साइबर जीआईएस का अवलोकन

धर्मेंद्र कुमार
वैज्ञानिक , जीआईटी एवं डीएल
dharmendra@iirs.gov.in

अनुक्रमणिका

जीआईएस क्या है

- GIS का पूरा नाम Geographic Information System है जिसे हिंदी में भौगोलिक सूचना प्रणाली कहा जाता है. यह एक अवधारणात्मक रूपरेखा है जो स्थानिक और भौगोलिक डेटा को रखने और विश्लेषण करने की क्षमता प्रदान करती है।
- जीआईएस एप्लिकेशन (या जीआईएस ऐप) कंप्यूटर आधारित उपकरण होता हैं जो उपयोगकर्ता को इंटरएक्टिव क्वेरी (उपयोगकर्ता-निर्मित खोजों) बनाने, स्थानिक और गैर-स्थानिक डेटा को संग्रहीत करने और संपादित करने, स्थानिक सूचना आउटपुट का विश्लेषण करने और इन परिष्कृत परिणामों को परोक्ष रूप से साझा करने की अनुमति देते हैं। उन्हें नक्शे के रूप में प्रस्तुत किया जा सकता है.
- एक अन्य परिपेक्ष मे जीआईएस एक भौगोलिक सूचना विज्ञान है। जो भौगोलिक अवधारणाओं, अनुप्रयोगों और प्रणालियों के वैज्ञानिक अध्ययन को आमतौर पर GIS के रूप में आरंभिक रूप में परिभाषित किया जाता है।

साइबर सुरक्षा क्या है

- साइबर सुरक्षा कंप्यूटर, नेटवर्क और सॉफ्टवेयर को साइबर आक्रमण से दूर रखने का तरीका है. जिसमे कंप्यूटर और नेटवर्क में उपलब्ध किसी भी प्रकार की सूचनाओं और डाटा को सुरक्षित और गोपनीय रखने का अभ्यास किया जाता है.
- साइबर सुरक्षा एक जटिल प्रक्रिया है. और इसमें कई प्रकार के जोखिम प्रबंधन, टूल, प्रशिक्षण, अभ्यास और तकनीक लगती है. इन सारी वस्तु का एक साथ रख कर ही साइबर सुरक्षा का कठोर प्रबंध किया जाता है. प्रशिक्षित विशेषज्ञों द्वारा लगातार अभ्यास और नवीन तकनीक पर अनुसंधान से साइबर सुरक्षा के लक्ष्य को प्राप्त किया जाता है.
- साइबर सुरक्षा की अन्य परिभाषा यह भी है कि इंटरनेट से जुड़े सिस्टम्स के लिए एक सुरक्षा होती है जो उपकरण (Devices) , Hardwares , Softwares और Data को साइबर अपराध से बचाने का काम करती है , आसान शब्दों में साइबर सुरक्षा सिस्टम, नेटवर्क और प्रोग्राम्स को डिजिटल हमलों से बचाने और रक्षा करने का अभ्यास है .

साइबर सुरक्षा क्या है

- साइबर सुरक्षा जिसे कंप्यूटर सुरक्षा या इनफार्मेशन टेक्नोलॉजी सुरक्षा भी कहा जाता है यह डाटा , कम्प्यूटर्स , नटवर्क और सॉफ्टवेयर को साइबर आक्रमण से दूर रखने का एक तरीका है . साइबर सुरक्षा में कंप्यूटर और नेटवर्क में उपलब्ध किसी भी प्रकार की सूचनाओं और डाटा को सुरक्षित और गोपनीय रखने का अभ्यास किया जाता है . यह सॉफ़्टवेयर या इलेक्ट्रॉनिक डेटा की चोरी या क्षति के साथ-साथ उनके द्वारा प्रदान की जाने वाली सेवाओं के विघटन या गलत पहचान से कंप्यूटर सिस्टम और नेटवर्क की सुरक्षा है।
- इसका अर्थ इंटरनेट पर सुरक्षा से है जब आप इंटरनेट यूज़ करते है या इंटरनेट से जुड़े होते है तब कई प्रकार का खतरा आप पर बना रहता है क्योंकि हैकर्स काफी सारे अलग अलग तरीकों से साइबर सुरक्षा का उल्लंघन करके आपके सिस्टम तक पहुँच सकते है और आपके पर्सनल डाटा का गलत इस्तेमाल कर सकते है इसी खतरे को रोकने के लिए साइबर सुरक्षा का उपयोग किया जाता है। इंटरनेट नेटवर्क से जुडी Devices , Softwares और Data और नेटवर्क को सुरक्षा प्रदान करना होता है जिसको सुरक्षा परतों द्वारा सुरक्षित किया जाता है।

साइबर सुरक्षा रणनीति

- एक मजबूत साइबर सुरक्षा रणनीति में साइबर अपराध से बचाव के लिए सुरक्षा की परतें होती हैं। जिसमें ऐसे साइबर हमलों से बचाव शामिल हैं जो डेटा तक पहुंचने, बदलने या नष्ट करने का प्रयास करते हैं; उपयोगकर्ताओं या संगठन से धन उगाहना; या सामान्य व्यावसायिक संचालन को बाधित करने का लक्ष्य है। रणनीति के प्रमुख बिन्दुओं को नीचे संबोधित किया गया है:
  - महत्वपूर्ण बुनियादी ढांचा सुरक्षा - कंप्यूटर सिस्टम, नेटवर्क और अन्य संपत्तियों की सुरक्षा के लिए अभ्यास जो समाज राष्ट्रीय सुरक्षा, आर्थिक स्वास्थ्य और/या सार्वजनिक सुरक्षा के लिए निर्भर करता है।
  - नेटवर्क सुरक्षा - एक कंप्यूटर नेटवर्क को घुसपैठियों से बचाने के लिए सुरक्षा उपाय, जिसमें वायर्ड और वायरलेस (वाई-फाई) दोनों कनेक्शन शामिल हैं।
  - एप्लिकेशन सुरक्षा - ऐसी प्रक्रियाएं जो ऑन-प्रिमाइसेस और क्लाउड में काम कर रहे एप्लिकेशन को सुरक्षित रखने में मदद करती हैं। डेटा को कैसे संभाला जाता है, उपयोगकर्ता प्रमाणीकरण, आदि के लिए विचारों के साथ डिजाइन चरण में अनुप्रयोगों में सुरक्षा का निर्माण किया जाना चाहिए।

साइबर सुरक्षा रणनीति

- क्लाउड सुरक्षा - विशेष रूप से, सच्ची गोपनीय कंप्यूटिंग जो ग्राहक की गोपनीयता, व्यावसायिक आवश्यकताओं और नियामक अनुपालन का समर्थन करने के लिए क्लाउड डेटा को स्थिर रूप से (भंडारण में), गति में (जैसा कि यह यात्रा करता है, क्लाउड से और भीतर) और उपयोग में (प्रसंस्करण के दौरान) मानक रूप से समाहित करता है, जिसमे महत्वपूर्ण बुनियादी ढांचा सुरक्षा - कंप्यूटर सिस्टम, नेटवर्क और अन्य संपत्तियों की सुरक्षा के लिए अभ्यास जो समाज राष्ट्रीय सुरक्षा, आर्थिक स्वास्थ्य और/या सार्वजनिक सुरक्षा आदि शामिल है।
- सूचना सुरक्षा - डेटा सुरक्षा उपाय, जैसे सामान्य डेटा संरक्षण विनियमन या जीडीपीआर, जो आपके सबसे संवेदनशील डेटा को अनधिकृत पहुंच, जोखिम या चोरी से सुरक्षित करते हैं।

साइबर सुरक्षा रणनीति

- अंतिम उपयोगकर्ता शिक्षा - समापन बिंदु सुरक्षा को मजबूत करने के लिए पूरे संगठन में सुरक्षा जागरूकता का निर्माण। उदाहरण के लिए, उपयोगकर्ताओं को संदिग्ध ईमेल अनुलग्नकों को हटाने, अज्ञात USB उपकरणों के उपयोग से बचने आदि के लिए प्रशिक्षित किया जा सकता है।
- डिजास्टर रिकवरी / बिजनेस निरंतरता योजना - अनियोजित घटनाओं, जैसे प्राकृतिक आपदाओं, बिजली की कटौती, या साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने के लिए उपकरण और प्रक्रियाएं, प्रमुख कार्यों में न्यूनतम व्यवधान के साथ।

साइबर सुरक्षा के प्रकार

- साइबर सुरक्षा के प्रकार ; साइबर सुरक्षा डिजिटल हमलों से कंप्यूटर, सर्वर, मोबाइल डिवाइस, इलेक्ट्रॉनिक सिस्टम, नेटवर्क और डेटा का बचाव करने का एक अभ्यास है , साइबर सुरक्षा को Information Security /Information Technology Security तथा इलेक्ट्रॉनिक इन्फॉर्मेशन सिक्योरिटी भी कहा जाता है .
- साइबर सुरक्षा में डाटा सुरक्षित रखने के लिए अलग अलग तत्वों का समावेश होता है , साइबर में सुरक्षा अलग अलग परतों द्वारा नेटवर्क को अधिक से अधिक सुरक्षा प्रदान की जाती है। साइबर सुरक्षा एक काफी महत्वपूर्ण विषय है जिसके निम्नलिखित प्रकार होते है.
  - नेटवर्क सुरक्षा : इसमें नेटवर्क की Incoming और Outgoing ट्रैफिक अर्थात नेटवर्क से आने जाने वाली ट्रैफिक को कंट्रोल तथा मैनेज किया जाता है जिसमे नेटवर्क में आने वाले Attacks और Threats को रोका जाता है इस सुरक्षा को आप नेटवर्क की पहली परत भी कह सकते है .

साइबर सुरक्षा के प्रकार

- एप्लीकेशन सुरक्षा: इसमें सॉफ्टवेयर और उपकरणो को Threats से बचाने का अभ्यास किया जाता है , जितनी भी ऍप्लिकेशन्स नेटवर्क में इस्तेमाल होती है उनके development और installation को ध्यान में रखा जाता है। Application Security में Application के डेवलपमेंट के दौरान उनकी सुरक्षा को लेकर विशेष ध्यान रखा जाता है और इंस्टालेशन के दौरान भी इस चीज का विशेष ध्यान रखा जाता है .
- सूचना सुरक्षा : इस साइबर सुरक्षा के प्रकार में डाटा को सुरक्षित रखना और उसे डिजिटल हमलों से बचाना यह मुख्य उद्देश्य होता है Data स्टोर डाटा हो या प्रवाहित दोनों को सुरक्षित रखा जाता है ।
- ईमेल सुरक्षा : ईमेल को सुरक्षित रखने के लिए और ईमेल से होने वाले अटैक्स से बचने के लिए कई प्रकार के Email Security Devices तथा Software का प्रयोग किया जाता है ।

साइबर सुरक्षा के प्रकार

- नेटवर्क एक्सेस कंट्रोल (Network Access Control) यह किसी भी यूजर को नेटवर्क से जुड़ते समय की काफी सुरक्षित प्रक्रिया होती है जिसमे Users के Roles के अनुसार नेटवर्क में जुड़ने के लिए पॉलिसी बना दी जाती है जिस कारण कोई भी अन्य यूजर नेटवर्क से नहीं जुड़ सकता क्योंकि यहाँ पर नेटवर्क से जुड़ने के अधिकारों को सिमित कर दिया जाता है .
- डाटा लॉस प्रिवेंशन (Data Loss Prevention) इस प्रक्रिया में डाटा को सुरक्षित रखा जाता है और एनकोड किया जाता है जिससे किसी भी प्रकार से डाटा चोरी या लीक ना हो पाएं .

साइबर हमलों के प्रकार

- एस क्यू एल इंजेक्शन: यह यह साइबर हमले का एक प्रकार है जिसमे साइबर अपराधी यूजर के के डाटा को डेटाबेस से चुराता है तथा उसे नियंत्रित करता है । यूजर के डेटाबेस में कमजोरिया ढूंढकर साइबर अपराधी कुछ विद्वेषपूर्ण SQL queries और कोड के माध्यम से यूजर के डटबसे तक पोहोंच जाते है और उसे चुरा लेते है तथा नियंत्रित करते है ।
- मालवेयर : मालवेयर अटैक साइबर हमलों का सबसे कॉमन प्रकारों में से एक है। Malicious (विद्वेषपूर्ण) सॉफ्टवेयर को मालवेयर कहा जाता है। Malware यह हैकर्स या साइबर अपराधियों द्वारा बनाया हुआ एक खतरनाक कंप्यूटर सॉफ्टवेयर प्रोग्राम होता है जो अन्य Users को परेशान करने और उनकी सिस्टम्स को खराब (damage) करने हेतु बनाया गया होता है । Malware के भी अनेक प्रकार के होते हैं जैसे एडवेयर बॉटनेट्स वायरस ट्रोजन्स स्पाई-वेयर रैनसमवेयर

साइबर हमलों के प्रकार

- अंदरूनी धमकी :वर्तमान या पूर्व कर्मचारी, व्यावसायिक साझेदार, ठेकेदार, या कोई भी व्यक्ति जिसकी पूर्व में सिस्टम या नेटवर्क तक पहुंच है, यदि वे अपनी एक्सेस अनुमतियों का दुरुपयोग करते हैं, तो उन्हें एक अंदरूनी खतरा माना जा सकता है। अंदरूनी खतरे पारंपरिक सुरक्षा समाधानों जैसे फायरवॉल और घुसपैठ का पता लगाने वाली प्रणालियों के लिए अदृश्य हो सकते हैं, जो बाहरी खतरों पर ध्यान केंद्रित करते हैं।

- मैन-इन-दी-मिडिल : यह साइबर हमले का एक ऐसा प्रकार है जिसमे कोई दो लोगों के कम्युनिकेशन के बिच में साइबर अपराधी नेटवर्क के साथ छेड़छाड़ करके कम्युनिकेशन का एक्सेस ले लेते है और उसे कम्युनिकेशन करते है , इस साइबर हमले से अटैकर्स Users के बिच में चल रहे कम्युनिकेशन को एक्सेस कर लेते है जिसकी यूजर को कोई जानकारी भी नहीं होती है।

साइबर हमलों के प्रकार

- फिशिंग : यह साइबर हमले का एक प्रकार है जिसमे साइबर अपराधी यूजर को Fake Email या Fake SMS के जरिये एक फर्जी लिंक भेजता है जिससे यूजर की पर्सनल डिटेल्स को चुराया जाता है जैसे Login ID और Password , Credit Card / Debit Card की डिटेल्स .
- डिस्ट्रीब्यूटेड डिनायल-ऑफ-सर्विस (DDoS) :एक DDoS हमला एक सर्वर, वेबसाइट या नेटवर्क को ट्रैफ़िक के साथ ओवरलोड करके क्रैश करने का प्रयास करता है, आमतौर पर कई समन्वित प्रणालियों से। डीडीओएस सरल नेटवर्क प्रबंधन प्रोटोकॉल (एसएनएमपी) के माध्यम से उद्यम नेटवर्क पर हमला करता है, जो मॉडेम, प्रिंटर, स्विच, राउटर और सर्वर के लिए उपयोग किया जाता है।
- जीरो डे : यह साइबर हमले का एक ऐसा प्रकार है जिसमे किसी सिस्टम के सॉफ्टवेयर में Loopholes को ढूंढ कर उन्हें निशाना बनाया जाता है इस अटैक में सॉफ्टवेयर को निशाना बनाकर साइबर अपराधियों द्वारा उस सॉफ्टवेयर के साथ छेड़छाड़ की जाती है।

साइबर हमलों के प्रकार

- डेनियल-ऑफ़-सर्विस अटैक: इस साइबर हमले में साइबर अपराधियों द्वारा किसी यूजर या संस्था के सिस्टम और नेटवर्क को कार्य करने से रोका जाता है। इस साइबर हमले में साइबर क्रिमिनल एक कंप्यूटर सिस्टम को ट्रैफिक के साथ नेटवर्क और सर्वर को भारी करके वैध अनुरोधों को पूरा करने से रोकते हैं इस हमले से साइबर अपराधी सिस्टम को अनुपयोगी बना सकते है और किसी संगठन या किसी व्यक्ति के महत्वपूर्ण कार्यों को रोक सकते है।

- साइबर हमलों के इसके अलावा भी कई सारे प्रकार है क्योंकि साइबर अपराधी नए नए तरीके और तकनीकें ढूंढते ही रहते है और दुनिया में कई सारे ऐसे साइबर हमलों की तकनीकें है जो अभी तक दुनिया के सामने नहीं आयी है जो आने वाले समय में शायद ही हमे पता चलें।

साइबर सुरक्षा और जीआईएस

- एक्सेस कंट्रोल और एसेट मैनेजमेंट के लिए भू-स्थानिक डेटा लाना: अभिगम नियंत्रण साइबर सुरक्षा का एक महत्वपूर्ण हिस्सा है क्योंकि यह सुनिश्चित करता है कि लोग अपने आवश्यक संसाधनों का उपयोग कर सकें। साथ ही, यह अनावश्यक रूप से किसी कंपनी की सुरक्षा प्रथाओं से समझौता करने की पहुंच प्रदान नहीं करता है। लक्ष्य संगठन के सुरक्षा मानकों को बनाए रखते हुए उपयोगकर्ता के लिए घर्षण को कम करना है।
- पैरामीटर सेट करने के लिए विभिन्न विकल्प मौजूद हैं जो किसी व्यक्ति को विशिष्ट संसाधनों का उपयोग करने की अनुमति देते हैं या अस्वीकार करते हैं। कुछ कंपनियां किसी व्यक्ति या डिवाइस के चारों ओर एक आभासी सीमा बनाने के लिए भू-स्थानिक डेटा का उपयोग करती हैं। उदाहरण के लिए, एक अधिकृत व्यक्ति को काम पर गोपनीय जानकारी के डेटाबेस तक पहुंचने की अनुमति हो सकती है, लेकिन घर से नहीं - या कार्यस्थल से पांच मील दूर भी।
- यह दृष्टिकोण कंपनी के नेटवर्क से जुड़े भौतिक उपकरणों के लिए भी काम कर सकता है। यदि कोई कर्मचारी इस नियम की उपेक्षा करता है कि एक महंगे कनेक्टेड गैजेट को साइट पर ही रहना चाहिए और उसे घर लाने का प्रयास करता है, तो एक व्यवस्थापक अलर्ट प्राप्त कर सकता है और आगे की कार्रवाई कर सकता है। एक्सेस कंट्रोल टूल आमतौर पर समूहों के लिए अनुमतियां सेट करने या संगठन की जरूरतों के आधार पर कस्टम पैरामीटर लागू करने की अनुमति देते हैं। भू-स्थानिक डेटा उन विशिष्टताओं पर भी लागू हो सकता है।

साइबर सुरक्षा और जीआईएस

- हमले के परिदृश्य पर व्यापक नज़र डालें : व्यवसाय विभिन्न तरीकों से अपने संचालन को बेहतर बनाने के लिए डेटा मैपिंग पर भरोसा करते हैं। उदाहरण के लिए, एक दंत चिकित्सा पद्धति एक नक्शा बना सकती है जिसमें रोगी स्थानों का टूटना दिखाया जा सकता है और जहां सुविधा प्रतिनिधियों को अधिक लोगों को आकर्षित करने के लिए अधिक विपणन में निवेश करना चाहिए। वैकल्पिक रूप से, एक तलाक वकील एक का उपयोग यह देखने के लिए कर सकता है कि किसी शहर या राज्य के किन क्षेत्रों में जनसंख्या डेटा के आधार पर उनकी सेवाओं की सबसे अधिक आवश्यकता है।

- साइबर सुरक्षा पेशेवर साइबर हमले के वास्तविक समय के उदाहरणों को ट्रैक करके कुछ ऐसा ही करते हैं। विभिन्न प्रकार के इंटरेक्टिव मानचित्र मौजूद हैं, जिनमें रंग-कोडिंग और फ़िल्टरिंग वाले मानचित्र शामिल हैं, जो उपयोगकर्ताओं को डेटा को कुशलतापूर्वक पचाने और आवश्यक होने पर उस पर कार्य करने में मदद करते हैं।

- ये स्थान-आधारित संसाधन आईटी सुरक्षा विशेषज्ञों को उन रुझानों को नोटिस करने में मदद करते हैं जिन्हें वे अन्यथा अनदेखा कर सकते हैं। फिर वे हमलों को रोकने और उनसे निपटने के लिए बेहतर तरीके से तैयार होते हैं।

साइबर सुरक्षा और जीआईएस

- राष्ट्रीय सुरक्षा के लिए जीपीएस सिस्टम में सुधार का आकलन करना:

- ग्लोबल पोजिशनिंग सिस्टम (जीपीएस) डेटा ने हाल ही में ट्रम्प प्रशासन का ध्यान आकर्षित किया। इस विषय ने संयुक्त राज्य के नेता को एक कार्यकारी आदेश जारी करने के लिए जीपीएस के उपयोग और स्थिति, नेविगेशन और समय को प्रभावित करने वाली समान तकनीकों पर सार्वजनिक इनपुट मांगने का कारण बना दिया।

- वर्तमान उपयोग के मामलों से अधिक परिचित होने के अलावा, संघीय अधिकारियों ने यह समझने की कोशिश की कि ऐसी प्रणालियों की साइबर सुरक्षा को कैसे मजबूत किया जाए। उन्होंने उन प्रौद्योगिकियों पर देश की पहले से ही उच्च और बढ़ती निर्भरता को पहचाना। खराब साइबर सुरक्षा विदेशी हैकरों से सुरक्षित रहने के देश के प्रयासों को सीधे नुकसान पहुंचा सकती है या प्रौद्योगिकी के उपयोग के मामले में संयुक्त राज्य अमेरिका को अन्य देशों से पीछे कर सकती है।

- अनुरोधित जानकारी एकत्र करने के बाद, इस परियोजना पर काम करने वाली टीम का लक्ष्य फरवरी 2021 तक इस मामले पर एक रिपोर्ट का अंतिम संस्करण जारी करना है। हालांकि, यह जल्द ही एक मसौदा संस्करण पेश करेगा, और जनता अब तक की सामग्री पर टिप्पणी कर सकती है।

साइबर सुरक्षा और जीआईएस

- साइबर घटनाओं के प्रभाव को समझना: भौगोलिक सूचना प्रणाली (जीआईएस) सामग्री एक अन्य प्रकार का भू-स्थानिक डेटा है जो साइबर सुरक्षा को प्रभावित करती है। जब साइबर सुरक्षा व्यवसायी ऑनलाइन गतिविधि को भू-स्थानिक परत से जोड़ते हैं, तो उन्हें एक स्पष्ट तस्वीर मिलती है कि नेटवर्क गतिविधि कहां होती है और किन उपकरणों से होती है। मिशन-महत्वपूर्ण नेटवर्क के लिए इस तरह के विवरण महत्वपूर्ण हो जाते हैं, जैसे कि संचार, ऊर्जा आपूर्ति या आपदा वसूली से जुड़े।

- उपकरण आज उपलब्ध हैं जो किसी संगठन के मौजूदा तकनीकी ढांचे के भीतर जीआईएस डेटा को एकीकृत करने की अनुमति देते हैं। उपयोगकर्ता विभागों के बीच सहयोग की सुविधा के लिए डेटा को अन्य अधिकृत पार्टियों के साथ भी साझा कर सकते हैं।

- उपयोगकर्ताओं को यह समझने में सक्षम बनाने के अलावा कि भविष्य के साइबर हमले उन्हें कैसे प्रभावित कर सकते हैं, ये नवाचार दुर्भावनापूर्ण घुसपैठ से तेजी से, अधिक आत्मविश्वास से उबरने को बढ़ावा देते हैं और उन्हें पहले स्थान पर रोक सकते हैं। इसके अलावा, वे प्रकट कर सकते हैं कि नेटवर्क के किन पहलुओं में सबसे अधिक अनसुलझे मुद्दे हैं, साइबर सुरक्षा पेशेवरों को अपने काम को प्राथमिकता देने में सक्षम बनाते हैं।

साइबर सुरक्षा और जीआईएस

- साइबर सुरक्षा प्रयासों में सुधार
- ये उदाहरण दिखाते हैं कि साइबर सुरक्षा योजनाओं में भू-स्थानिक डेटा को शामिल करना क्यों आवश्यक है। जैसे-जैसे हैकर्स के हमले अधिक विस्तृत और हानिकारक होते जाते हैं, सुरक्षा टीमों को नेटवर्क और डिजिटल इन्फ्रास्ट्रक्चर को सुरक्षित रखने के सर्वोत्तम तरीकों का निर्धारण करना चाहिए। भू-स्थानिक डेटा उपयोगी जानकारी प्रदान कर सकता है जो अधिक प्रभावी निर्णय लेने की ओर ले जाता है।

साइबर सुरक्षा मे जीआईएस अनुप्रयोग

- साइबर सुरक्षा और भू-स्थानिक प्रौद्योगिकियां: वैसे तो साइबर सुरक्षा सबसे बड़े क्षेत्रों में से एक रही है, जिसमें जीआईएस और सुरक्षा का उदय हुआ है। विशेष रूप से, महत्वपूर्ण बुनियादी ढांचे के खिलाफ हमले, जैसे कि विद्युत शक्ति प्रणाली, जीआईएस अनुप्रयोगों द्वारा संबोधित एक महत्वपूर्ण भेद्यता क्षेत्र रहा है।

- इसे एक उदाहरण द्वारा समझने का प्रयास करते है। इलेक्ट्रिक पावर जीआईएस चीन में पावर ग्रिड निर्माण को आगे बढ़ाने के लिए प्रमुख सूचना प्रौद्योगिकियों में से एक है, और व्यापक रूप से पावर ग्रिड निर्माण योजना, मौसम और बिजली वितरण प्रबंधन में उपयोग किया जाता है। मोबाइल अनुप्रयोगों पर आधारित विद्युत शक्ति जीआईएस की शुरूआत भौगोलिक सूचना प्रणाली का एक प्रभावी विस्तार है जिसका व्यापक रूप से विद्युत ऊर्जा उद्योग में उपयोग किया गया है। यह देश के लिए विश्वसनीय, सस्ती और टिकाऊ बिजली सेवा प्रदान करता है। विद्युत शक्ति जीआईएस के सामान्य संचालन को बनाए रखने के लिए सटीक राज्य अनुमान महत्वपूर्ण शर्तें हैं। प्रदान कर सकते हैं, जिससे ऊर्जा का अनुचित संतुलन और आउटेज हो सकता है।

साइबर सुरक्षा मे जीआईएस अनुप्रयोग

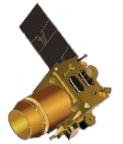
- हाल के शोध से पता चला है कि हमलावर जटिल झूठे डेटा को पावर सिस्टम में इंजेक्ट कर सकते हैं। इस नए प्रकार के झूठे डेटा का इंजेक्शन हमला (लोड अखंडता हमला एलआईए) हमले के उद्देश्य को प्राप्त करने के लिए नियमित पहचान को सफलतापूर्वक बायपास कर सकता है, ताकि नियंत्रण केंद्र गलत निर्णयों की एक श्रृंखला बना सके। अंततः, ग्रिड में बिजली के असमान वितरण के लिए अग्रणी। मोबाइल एप्लिकेशन के आधार पर इलेक्ट्रिक पावर जीआईएस सिस्टम की सुरक्षा सुनिश्चित करने के लिए, हमले तंत्र का विश्लेषण करना और एक नए प्रकार के हमले का प्रस्ताव देना और बिजली के वातावरण में संबंधित पहचान विधि और रोकथाम रणनीति का अध्ययन करना बहुत महत्वपूर्ण है।

- बिजली प्रदाता अक्सर मांग के अनुमानों पर निर्भर करते हैं जो बिजली को संतुलित और प्रदान करता है जहां इसकी सबसे अधिक आवश्यकता होती है। साइबर हमले बिजली के निर्णय लेने वालों को गलत डेटा भेज कर पूरे तंत्र को भारी हानी पहुंचा सकते हैं।

साइबर सुरक्षा मे जीआईएस अनुप्रयोग

- डिटेक्शन सॉफ्टवेयर ने ऊर्जा के वितरण की निगरानी के लिए जीआईएस पावर ग्रिड मैपिंग का उपयोग किया है, लेकिन वितरण भार में विसंगतियों का पता लगाने के लिए सुरक्षा पहचान एल्गोरिदम को भी एकीकृत किया गया है जो यह पता लगाता है कि क्या ऑपरेटरों को गलत जानकारी भेजी जा रही है। इरादा वितरण भार और किए जा रहे निर्णयों के सापेक्ष विषम फ़ीड खोजने का है। यह स्मार्ट-ग्रिड अनुप्रयोगों का हिस्सा बन गया है जो पिछले एक दशक में सक्रिय विकास में हैं।

- हम जो देखते हैं वह यह है कि सॉफ्टवेयर जीआईएस विधियों या अनुप्रयोगों का उपयोग पारंपरिक सुरक्षा उपकरणों, जैसे सीसीटीवी, लेकिन साथ ही विभिन्न प्रकार के अनुप्रयोगों के लिए डेटा के अन्य नए रूपों के साथ करता है। यह न केवल सुरक्षा में सुधार करने में मदद करता है बल्कि भौतिक सुरक्षा खतरों के लिए प्रत्याशा और योजना को और अधिक आसानी से करने की अनुमति देता है बल्कि महत्वपूर्ण बुनियादी ढांचे जैसे क्षेत्रों पर साइबर सुरक्षा भी करता है।



अस्वीकरण

प्रस्तुति के लिए सामग्री को विभिन्न स्रोतों जैसे कि किताबें, ट्यूटोरियल (ऑनलाइन और ऑफलाइन), व्याख्यान नोट्स, इंटरनेट पर उपलब्ध कई संसाधनों से संकलित किया गया है। इस व्याख्यान/प्रस्तुति में निहित जानकारी केवल सामान्य जानकारी और शिक्षा के उद्देश्य के लिए है। जबकि हम जानकारी को अद्यतित और सही रखने का प्रयास करते हैं, हम सामग्री की पूर्णता और सटीकता के बारे में किसी भी प्रकार का कोई प्रतिनिधित्व नहीं करते हैं। इस प्रस्तुति सामग्री के माध्यम से साझा की गई जानकारी का उपयोग केवल शैक्षिक उद्देश्य के लिए किया जाना चाहिए।

धन्यवाद

Contact Details of the Faculty:

Email- dharmendra@iirs.gov.in
Tel- 0135 252 4342