है। इसके अंतर्गत उन सभी नियमों और उपायों का पालन किया जाता है, जिससे नेटवर्क को सुरक्षित रखा जा सके।

किसी भी नेटवर्क के आकार के अनुसार ही उसकी सिक्योरिटी सुनिश्चित की जाती है, जैसे यदि एक छोटे आकार का नेटवर्क है, तो उसमें **Basic Network Security** की आवश्यकता पड़ेगी, वहीँ जब एक बड़ा बिज़नेस है, जिसके नेटवर्क का आकार भी बड़ा है, तो वहाँ पर नेटवर्क सिक्योरिटी भी काफी **High** रहेगी। जिनमे हार्डवेयर थता सॉफ्टवेयर Solutions को उपयोग में लाया जाता है, ताकि नेटवर्क में होने वाले **Intrusions** और **Threat** Attacks को रोका जा सके।

एक High नेटवर्क सिक्योरिटी के अंतर्गत Access Control, Authentication Access, Antivirus Software, Application Security, Network Monitoring, Firewall, Encryption जैसे उपाय शामिल रहते हैं।

Cyber Attacks

साइबर अटैक के दोनों टर्म्स को अलग-अलग करके समझने का प्रयास करें तो Cyber जिसका मतलब होता है “इन्टरनेट या इन्टरनेट से जुडी चीजें" और Attack जिसका मतलब होता है “हमला करना” अतः Cyber Attack की परिभाषा को हम कुछ इस तरह कह सकते है की किसी आतंकी गतिविधि के उदेश्य से साइबर स्पेस में किसी आर्गेनाइजेशन या किसी की पर्सनल नेटवर्क में बिना अनुमति के इन्टरनेट या इन्टरनेट से जुडी चीजों जैसे- Website, Computer, Network, Data इत्यादि पर हमला करके उसपर कब्ज़ा करना साइबर अटैक कहलाता है.

साइबर अटैक करने वाले एक इंसान ही होता है पर वह कोई एक साधारण इंसान नहीं होता है बल्कि वह एक कंप्यूटर हैकिंग एक्सपर्ट होता है जो अनाधकृत रूप से किसी के नेटवर्क में घुसकर दूसरों की वेबसाइट, कंप्यूटर, डाटा इत्यादि को हैक अर्थात उसपर कब्ज़ा करते है जिसे हैकर कहा जाता है.

हैकर तीन तरह के होते है.

White Hat Hacker: इस तरह के हैकर अपनी ज्ञान का उपयोग किसी अवैध गतिविधि में शामिल होने के लिए नहीं करते है बल्कि ये अच्छे कामों के लिए यानि साइबर की सुरक्षा या अवैध गतिविधि को रोकने के लिए सरकार या किसी आर्गेनाइजेशन के द्वारा नियुक्त किये जाते है. जिसका काम होता है साइबर सिक्योरिटी को जांचना उससे बग निकलना तथा एक सिक्योर साइबर एनवायरनमेंट बनाना. इन्हें Ethical Hacker कहा जाता है.

Black Hat Hacker: इस तरह के हैकर्स को क्रैकर्स भी कहा जाता है, ये अपनी ज्ञान का दुरूपयोग करते है अर्थात ये अपनी ज्ञान का उपयोग ज्यादातर अवैध यानि गैरकानूनी गतिविधियों को अंजाम देने के लिए करते है. इन हैकर का काम होता है साइबर सिक्योरिटी को भंग करना जैसे- किसी की निजी जानकारी चुराना, किसी के अकाउंट हैक करना, वेबसाइट हैक करना इत्यादि. इस तरह से ये किसी की वेबसाइट, अकाउंट, कंप्यूटर या डाटा हैक करके उससे फिरोती की भी मांग करते है और उससे वे पैसा कमाते है.

Grey Hat Hacker: इस श्रेणी के में आनेवाले हैकर White Hat और Black Hat दोनों का सम्मिश्रण होते हैं क्योंकि ये अपने ज्ञान का उपयोग अपनी जरुरत तथा इच्छा के अनुसार करते है अर्थात ये कभी अच्छे काम करते है तो कभी-कभी गैरकानूनी काम भी करते हैं।

Types of Cyber Attacks

Malware Attack:

मैलवेयर एक मैलिशियस सॉफ्टवेयर होता है, जिसको अलग-अलग तरह के तरीके को अपनाकर जैसे ईमेल के माध्यम से मेसेज के माध्यम से इन्टरनेट पर पॉपअप दिखाकर आपके कंप्यूटर सिस्टम में इनस्टॉल करने की कोशिश की जाती है और जब आप अपने सिस्टम में गलती से इन सॉफ्टवेयर को इनस्टॉल कर लेते है तो आपके सिस्टम का कण्ट्रोल हैकर के हाथ में चला जाता है.

रैनसमवेयर सबसे अधिक इस्तेमाल किया जाने वाला मैलिशियस सॉफ्टवेयर है जो डेटा चोरी करने के लिए इस्तेमाल किया जाता है इसे रैनसमवेयर अटैक के नाम से जाना जाता है. एक बार मैलवेयर सिस्टम में इंस्टॉल हो जाने पर सभी संवेदनशील जानकारी हैकर का शिकार बन जाता है और उसे एन्क्रिप्ट कर दिया जाता है. फिर उन सारी डाटा को डिक्रिप्ट करवाने के लिए सिस्टम पर एक पॉप-अप मैसेज दिखाकर हैकर फिरौती के की मांग करता है. मैलिशियस सॉफ्टवेयर भी कई तरह के होते है जैसे- रैंसमवेयर, स्पाईवेयर, ट्रोजन, वर्म्स इत्यादि.

Fishing Attack:

यह साइबर की दुनियां में हैकर के द्वारा उपयोग किया जानेवाला सबसे आम तरीका है जिसमे हैकर आपको प्रलोभन के साथ मैलिशियस ईमेल भेजकर आपसे किसी लिंक पर क्लिक करवाकर आपकी निजी जानकारी चुराने की साजिश राचता है. इसके लिए वो अपने आप को आपके सामने किसी ब्रांड की तरह पेश करते हुए किसी लाटरी का प्रलोभन देकर या आपकी ही बैंक, फेसबुक, इन्स्ताग्राम अकाउंट की झूठी समस्या बताकर सुलझाने के लिए ईमेल भेजते है और उसमे दिए गए लिंक को क्लिक करने के लिए प्रेरित करते है. और जब आप उस लिंक पर क्लिक करते है तो वे आपके सिस्टम पर बेक एंड से अपना कण्ट्रोल बनाकर आपकी निजी जानकारी जैसे- कोई User Id, Password, Bank Details Etc. चुराकर आपको हानि पहुंचाते है.

Distributed Denial of Service (DDoS) Attack:

यह Cyber Attack का ही एक प्रकार है, जिसका मकसद किसी ऑनलाइन **Server**, **Application Website** या **Service** को बाधित (बंद) कर देना है,ताकि User's उस वेबसाइट या सर्विस को Access ना कर सकें। किसी भी **ऑनलाइन सर्विस**,**वेबसाइट** या **सर्वर** की एक प्रोसेसिंग स्पीड और यूजर Handling सीमा होती है,और यदि उस सीमा को लगातार Cross किया जाए तो एक समय बाद वह वेबसाइट या ऑनलाइन सर्विस **Slow** या **Crash** हो जाती है,यानि काम करना बंद कर देती है।

डीडीओएस अटैक में इसी पॉइंट को अटैकर Target करते हैं,और जिस **वेबसाइट** या **सर्विस** को Down करना है या Crash करना है,उस पर लगातार बड़ी भारी मात्रा में विभिन्न **Network Sources** (**Botnet**) से ट्रैफिक भेजा जाता है,जिससे की एक समय बाद वह टारगेट Crash हो जाता है।

Botnet मैलवेयर संक्रमित कम्प्यूटर्स का एक नेटवर्क होता है,जिसे किसी Attacking Party द्वारा Control किया जाता है,और DDOS अटैक के समय इसी Botnet नेटवर्क में स्थित कंप्यूटर्स द्वारा ट्रैफिक Generate किया जाता है,जिससे की टारगेट को डाउन किया जा सके।

SQL injection attack:

SQL जिसका फुल फॉर्म होता है Structured Query Language यह एक प्रोग्रामिंग लैंग्वेज है जिसका उपयोग Website के Back End में मोजूद सभी डेटाबेस को मैनेज अर्थात Retrieve तथा Modify करने के लिए किया जाता है. परन्तु हैकर इसी SQL का इस्तेमाल वेबसाइट को हैक करने के लिए करता है. इसमें एक ऐसी Technique का इस्तेमाल किया जाता है जिसे SQL Injection कहा जाता है जो हैकर के लिए काफी कारगर है. इस Technique का इस्तेमाल करके हैकर वे वेबसाइट को टारगेट करते है जिसकी डेटाबेस SQL पर मैनेज की गयी होती है. SQL Injection तकनीक में हैकर वेबसाइट के यूजर फॉर्म में ही Malicious Code को इनपुट करके वेबसाइट के डेटाबेस में प्रवेश करने की कोशिश करते है और अगर यदि इस कार्य में वो सफल हो जाते है तो वेबसाइट हैक कर लिया जाता है.

Brute Force Attack:

Brute Force Attack को **Dictionary Attack** भी कहा जाता है, यह एक हैकिंग अटैक है, जिससे पासवर्ड और पिन का पता लगाकर किसी कंप्यूटर, सर्वर, सोशल प्रोफाइल या बैंक अकाउंट को हैक किया जाता है।

यह एक पूरी तरह से अनुमान पर आधारित अटैक होता है, जिसमे किसी User का User Name और Password क्रैक करने के लिए **Software Tool** द्वारा लाखों शब्दों, न्यूमेरिक और सिंबल के अलग-अलग Combination's को लगातार Try किया जाता है, जब तक की पासवर्ड हैक ना हो जाए। और इसके लिए ब्रूट फोर्स सॉफ्टवेयर टूल में **Word List** फाइल को जोड़ा जाता है, यह एक Dictionary की तरह होती है, जिसमे लाखों प्रकार के शब्द होते हैं, और कई बार हैक किए जा रहे टारगेट से सम्बंधित इखट्ठा की गयी जानकारी के आधार पर भी **Custom Word List** के Sample's का इस्तेमाल किया जाता है, जिस से पासवर्ड क्रैक होने की संभावना बढ़ जाती है।

इस प्रक्रिया में काफी कम या अधिक समय दोनों लग सकते हैं, जो पूरी तरह से लगे हुए पासवर्ड की जटिलता पर निर्भर करता है। यानि पासवर्ड जितना लम्बा और मुश्किल होगा वह उतना ही अधिक सुरक्षित रहेगा, और उसे क्रैक करने में भी Hackers को काफी ज्यादा समय लगेगा।

How to avoid cyber attack

इन्टरनेट के माध्यम से होनेवाले साइबर अटैक से बचने के लिए अगर हम सब सजग हो और इससे से बचने के लिए कुछ जरुरी सतर्कता बरते तो स्वतः ही बहुत हद तक साइबर अटैक से बचा जा सकता है। इसके लिए जरुरी है की हम सब कुछ बातों का ध्यान रखें जैसे.

- इन्टरनेट पर मौजूद किसी फोरम या फालतू वेबसाइट पर अपनी व्यक्तिगत जानकारी को बेवजह किसी तीसरे पक्ष को शेयर ना करें.
- स्पैम मैसेज और ईमेल को न खोलें और न ही जवाब दें.
- इन्टरनेट पर मौजूद सोशल साइट जैसे- Facebook, Twitter, Instagram, Youtube इत्यादि पर अपनी Privet Information शेयर ना करें.
- इन्टरनेट के किसी भी प्लेटफार्म पर बनाये गए अकाउंट की User ID, Password इत्यादि को किसी दूसरों के साथ शेयर ना करें.
- इन्टरनेट के किसी भी प्लेटफार्म पर बनाये गए अकाउंट की Password बहुत ही Strong बनायें और हर जगह एक ही Password ना रखें.
- किसी भी लिंक या अटैचमेंट को खोलने से पहले यह सुनिश्चित कर लें की वो वैध और जेन्युइन माध्यम से आये है.
- बेवजह आनेवाले ईमेल या अंजान ईमेल पर Reply ना करें ना ही उसके द्वारा भेजे गए Attachment और Link पर क्लिक करें.
- SMS के माध्यम से आनेवाले Link जिसके बारे में आपको जानकारी नहीं हो उसपर क्लिक ना करें.
- अपने मोबाइल या कंप्यूटर पर free के चक्कर में फालतू हार्मफुल एप्लीकेशन इनस्टॉल नहीं करें.
- बेवजह फ़ोन के माध्यम से किसी को OTP, PIN, Password इत्यादि संवेदनशील इनफार्मेशन ना दें.
- अपने मोबाइल और कंप्यूटर में एक विश्वसनीय एंटीवायरस सॉफ्टवेयर जरूर रखें ताकि Harmful Virus, Application, Site, Link, Attachment इत्यादि Suspected होने के कंडीशन में आपको Alert दें, और इसे समय-समय अपडेट करते रहें ताकि नवीनतम क्रिएटेड Harmful Content को भी डिटेक्ट कर ले.

Future of IoT eco system

Artificial Intelligence (A.I) and Machine Learning (M.L)

क्या है आर्टिफिशियल इंटेलिजेंस?

सरलतम शब्दों में कहें तो आर्टिफिशियल इंटेलिजेंस का अर्थ है एक मशीन में सोचने-समझने और निर्णय लेने की क्षमता का विकास करना। आर्टिफिशियल इंटेलिजेंस को कंप्यूटर साइंस का सबसे उन्नत रूप माना जाता है और इसमें एक ऐसा दिमाग बनाया जाता है, जिसमें कंप्यूटर सोच सके...कंप्यूटर का ऐसा दिमाग, जो इंसानों की तरह सोच सके।

आर्टिफिशियल इंटेलिजेंस के प्रकार

- पूर्णतः प्रतिक्रियात्मक (Purely Reactive)
- सीमित स्मृति (Limited Memory)
- मस्तिष्क सिद्धांत (Brain Theory)
- आत्म-चेतन (Self Conscious)
- आर्टिफिशियल इंटेलिजेंस की शुरुआत 1950 के दशक में हुई थी। आर्टिफिशियल इंटेलिजेंस का अर्थ है-- बनावटी (कृत्रिम) तरीके से विकसित की गई बौद्धिक क्षमता।
- आर्टिफिशियल इंटेलिजेंस के जनक जॉन मैकार्थी के अनुसार यह बुद्धिमान मशीनों, विशेष रूप से बुद्धिमान कंप्यूटर प्रोग्राम को बनाने का विज्ञान और अभियांत्रिकी है अर्थात् यह मशीनों द्वारा प्रदर्शित की गई इंटेलिजेंस है।
- इसके ज़रिये कंप्यूटर सिस्टम या रोबोटिक सिस्टम तैयार किया जाता है, जिसे उन्हीं तर्कों के आधार पर चलाने का प्रयास किया जाता है, जिसके आधार पर मानव मस्तिष्क काम करता है।
- आर्टिफिशियल इंटेलिजेंस कंप्यूटर द्वारा नियंत्रित रोबोट या फिर मनुष्य की तरह इंटेलिजेंस तरीके से सोचने वाला सॉफ़्टवेयर बनाने का एक तरीका है।
- यह इसके बारे में अध्ययन करता है कि मानव मस्तिष्क कैसे सोचता है और समस्या को हल करते समय कैसे सीखता है, कैसे निर्णय लेता है और कैसे काम करता है।

आर्टिफिशियल इंटेलिजेंस के प्रमुख अनुप्रयोग

- कंप्यूटर गेम (Computer Gaming)
- प्राकृतिक भाषा प्रसंस्करण (Natural Language Processing)
- प्रवीण प्रणाली (Expert System)
- दृष्टि प्रणाली (Vision System)
- वाक् पहचान (Speech Recognition)
- बुद्धिमान रोबोट (Intelligent Robot)

इसके अलावा, किसी बेहद जटिल सिस्टम को चलाने...नई दवाएं तैयार करने...नए केमिकल तलाशने...खनन उद्योग से लेकर अंतरिक्ष...शेयर बाज़ार से लेकर बीमा कंपनियां...मानव जीवन का कोई क्षेत्र ऐसा नहीं बचा है, जिसमें आर्टिफ़िशियल इंटेलिजेंस का दखल न हो।

इसे इस उदहारण से समझने का प्रयास करते हैं...

आज विश्वभर में हवाई जहाज़ों की आवाजाही पूर्णतः कंप्यूटर पर निर्भर है। कौन-सा हवाई जहाज़ कब, किस रास्ते से गुज़रेगा...कहां सामान पहुंचाएगा...यह सब मशीनें तय करके निर्देश देती हैं। यानी एयर ट्रैफिक कंट्रोल के लिये आर्टिफिशियल इंटेलिजेंस का इस्तेमाल किया जा रहा है।

तात्पर्य यह कि जिस काम को करने में मनुष्य को समय अधिक लगता है या जो काम जटिल तथा दुष्कर है, वह इन मशीनी दिमाग़ों की मदद से चुटकियों में निपटाया जा सकता है।

मशीन लर्निंग (Machine Learning) क्या है?

जैसे आर्टिफिशियल इंटेलिजेंस ऐसे कंप्यूटर प्रोग्रामों के लिये इस्तेमाल किया जाता है, जो उन समस्याओं को हल करने की कोशिश करता है, जिसे मनुष्य आसानी से कर सकते हैं, जैसे किसी फ़ोटो को देखकर उसके बारे में बताना। उसी प्रकार एक अन्य काम जो इंसान आसानी से कर लेते हैं, वह है उदाहरणों से सीखना...और मशीन लर्निंग प्रोग्राम भी यही करने की कोशिश करते हैं अर्थात् कंप्यूटरों को उदाहरणों से सीखने के बारे में बताना। इसके लिये बहुत सारे अल्गोरिद्म आदि जुटाने पड़ते हैं, ताकि कंप्यूटर बेहतर अनुमान लगाना सीख सकें। लेकिन अब कम अल्गोरिद्म से मशीनों को तेज़ी से सिखाने के लिये मशीनों को ज़्यादा कॉमन सेंस देने के प्रयास किये जा रहे हैं, जिन्हें तकनीकी भाषा में 'रेग्यूलराइज़ेशन' कहा जाता है।

इसे एक उदहारण से और अधिक स्पष्ट करने का प्रयास करते हैं...

हॉलीवुड की फिल्म 'माइनॉरिटी रिपोर्ट' में टॉम क्रूज अभिनीत पुलिसमैन तीन पारलौकिक सी प्रतीत होने वाली शक्तियों से मिली सूचना के आधार पर भावी अपराधियों को कानून तोड़ने के पहले ही पकड़ लेता है।

वास्तव में ऐसा पूर्वानुमान लगाना अधिक कठिन है, लेकिन कंप्यूटर की पूर्वानुमान लगाने की बढ़ती क्षमता के कारण अब ऐसी संभावना कल्पना जगत तक ही सीमित नहीं प्रतीत होती। मशीन लर्निंग प्रोग्राम उल्लेखनीय रूप से सटीक पूर्वानुमान लगा सकता है। यह डेटा की भारी-भरकम मात्रा में पैटर्न तलाशने के सिद्धांत पर काम करता है।

इसे इस उदाहरण से स्पष्ट करने का प्रयास करते हैं...

किसी रेस्तराँ में साफ-सफाई को ही लीजिये। यह मशीन लर्निंग प्रोग्राम पता करता है कि नज़र में न आने वाले कौन से कारकों के मिलने से समस्या उत्पन्न होती है, लेकिन यदि एक बार मशीन को प्रशिक्षित कर दिया जाए तो वह रेस्तराँ के गंदे होने के जोखिम का आकलन कर सकेगा।

निष्कर्ष: आर्टिफिशियल इंटेलिजेंस की संकल्पना बहुत पुरानी है। ग्रीक मिथकों में 'मैकेनिकल मैन' की अवधारणा से संबंधित कहानियाँ मिलती हैं अर्थात् एक ऐसा व्यक्ति जो हमारे किसी व्यवहार की नकल करता है। प्रारंभिक यूरोपीय कंप्यूटरों को 'लॉजिकल मशीन' की तरह डिजाइन किया गया था यानी उनमें बेसिक गणित, मेमोरी जैसी क्षमताएँ विकसित कर इनका मैकेनिकल मस्तिष्क के रूप में इस्तेमाल किया गया था। लेकिन जैसे-जैसे तकनीक उन्नत होती गई और कैलकुलेशंस जटिल होते गए, उसी तरह आर्टिफिशियल इंटेलिजेंस की संकल्पना भी बदलती गई। इसके तहत इनको मानव व्यवहार की तरह विकास करने की कोशिश की गई, ताकि ये अधिकाधिक इस तरह से इंसानी कामों को करने में सक्षम हो सकें, जिस तरह से आमतौर पर हम सभी करते हैं।

गूगल के सीईओ सुंदर पिचाई का कहना है कि मानवता के फायदे के लिये हमने आग और बिजली का इस्तेमाल तो करना सीख लिया, पर इसके बुरे पहलुओं से उबरना जरूरी है। इसी प्रकार आर्टिफिशियल इंटेलिजेंस भी ऐसी ही तकनीक है और इसका इस्तेमाल कैंसर के इलाज में या जलवायु परिवर्तन से जुड़ी समस्याओं को दूर करने में भी किया जा सकता है। आर्टिफिशियल इंटेलिजेंस का निर्माण हमारी सभ्यता के इतिहास की सबसे बड़ी घटनाओं में से है। लेकिन सच यह भी है कि यदि इसके जोखिम से बचने का तरीका नहीं ढूँढा, तो इसके गंभीर परिणाम हो सकते हैं, क्योंकि तमाम लाभों के बावजूद आर्टिफिशियल इंजेलिजेंस के अपने खतरे हैं। कुल मिलाकर एक शक्तिशाली कृत्रिम बुद्धिमत्ता का उदय हमारे लिये फायदेमंद भी हो सकता है और नुकसानदेह भी। फिलहाल हम नहीं जानते कि इसका स्वरूप आगे क्या होगा, इसीलिये इस संदर्भ में और ज़्यादा शोध किये जाने की ज़रूरत है।