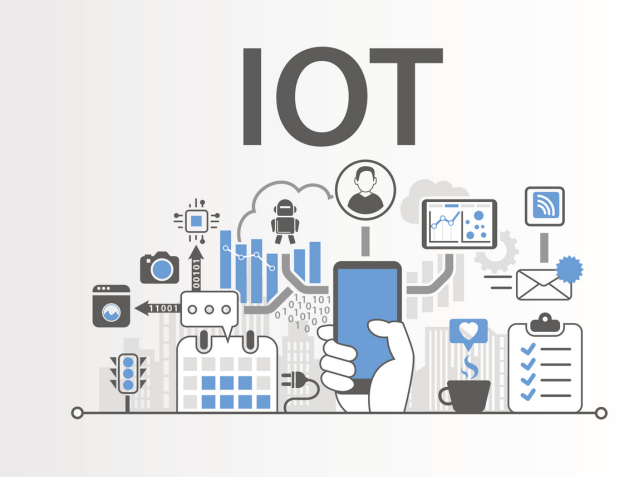
इंटरनेट ऑफ थिंग्स के युग में डाटा सुरक्षा की चुनौती



आज के समय में राजनैतिक एवं आर्थिक क्षेत्र में बडे-बड़े घोटाले और उलट-फेर हो रहे हैं। ऐसा माना जा रहा है कि इन सबके पीछे 'इंटरनेट ऑफ थिंग्स' का हाथ है। दरअसल, तकनीक की प्रगति के साथ हमारे अधिकांश उपकरण एक-दूसरे से जुड़े हुए रहने लगे हैं।

विश्व में तकनीक की दृष्टि से तीन बड़े स्तरों पर काम हो रहा है। इनमें (1) इंटरनेट ऑफ थिंग्स (2) आर्टिफिशियल इंटेलीजेंस या मशीन लर्निंग, और (3) क्रिप्टोकरंसी हैं।

यहाँ हम इंटरनेट ऑफ थिंग्स के बारे में बात कर रहे हैं। आज हमारे हर छोटे-बड़े उपकरण के द्वारा हमारी निजी जानकारियों का पता लगाया जा सकता है। इसका सीधा सा अर्थ इन उपकरणों को हैक करने से है।

एक स्मार्ट सिटी में सेंसर और कैमरे के जरिए नजर रखी जाती है। एक हैकर के लिए इनके जरिए सूचना एकत्रित करना कोई बड़ी बात नहीं है। इस सूचना की सुरक्षा के लिए एनक्रिप्शन ही अच्छा उपाय है, और क्रिप्टोग्रैफी के जरिए ऐसा करना संभव हो सकता है।

इंटरनेट ऑफ थिंग्स से जुड़े उपकरण की सुरक्षा के लिए मैसेज ऑथेन्टिकेशन कोड का इस्तेमाल किया जाना चाहिए। सामान्य भाषा में इसे वन टाइम पासवर्ड (ओ.टी.पी) कहते है। बैंक से संबंधित जानकारी, क्रेडिट कार्ड या डेबिट कार्ड आदि के लिए उपभोक्ता को इसी प्रकार की सुविधा दी जाती है।

डाटा सुरक्षा के क्षेत्र में 'लाइट वेट क्रिप्टोग्रैफी' तुलनात्मक रूप से अधिक सक्षम तकनीक है।

क्रिप्टोग्रैफी कोई जादू की छड़ी नहीं है, जिसे घुमाकर साइबर सुरक्षा का काम पूरा माना जा सके। यह एक गणितीय संरचना है, जो अत्यधिक जटिल होती है। लेकिन ऐसा नहीं कि इसका कोई तोड़ नहीं है। एनक्रिप्शन कितना भी जटिल

क्यों न हो, इसे हैक करने वाले तैयार होते जाते हैं। अतः यह एक निरंतर प्रक्रिया है। हमें हर समय सजग और प्रयत्नशील रहने की आवश्यकता है।

'द टाइम्स ऑफ इंडिया' में प्रकाशित अतानू विश्वास और विमल रॉय के लेख पर आधारित। 7 जून, 2018