विशेष/इन-डेप्थ: साइबर वर्ल्ड और डेटा एन्क्रिप्शन

drishtiias.com/hindi/printpdf/data-encryption

संदर्भ एवं पृष्ठभूमि

डेटा हमारी ज़िंदगी का अहम हिस्सा बन चुका है। लेकिन हमारी तमाम आर्थिक जानकारी, कान्टेक्ट नंबर, बॉयोमेट्रिक पहचान, घर और दफ्तर का पता, हमारी दैनिक गतिविधियाँ लोगों की नज़र में हैं। हाल ही में कुछ ऐसी रिपोर्ट्स सामने आईं जिनमें कहा गया था कि गूगल पर **मेरा आधार, मेरी पहचान** सर्च करने पर कथित तौर पर आधार की पीडीएफ फाइल उपलब्ध हो जाती है। इसके बाद आधार कार्ड जारी करने वाली संस्था भारतीय विशिष्ट पहचान प्राधिकरण (UIDAI) ने लोगों को किसी भी सेवा का लाभ लेने के लिये इंटरनेट पर आधार जैसी अपनी व्यक्तिगत जानकारी साझा करते समय सावधानी बरतने के लिये कहा है।

Watch Video At:

https://youtu.be/PW-W51sWzQI

इससे पहले फेसबुक डेटा के दुरुपयोग का मुद्दा भी चर्चा में रहा था, **(इस मुद्दे पर राज्यसभा टीवी डिस्कशन पर 23 मार्च को अलग से डिबेट कवर की गई है)**।

ऐसे में सवाल उठता है कि हमारा जो भी डेटा (पहचान, पता-ठिकाना आदि) साइबर संसार में यहाँ-वहाँ बिखरा पड़ा है, वह कितना सुरक्षित है और उसे कैसे सुरक्षित रखा जा रहा है। वैसे UIDAI के कहे बिना भी लोगों को किसी सेवा प्रदाता या वेंडर से सेवा प्राप्त करने के लिये इंटरनेट पर आधार सहित अन्य व्यक्तिगत जानकारी साझा करते समय कुछ सावधानियाँ बरतनी चाहिये।

क्रिप्टोग्राफी क्या है?

- क्रिप्टोग्राफी मूल रूप से एक ग्रीक शब्द है, जो 'गुप्त' और 'लिखावट' का मिला-जुला अर्थ देता है।
- यह एक प्रकार का कूट-लेखन (Encode) है, जिसमें भेजे गये संदेश या जानकारी को सांकेतिक शब्दों में बदल दिया जाता है।
- इसे भेजने वाला या पाने वाला ही पढ़ सकता या खोल सकता है।
- क्रिप्टोग्राफी का संबंध डेटा की सुरक्षा और उससे संबंधित विषयों, विशेषकर एनक्रिप्शन से होता है।
- वर्तमान में जो क्रिप्टोसिस्टम हम देखते हैं, उसकी शुरुआत 1970 के दशक में हुई थी।
- तब अमेरिकी सरकार ने डेटा एन्क्रिप्शन स्टैंडर्ड तैयार किया था, जिसमें 56 बिट की 'सीक्रेट की' का इस्तेमाल होता था।
- इसकी सीमाओं को देखते हुए जल्द ही एडवांस एन्क्रिप्शन स्टैंडर्ड सामने आया, जिसमें कम-से-कम 126 बिट की 'सीक्रेट की' का इस्तेमाल होता था। आज यह इंटरनेट जगत में सबसे अधिक उपयोग में लाया जाने वाला क्रिप्टोसिस्टम है।

यह एक बहुविषयक विषय है, जो कई क्षेत्रों से जुड़ा होता है। कुछ दशकों पहले तक क्रिप्टोग्राफी मूल रूप से भाषा से जुड़ी होती थी, पर वर्तमान डिजिटल दौर में क्रिप्टोग्राफी में मैथमैटिक्स, नंबर थ्योरी, इंफॉर्मेशन थ्योरी, कंप्यूटेशनल कॉम्प्लेक्सिटी, स्टैटिस्टिक्स और कॉम्बिमेटोरिक्स का भरपूर प्रयोग होता है। क्रिप्टोग्राफी कम्प्यूटर और नेटवर्क सिक्योरिटी के लिये प्रयुक्त की जाती है।

(टीम दृष्टि इनपुट)

क्या है डेटा एन्क्रिप्शन?

कंप्यूटर पर हम सामान्यतया जिस फाइल में काम करते हैं, उसे टेक्स्ट फॉर्मेट फाइल कहते हैं, जिसे कोई भी पढ़ या समझ सकता है। लेकिन जब हम यह चाहते हैं कि फाइल में जो लिखा है उसे कोई अन्य पढ़ न पाए तो उसे एन्क्रिप्ट करना होता है। इसके बाद इसमें लिखा हुआ टेक्स्ट कुछ इस तरह दिखाई देता है जिसे पढ़ना लगभग असंभव होता है। इस प्रक्रिया को डेटा **एन्क्रिप्शन** कहते हैं। इंटरनेट पर डेटा को सुरक्षित रखने के लिये एन्क्रिप्शन किया जाता है, जो इसे हैक होने से बचाता है और उसका गलत प्रयोग होने की आशंका नहीं रहती।

कैसे किया जाता है एन्क्रिप्शन?

- एन्क्रिप्शन एक ऐसी तकनीक है जो इंफार्मेशन को एक अपठनीय कोड भाषा में परिवर्तित कर देता है, जिसे एक्सेस करना कठिन होता है। डेटा या इंफार्मेशन को एन्क्रिप्ट करने के लिये एक 'की' का प्रयोग होता है जो सेंडर और रिसीवर के पास सुरक्षित होती है।
- डेटा को एक एल्गोरिथम द्वारा एन्क्रिप्ट किया जाता है, जिसे Cipher कहते हैं। इससे एन्क्रिप्टेड जानकारी मिलती है और एन्क्रिप्ट की गई जानकारी या सूचना को Ciphertext कहते हैं। एन्क्रिप्ट होने के बाद डेटा पूरी तरह से सुरक्षित हो जाता है।

- एन्क्रिप्ट की गई जानकारी को फिर से पढ़ने योग्य बनाने की प्रक्रिया को **डिक्रिप्शन** कहा जाता है। इस प्रक्रिया में भी उसी 'की' का प्रयोग होता है, जिससे डेटा एन्क्रिप्ट किया गया था।

एंड-टू-एंड एन्क्रिप्शन

- डेटा को 100 प्रतिशत सुरक्षित करने की प्रक्रिया को **एंड-टू-एंड एन्क्रिप्शन** कहा जाता है। अर्थात् ऐसे डेटा को केवल भेजने वाले (Sender) और जिसके लिये ये मैसेज होगा (Receiver) वही देख सकते हैं।
- एंड-टू-एंड एन्क्रिप्शन लागू होने के बाद कोई तीसरा इसे देख, पढ़ या समझ नहीं सकता और इसे कोई ट्रेस भी नहीं कर सकता।
- ऐसे भेजे हुए सभी मैसेज, फोटो, वीडियो, फाइल और वॉयस मैसेज, सूचनाएँ तथा अन्य सभी जानकारियाँ 100 प्रतिशत सुरक्षित हो जाते हैं।
- एंड-टू-एंड एन्क्रिप्शन के बाद साइबर अपराधी और हैकर्स भी इसे नहीं पढ़ सकते क्योंकि यह 256 बिट स्ट्रॉन्ग होता है, जिसे हैकर्स ब्रूट फोर्स मेथड से भी क्रैक नहीं कर सकते।

पब्लिक और प्राइवेट 'की' क्या है?

एन्क्रिप्शन में डेटा एन्क्रिप्ट करने के लिये एल्गोरिथम का उपयोग किया जाता है और इसे केवल एक विशेष 'की' के उपयोग से डिक्रिप्ट किया जा सकता है। व्यापक रूप से प्रयुक्त एन्क्रिप्शन विधियों में से प्राइवेट 'की' एन्क्रिप्शन और पब्लिक 'की' एन्क्रिप्शन हैं।

- प्राइवेट 'की' एन्क्रिप्शन में सेंडर और रिसीवर डेटा को एन्क्रिप्ट करने के लिये समान 'की' साझा करते हैं। अर्थात् दोनों पक्ष एक ही 'की' को डेटा के एन्क्रिप्शन और डिक्रिप्शन के लिये उपयोग करते हैं।
- पब्लिक 'की' एन्क्रिप्शन में दो भिन्न, लेकिन गणितीय संबंधित 'की' का उपयोग किया जाता है।पब्लिक 'की' एन्क्रिप्शन में आपको लॉक करने के लिये एक 'की' और अनलॉक करने के लिये एक अन्य 'की' चाहिये होती है। एक 'की' को दूसरे के स्थान पर इस्तेमाल नहीं किया जा सकता।

(टीम दृष्टि इनपुट)

आधार का क्रिप्टोसिस्टम

- आधार का बायोमेट्रिक सॉफ्टवेयर बाहर से मंगाया गया है, लेकिन डेटा नियंत्रण UIDAI के पास है।
- एक आधार कार्ड पर आने वाली लागत एक डॉलर से भी कम है और आधार के 6000 सर्वर इंटरनेट से नहीं जुड़े हैं।
- आधार का सारा बॉयोमेट्रिक डेटा 2048 बिट एनक्रिप्शन से सुरक्षित है और इसे चुरा पाना किसी के लिये भी असंभव है।
- इसके लिये इस समय दुनिया में मौजूद सबसे उन्नत एन्क्रिप्शन 'पब्लिक की' PKI 2048 और AES 256 का इस्तेमाल किया जा रहा है। ये 248 और 256 बिट सिस्टम पर काम करते हैं।
- इसकी एन्क्रिप्शन-की (तीन अंकों का सुरक्षित लॉकिंग सिस्टम) को तीन सुपरकंप्यूटर भी अनंत काल तक नहीं तोड़ सकते।
- UIDAI आधार से जुड़ी कोई भी जानकारी किसी से साझा नहीं करता, सिर्फ केवाईसी के लिये ही निजी जानकारी दी जाती है।
- यदि किसी आधार कार्ड से कोई लेन-देन होता है तो UIDAI लोकेशन या लेन-देन के उद्देश्य को इकट्ठा नहीं करता।

बिग डेटा
बिग डेटा एक ऐसी प्रक्रिया है जिसके तहत डेटा के विशाल समूह एकत्रित किये जाते हैं और उनका विश्लेषण किया जाता है। वर्तमान युग डेटा का युग है और बिग डेटा और उसके विश्लेषण के माध्यम से दिये हुए पैटर्न को जानने, बाज़ार एवं उपभोक्ताओं के रुख का विश्लेषण करने का प्रयास किया जाता है। यही कारण है कि आर्थिक क्रियाकलापों में एवं अन्य विभिन्न क्षेत्रों में बिग डेटा का महत्त्वपूर्ण स्थान है। बिग डेटा अर्थव्यवस्था के विभिन्न क्षेत्रों को प्रभावित करने की क्षमता रखता है। इस संबंध में सबसे महत्त्वपूर्ण ज़रूरत ऐसी व्यवस्था बनाने की है, ताकि डेटा की सुरक्षा की जा सके।

प्राथमिक क्षेत्र: बिग डेटा के विश्लेषण के माध्यम से स्थानीय पर्यावरण, मौसम का पैटर्न तथा मृदा की गुणवत्ता जानने में मदद प्राप्त की जा सकती है। साथ ही उर्वरकों की ज़रूरत एवं बीजों की गुणवत्ता जानने में भी मदद प्राप्त की जा सकती है।

द्वितीयक क्षेत्र: बिग डेटा के माध्यम से बाज़ार और उपभोक्ताओं के रुख को समझने तथा अंतर्राष्ट्रीय स्तर पर उत्पादों की मांग को समझने में मदद मिल सकती है। इसका प्रयोग विदेशी निवेशक अन्य देशों के बाज़ारों की स्थिति को जानने के लिये करते हैं।

सेवा क्षेत्र: परिवहन के क्षेत्र में बिग डेटा के ज़रिये क्रांतिकारी परिवर्तन लाया जा रहा है। ओला, उबर कैब सेवाओं में इसे देखा जा सकता है। इससे बैंकिंग क्षेत्र में भी महत्त्वपूर्ण परिवर्तन लाए जा सकते हैं। वृहद् डेटा विश्लेषण करके NPA आदि का समाधान ढूँढा जा सकता है। ई-कॉमर्स के क्षेत्र में भी बिग डेटा का महत्त्वपूर्ण योगदान है।

(टीम दृष्टि इनपुट)

CIDR: आधार का डेटा सरकारी संस्था सेंट्रल इंफार्मेशन डेटा रेपोज़िटरी (CIDR) में 10 मीटर ऊँची और 4 मीटर चौड़ी दीवार के पीछे सुरक्षित है। यह दावा सरकार की ओर से सर्वोच्च न्यायालय में किया गया। इसी के पास आधार की समस्त जानकारियाँ सँभालने की और अपडेट करने की ज़िम्मेदारी है। इसी से प्रमाणीकरण और eKYC के लिये जानकारी तथा सूचनाएँ मांगी जाती है। आपका रॉ बायोमेट्रिक डेटा एन्क्रिप्टेड फॉर्म में CIDR में ही सुरक्षित रहता है। इसका पूरा तंत्र भारत के भीतर ही काम करता है और सूचनाएँ भी भारत में रूट होती हैं।

केंद्र सरकार आगामी जुलाई से आधार कार्ड के लिये **फेस आईडी** लागू करने की योजना पर काम कर रही है।

क्वांटम क्रिप्टोग्राफी

यह तकनीक गणित के बजाय भौतिकी पर आधारित होती है। पारंपरिक एन्क्रिप्शन 'की' की नकल हैकरों द्वारा कर लेने के बाद इस समस्या के समाधान के लिये 'क्वांटम की डिस्ट्रीब्यूशन' (Quantum Key Distribution) के नाम से क्वांटम क्रिप्टोग्राफी पर आधारित एक महत्त्वपूर्ण एप्लीकेशन बनाया गया।इसमें अभेद्य क्रिप्टोसिस्टम के विकास के लिये कुछ विशेष कणों या प्रकाश तरंगों (फोटोन) तथा उनकी मूलभूत क्वांटम विशेषताओं का प्रयोग किया जाता है।

- यह तकनीक काफी व्यावहारिक है क्योंकि किसी प्रणाली की क्वांटम अवस्था का मापन उस पूरी प्रणाली में अवरोध उत्पन्न किये बिना असंभव है।
- 'क्वांटम 'की' डिस्ट्रीब्यूशन' एक विशेष एप्लीकेशन है क्योंकि इसकी 'की' में प्रकाश कणों (फोटोन) का प्रयोग किया जाता है।
- क्वांटम क्रियाविधि के सिद्धांतों के अनुसार, ऐसी 'की' को पढ़ने या इसकी नकल करने का प्रयास करने वाले हैकर द्वारा स्वतः ही इसकी अवस्था में परिवर्तन हो जाएगा।
- इस प्रक्रिया में हैकर के फिंगर प्रिंट भी छूट जाएंगे तथा इस तरह सूचनाओं को पढ़ने या उसमें बाधा पहुँचाने के प्रयासों को सूचना पाने वाले तथा भेजने वाले द्वारा आसानी से पकड़ा जा सकता है।
- इस तकनीक के विकास से बैंकों, वित्तीय व सरकारी संस्थाओं के लिये क्वांटम-सुरक्षित अवसंरचना विकसित की जा सकती है और डेटा की पूरी सुरक्षा सुनिश्चित की जा सकती है।
- वर्तमान में क्वांटम बिट्स का प्रयोग करने वाले लघु क्वांटम कंप्यूटर ही मौजूद हैं, वह भी बेहद कम संख्या में, लेकिन गूगल, आईबीएम तथा इंटेल जैसी कंपनियाँ इस पर कार्य कर रही हैं।

(टीम दृष्टि इनपुट)

मेरे डेटा का मालिक कौन?

इस प्रश्न में यदि आप डेटा को किसी भौतिक वस्तु (जैसे-कार अथवा घर) से प्रतिस्थापित कर देते हैं तो इसका उत्तर बेशक 'मैं' होगा। लेकिन डिजिटल विश्व में स्वामित्व की अवधारणा में कई परिवर्तन हुए हैं। सामग्री पर स्वामित्व के अलावा भी डेटा से संबंधित डेटा संरक्षण के कई ऐसे मंच हैं जो आपकी (व्यक्तिगत डेटा) और आपसे संबंधित डेटा (जिसका सृजन आपको, आपकी सामग्री और आपकी गतिविधियों को देखकर किया गया) की पहचान करते हैं। ये सभी इस बात पर ज़ोर देते हैं कि आपके विषय में प्राप्त सूचनाओं जैसे-आपका नाम, पत्राचार का पता, फोन, ई-मेल, संपर्क प्राथमिकताएँ और डेबिट/क्रेडिट कार्ड सूचनाओं को इन मंचों के माध्यम से उनकी सहयोगी कंपनियों, सामरिक भागीदारों अथवा अन्य सेवा प्रदाताओं के साथ साझा किया जा सकता है। इन डेटा में आपके व्यवसाय, भाषा, पिन कोड, क्षेत्र कोड, अद्वितीय डिवाइस पहचानकर्त्ता, URL, स्थान और समय क्षेत्र जैसी सूचनाओं के साथ कुछ में मित्रों और पारिवारिक सदस्यों के विषय में जानकारियाँ भी शामिल हो सकती हैं। इसके अतिरिक्त, आपका भौतिक स्थान और ऑनलाइन गतिविधियों को भी कई तकनीकी माध्यमों का उपयोग करके ट्रैक किया जा सकता है जबकि प्रायः आप इनसे अनभिज्ञ रहते हैं। इन मंचों पर आपके डेटा पर पूर्ण स्वामित्व स्थापित कर लिया जाता है, जबकि वास्तविक स्वामी का अपने डेटा पर कोई अधिकार नहीं रह जाता।

(टीम दृष्टि इनपुट)

निष्कर्ष: कंप्यूटर, मोबाइल और इंटरनेट...इन तीन शब्दों में देश-दुनिया का ज्ञान, सामान, सेवाएँ, जानकारियाँ, मनोरंजन, सूचनाएँ समा गई हैं और आज इनके बिना जीवन की कल्पना ही नहीं की जा सकती। इन तीनों का डेटा से कुछ वैसा ही रिश्ता है, जो साँसों का हमारे शरीर के साथ है। आम आदमी की चिंता यह है कि उसका जो भी डेटा अंतहीन साइबर संसार में बिखरा पड़ा है, वह सुरक्षित रहे और इस मामले में उसकी सबसे बड़ी परेशानी यह है कि विज्ञान और तकनीक की भाषा उसकी समझ से बाहर है।

सरकारी योजनाओं का फायदा लेने के लिये केंद्र ने आधार को ज़रूरी किया है। इसके खिलाफ तीन अलग-अलग याचिकाओं पर सर्वोच्च न्यायालय में सुनवाई चल रही है, जिनमें आधार की कानूनी वैधता, डेटा सुरक्षा और इसे लागू करने के तरीकों को चुनौती दी गई है। वैसे भी इंटरनेट और मशीन के साथ कभी भी कोई समस्या आ सकती है। ऐसे में जरूरी है कि बायोमेट्रिक के अलावा प्रमाणीकरण की कोई अन्य व्यवस्था भी की जाए। फिलहाल ऐसी कोई व्यवस्था नहीं है, जिसके तहत अगर किसी के बायोमेट्रिक्स का मिलान न हो, तो ऐसे लोगों को ज़रूरी सेवाओं के लाभ से वंचित न किया जाए। वैसे आधार अधिनियम की धारा-7 में ऐसी ही दिक्कतों से निपटने की बात की गई है।

भारत में आज 46 करोड़ से ज़्यादा इंटरनेट यूजर्स हैं और वे किसी-न-किसी रूप में डिजिटल सेवाओं से जुड़े हैं। इंटरनेट पर उनका डेटा किसी न किसी रूप में मौजूद है और यह सुनिश्चित करने वाला कोई नहीं है कि वह डेटा किस हद तक सुरक्षित है। अतः यह सुनिश्चित करने के लिये कि डेटा के स्वामी का अपने डेटा पर पूर्ण नियंत्रण है तथा वह प्रत्येक मंच जो डेटा का अनुसरण अथवा इसका उपयोग करता है, उसके लिये व्यापक स्वरूप में स्वीकार्य नोटिस, पसंद और सहमति, संग्रह सीमा, उद्देश्य सीमा, पहुँच और संशोधन मानदंड, सूचना मानकों का खुलासा, सुरक्षा, स्पष्टता और जवाबदेहिता पर भी पूर्ण नियंत्रण रखने के लिये एक तकनीकी ढाँचे की अतिशीघ्र आवश्यकता है।