# इंटरनेट ऑफ थिंग्स की सुरक्षा

## प्रिलिम्स के लिये:

इंटरनेट ऑफ थिंग्स (IoT), आर्टिफिशियल इंटेलिजेंस / मशीन लर्निंग, क्लाउड / एज कंप्यूटिंग

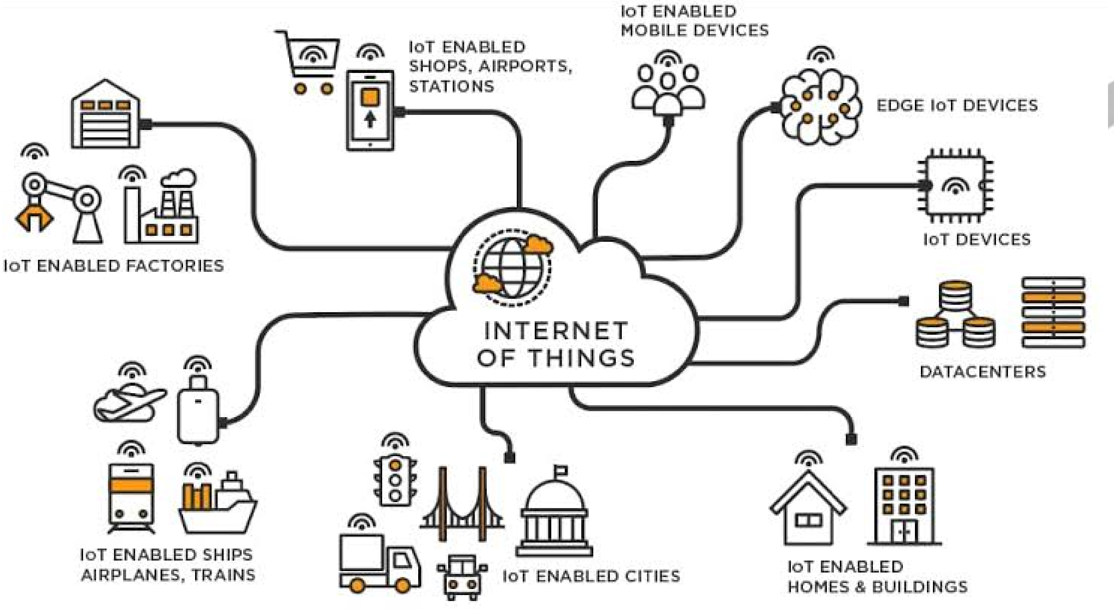
## मेन्स के लिये:

उपभोक्ता इंटरनेट ऑफ थिंग्स (IoT) को सुरक्षित करने के लिये अभ्यास संहिता, साइबर-सिक्योरिटी, इंटरनेट ऑफ थिंग्स और इसके उपयोग।

## चर्चा में क्यों?

हाल ही में संचार मंत्रालय, दूरसंचार विभाग के अंतर्गत आने वाले दूरसंचार इंजीनियरिंग केंद्र (TEC) ने उपभोक्ता इंटरनेट ऑफ थिंग्स (IoT) उपकरणों को सुरक्षित करने के उद्देश्य से **"उपभोक्ता इंटरनेट ऑफ थिंग्स (IoT) को सुरक्षित करने के लिये अभ्यास संहिता"** (Code of Practice for Securing Consumer Internet of Things) नामक एक रिपोर्ट जारी की है।

- ये दिशा-निर्देश उपभोक्ता IoT उपकरणों और पारिस्थितिकी तंत्र को सुरक्षित करने के साथ-साथ सुभेद्यताओं को प्रबंधित करने में मदद करेंगे।




//

## प्रमुख बिंदु

- **इंटरनेट ऑफ थिंग्स:**
  - **परिभाषा**: सामान्य रूप से यह इंटरनेट का एक नेटवर्क है जो उन वस्तुओं को आपस में जोड़ता है जो डेटा को संग्रहित और परिवर्तित करने में सक्षम हैं।
  - **फास्टिंग ग्रोइंग टेक्नोलॉजी में से एक:** यह दुनिया भर में सबसे तेज़ी से उभरती प्रौद्योगिकियों में से एक है, जो समाज, उद्योग और उपभोक्ताओं के लिये काफी लाभकारी अवसर प्रदान करती है।
  - **IoT का उपयोग:** इसका उपयोग बिजली, मोटर वाहन, सुरक्षा और निगरानी, दूरस्थ स्वास्थ्य प्रबंधन, कृषि, स्मार्ट होम और स्मार्ट

सिटी आदि में प्रयुक्त उपकरणों का उपयोग करके स्मार्ट बुनियादी ढाँचे को बनाने के लिये किया जा रहा है।

- **एक स्मार्ट डिवाइस**- यह अत्यंत आधुनिक इलेक्ट्रॉनिक उपकरण है जो स्वायत्त कंप्यूटिंग और डेटा एक्सचेंज के लिये तार या वायरलेस के माध्यम से अन्य उपकरणों से कनेक्ट करने में सक्षम है।

- **पूरक तकनीकें:** IoT सेंसर, संचार प्रौद्योगिकियों (सेलुलर और गैर-सेलुलर), आर्टफिशियल इंटेलिजेंस / मशीन लर्निंग, क्लाउड / एज कंप्यूटिंग आदि जैसी कई तकनीकों में हालिया प्रगति से लाभान्वित हुआ है।

- **IOT का परिमाण:** यह अनुमान लगाया गया है कि वर्ष 2025 तक वैश्विक स्तर पर लगभग 11.4 बिलियन उपभोक्ता IoT डिवाइस और 13.3 बिलियन इंटरप्राइजेज़ IoT डिवाइस से युक्त होंगे, यानी उपभोक्ता IoT डिवाइस सभी IoT उपकरणों का लगभग 45% हिस्सा होंगे।
  - 'मार्केट्स एंड मार्केट्स' द्वारा प्रकाशित एक मार्केट रिसर्च रिपोर्ट के अनुसार, वैश्विक IoT सुरक्षा बाज़ार का आकार वर्ष 2018 में USD 8.2 बिलियन से बढ़कर वर्ष 2023 तक USD 35.2 बिलियन होने की उम्मीद है।
- **दिशा-निर्देशों की आवश्यकता:**
  - **प्रत्याशित वृद्धि:** IoT उपकरणों की प्रत्याशित वृद्धि को देखते हुए यह सुनिश्चित करना महत्त्वपूर्ण है कि IoT समापन बिंदु सुरक्षा और सुरक्षा मानकों का अनुपालन करते हैं।
  - **साइबर-सुरक्षा हमला:** दैनिक जीवन में उपयोग किये जा रहे उपकरणों/नेटवर्क की हैकिंग से कंपनियों, संगठनों, राष्ट्रों और अधिक महत्त्वपूर्ण रूप से लोगों को नुकसान होगा।
    - इसलिये IoT इकोसिस्टम को एंड-टू-एंड यानी डिवाइस से एप्लीकेशन तक सुरक्षित करना बहुत महत्त्वपूर्ण है।
    - कनेक्टेड IoT उपकरणों के लिये 'एंड टू एंड' सुरक्षा सुनिश्चित करना इस बाज़ार में सफलता की कुंजी है। इस सुरक्षा के बिना IoT का अस्तित्व समाप्त हो जाएगा।
  - **गोपनीयता संबंधी चिंताएँ:** इस डेटा-संचालित भविष्य में सरकारी निगरानी में वृद्धि और नागरिक अधिकारों के परिणामी अतिक्रमण, असंतोष या हाशिए के समुदायों के दमन की संभावना के बारे में चिंता बढ़ रही है।
  - **साइबर सुरक्षा हमले के परिणाम:** ऐसे हमलों के संभावित परिणामों में शामिल हो सकते हैं:
    - महत्त्वपूर्ण सेवाओं/बुनियादी ढाँचे में रुकावट।
    - निजिता का उल्लंघन।
    - जीवन, धन, समय, संपत्ति, स्वास्थ्य, संबंधों आदि की हानि।
    - नागरिक अशांति सहित राष्ट्रीय स्तर पर व्यवधान।
- **उपभोक्ता IoT हासिल करने के लिये दिशा-निर्देश:**
  - **कोई यूनिवर्सल डिफॉल्ट पासवर्ड नहीं:** प्रति डिवाइस सभी IoT डिवाइस डिफॉल्ट पासवर्ड अद्वितीय होंगे और/या डिवाइस प्रोविज़निंग के दौरान उपयोगकर्त्ता को एक पासवर्ड चुनने की आवश्यकता होगी जो सर्वोत्तम आदेशों का पालन करता हो।
  - **संवेदनशील रिपोर्ट को प्रबंधित करने के लिये एक साधन लागू करना:** IoT डेवलपर्स को भेद्यता प्रकटीकरण नीति के हिस्से के रूप में एक समर्पित सार्वजनिक संपर्क बिंदु प्रदान करना चाहिये।
  - **सॉफ्टवेयर को अद्यतन रखना:** IoT उपकरणों में **सॉफ्टवेयर** घटकों को सुरक्षित रूप से अद्यतन करने योग्य होना चाहिये।
  - **संवेदनशील सुरक्षा मापदंडों को सुरक्षित रूप से संग्रहीत करना** : IoT उपकरणों को सुरक्षा मापदंडों जैसे कि कुंजी और क्रेडेंशियल, प्रमाणपत्र, डिवाइस पहचान आदि जो कि डिवाइस के सुरक्षित संचालन के लिये महत्त्वपूर्ण हैं, को संग्रहीत करने की आवश्यकता हो सकती है।
  - **सुरक्षित संचार:** किसी भी दूरस्थ प्रबंधन और नियंत्रण सहित सुरक्षा-संवेदनशील डेटा, जो तकनीकी गुणों तथा डिवाइस के उपयोग हेतु उपयुक्त हो, को ट्रांज़िट में एन्क्रिप्ट किया जाना चाहिये।
  - **प्रत्यक्ष हमलों की बारंबारता को कम करना:** उपकरणों और सेवाओं को 'कम-से-कम विशेषाधिकार के सिद्धांत' पर काम करना चाहिये।
    - **'कम-से-कम विशेषाधिकार के सिद्धांत' के अनुसार, किसी व्यक्ति को केवल वही विशेषाधिकार दिये जाने चाहिये जो उसके कार्य को पूरा करने के लिये आवश्यक हों।**
  - **व्यक्तिगत डेटा की सुरक्षा सुनिश्चित करना:** यदि डिवाइस व्यक्तिगत डेटा को एकत्र या प्रसारित करता है, तो ऐसे डेटा को सुरक्षित रूप से संग्रहीत किया जाना चाहिये।
  - **सिस्टम को लचीला बनाना:** IoT उपकरणों और सेवाओं में लचीलापन लाया जाना चाहिये जहाँ उनका उपयोग अन्य भरोसेमंद सिस्टम द्वारा करना आवश्यक हो।

## आगे की राह

- **डेटा सुरक्षा से संबंधित चिंताओं को संबोधित करना:** IoT तकनीक स्पष्ट रूप से दुनिया भर के नागरिकों के लिये सकारात्मक रूप से महत्त्वपूर्ण है, जिससे अधिक लाभ के साथ गोपनीयता के लिये संभावित जोखिम भी उत्पन्न होता है।
  - डेटा संरक्षण हेतु इस चिंता को दूर करने की आवश्यकता होगी और IoT निर्माताओं को अपने उपकरणों के प्रति उपभोक्ता विश्वास को बनाए रखना होगा।
  - इस संदर्भ में डेटा संरक्षण विधेयक, 2019 सही दिशा में एक कदम है।
- **वैश्विक विचार-विमर्श की आवश्यकता:** वैश्विक स्तर पर कानून निर्माताओं, उपकरण निर्माताओं और कानून प्रवर्तन एजेंसियों को जोखिमों को कम करते हुए IoT से अधिक लाभ प्राप्त करने हेतु एक साथ आना चाहिये।

## स्रोत: पी.आई.बी

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/securing-internet-of-things