एंड-टू-एंड एन्क्रिप्शन

प्रिलिम्स के लिये:

क्रिप्टोग्राफिक कुंजियाँ, डेटा सुरक्षा, डेटा सुरक्षा कानून।

मेन्स के लिये:

एंड-टू-एंड एन्क्रिप्शन के लाभ और हानि।

चर्चा में क्यों?

हाल ही में Apple ने घोषणा की है कि वह आईक्लाउड (iCloud) पर **एंड-टू-एंड एन्क्रिप्शन (E2EE)** द्वारा संरक्षित डेटा पॉइंट्स को 14 से 23 श्रेणियों तक बढ़ाएगा।

घोषणा का उद्देश्य:

- Apple द्वारा डेटा-ब्रीच-रिसर्च (data-breach-research) के अनुसार, वर्ष 2013 और 2021 के बीच डेटा ब्रीच की कुल संख्या तीन गुना से अधिक हो गई। अकेले वर्ष 2021 में 1.1 बिलियन व्यक्तिगत रिकॉर्ड का डेटा सामने आया।
- एंड-टू-एंड एन्क्रिप्शन के साथ, **क्लाउड में डेटा का उल्लंघन होने की स्थिति में भी उपयोगकर्त्ता का डेटा सुरक्षित रहेगा।** अच्छी तरह से वित्त पोषित समूहों द्वारा शुरू किये गए **हैकिंग हमलों के लक्ष्यों हेतु सुरक्षा की अतिरिक्त परत मूल्यवान होगी।**

एंड-टू-एंड एन्क्रिप्शन:

- **परिचय:**
  - एंड-टू-एंड एन्क्रिप्शन एक संचार प्रक्रिया है जो दो उपकरणों के बीच साझा किये जा रहे डेटा को एन्क्रिप्ट करती है।
  - यह क्लाउड सेवा प्रदाताओं, इंटरनेट सेवा प्रदाताओं (ISPs) और साइबर अपराधियों जैसे तीसरे पक्षों को डेटा तक पहुँचने से रोकता है, विशेषतः जब डेटा स्थानांतरित किया जा रहा हो।
- **तंत्र:**
  - संदेशों को एन्क्रिप्ट और डिक्रिप्ट करने के लिये उपयोग की जाने वाली क्रिप्टोग्राफिक कुंजियों को एंडपॉइंट्स पर संग्रहीत किया जाता है।
  - एंड-टू-एंड एन्क्रिप्शन की प्रक्रिया एक एल्गोरिथ्म का उपयोग करती है जो मानक पाठ को अपठनीय प्रारूप में बदल देती है।
  - इस प्रारूप को केवल डिक्रिप्शन कुंजियों वाले लोगों द्वारा अनस्क्रैम्बल किया और पढ़ा जा सकता है, जो केवल एंडपॉइंट्स पर संग्रहीत होते हैं और सेवा प्रदान करने वाली कंपनियों सहित किसी भी तीसरे पक्ष के साथ नहीं।
- **उपयोग:**
  - व्यावसायिक दस्तावेज़ों, वित्तीय विवरणों, कानूनी कार्यवाहियों और व्यक्तिगत वार्तालापों को स्थानांतरित करते समय E2EE का लंबे समय से उपयोग किया जाता रहा है।
  - संग्रहीत डेटा तक पहुँचने के दौरान इसका उपयोग उपयोगकर्त्ताओं के प्राधिकरण को नियंत्रित करने के लिये भी किया जा सकता है।
  - संचार को सुरक्षित करने के लिये **एंड-टू-एंड एन्क्रिप्शन का उपयोग किया जाता है।**
  - इसका उपयोग पासवर्ड सुरक्षित करने, **संग्रहीत डेटा की सुरक्षा और क्लाउड स्टोरेज पर डेटा की सुरक्षा के लिये भी किया जाता है।**

एंड-टू-एंड एन्क्रिप्शन के लाभ (E2EE):

- **संप्रेषण में सुरक्षा:**
  - एंड-टू-एंड एन्क्रिप्शन सार्वजनिक कुंजी क्रिप्टोग्राफी का उपयोग करता है, जो एंडपॉइंट उपकरणों पर निजी कुंजी संग्रहीत करता है।

संदेशों को केवल इन कुंजियों का उपयोग करके डिक्रिप्ट किया जा सकता है, इसलिये केवल **एंडपॉइंट डिवाइस तक पहुँच रखने वाले लोग ही संदेश को पढ़ने में सक्षम होते हैं।**

- **तीसरे पक्ष से सुरक्षा::**
  - E2EE यह सुनिश्चित करता है कि उपयोगकर्त्ता डेटा सेवा प्रदाताओं, क्लाउड स्टोरेज प्रदाताओं और एन्क्रिप्टेड डेटा को प्रबंधित करने वाली **कंपनियों सहित अनुचित पार्टियों से सुरक्षित है।**
- **हस्तक्षेप रहित:**
  - डिक्रिप्शन कुंजी को E2EE के साथ प्रदान करने की आवश्यकता नहीं है क्योंकि यह प्राप्तकर्त्ता के पास पहले से ही मौजूद होती है।
  - यदि सार्वजनिक कुंजी के साथ एन्क्रिप्ट किया गया किसी संदेश भेजे जाने के दौरान किसी प्रकार की छेड़छाड़ की जाती है, तो **प्राप्तकर्त्ता इसे डिक्रिप्ट नहीं कर पाएगा छेड़छाड़ की गई सामग्री तक पहुँच की सुविधा भी नहीं रहेगी।**
- **अनुपालन:**
  - कई उद्योग विनियामक अनुपालन कानूनों से बँधे हैं जिनके लिये **एन्क्रिप्शन-स्तर की डेटा सुरक्षा की आवश्यकता होती है।**
  - E2EE डेटा को अपठनीय बनाकर उसे सुरक्षित रखने में **संगठनों की मदद** कर सकता है।

E2EE से हानि:

- **समापन बिंदुओं को परिभाषित करने में जटिलता:**
  - कुछ E2EE कार्यान्वयन **एन्क्रिप्टेड डेटा को ट्रांसमिशन के दौरान कुछ बिंदुओं पर एन्क्रिप्ट और पुनः एन्क्रिप्ट करने की अनुमति देते हैं।**
  - यह संचार सर्किट के समापन बिंदुओं को स्पष्ट रूप से परिभाषित और अलग करता है। यदि **एंडपॉइंट्स/समापन बिंदुओं से छेड़छाड़ की जाती है, तो एन्क्रिप्टेड डेटा प्रकट हो सकता है।**
- **बहुत अधिक गोपनीयता:**
  - सरकार और कानून प्रवर्तन एजेंसियाँ चिंता व्यक्त करती हैं कि **E2EE अवैध सामग्री साझा करने वाले लोगों की रक्षा कर सकता** है क्योंकि सेवा प्रदाता कानून प्रवर्तन को सामग्री तक पहुँच प्रदान करने में असमर्थ हैं। ।
- **मेटाडेटा हेतु सुरक्षा का अभाव:**
  - हालाँकि संप्रेषण में संदेश एन्क्रिप्टेड होते हैं, सन्देश से संबंधित सूचना जैसे **संदेश की तिथि और भेजने वाले की जानकारी अभी भी दिखाई दे रही होती है** और यह डेटा का दुरुपयोग करने वालों के लिये सहायक हो सकती है।

भारत में एन्क्रिप्शन के लिये कानूनी ढाँचा:

- **न्यूनतम एन्क्रिप्शन मानक:**
  - **भारत में एन्क्रिप्शन संबंधी कोई विशिष्ट कानून नहीं है।** हालाँकि, **बैंकिंग, वित्त** और **दूरसंचार उद्योगों** को नियंत्रित करने वाले कई उद्योग मानदंडों में **न्यूनतम एन्क्रिप्शन मानक शामिल हैं जिनका उपयोग** लेनदेन की सुरक्षा के लिये किया जाना चाहिये।
- **एन्क्रिप्शन प्रौद्योगिकियों पर प्रतिबंध:**
  - ISP और DoT के बीच लाइसेंसिंग समझौते के अनुसार, **उपयोगकर्त्ताओं** को पूर्व मंज़ूरी के बिना सममित (सिमिट्रिक) कुंजी एल्गोरिदम या तुलनीय तरीकों का उपयोग करके **40 बिट्स से बड़े एन्क्रिप्शन मानकों का उपयोग करने की अनुमति नहीं है।**
  - ऐसे कई अतिरिक्त नियम और अनुशंसाएँ हैं **जो विशेष क्षेत्रों के लिये 40 बिट्स से अधिक एन्क्रिप्शन स्तर का उपयोग करते हैं।**
- **[सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021:]()**
  - सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021 पूर्व के सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश) नियम 2011 के स्थान पर लाया गया।
  - नियमों के एक नए सेट में व्हाट्सएप, टेलीग्राम, सिग्नल आदि जैसे सोशल मैसेजिंग एप्लिकेशन की एंड-टू-एंड एन्क्रिप्शन तकनीकों को प्रभावित करने की क्षमता है।
- **[सूचना प्रौद्योगिकी अधिनियम, 2000]()**:
  - यह संचार के इलेक्ट्रॉनिक और वायरलेस मोड को नियंत्रित करता है और यह एन्क्रिप्शन संबंधी किसी भी ठोस प्रावधान या नीति से रहित है।

[स्रोत: द हिंदू]()

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/end-to-end-encryption