

आधुनिक पुस्तकालयों में साइबर सुरक्षा और डेटा गोपनीयता: डिजिटल लॉग एवं पाठक डेटा प्रबंधन का एक विश्लेषणात्मक अध्ययन

रंजीत कुमार ग्रंथपाल

शास.एस.एन.जी.महाविद्यालय मुंगेली, छत्तीसगढ़, भारत

सारांश

सूचना और संचार प्रौद्योगिकी (ICT) के प्रसार ने पारंपरिक पुस्तकालयों को एकीकृत डिजिटल सूचना केंद्रों में बदल दिया है। आज पुस्तकालय केवल पुस्तकों के भौतिक आदान-प्रदान तक सीमित नहीं हैं, बल्कि वे बड़े पैमाने पर डिजिटल लॉग (Digital Logs), वेब सर्च हिस्ट्री, ई-संसाधन एक्सेस रिकॉर्ड और पाठकों के व्यक्तिगत डेटा (Patron Data) का प्रबंधन करते हैं। यह डेटा जहाँ पुस्तकालय की सेवाओं को बेहतर बनाने में सहायक है, वहीं यह साइबर अपराधियों के लिए भी एक संवेदनशील लक्ष्य बन चुका है। प्रस्तुत शोध पत्र आधुनिक पुस्तकालयों में डिजिटल लॉग और पाठक डेटा के प्रबंधन से जुड़ी साइबर सुरक्षा चुनौतियों का विश्लेषण करता है। इसके साथ ही, यह शोध पत्र भारत के 'डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (DPDP Act, 2023)' के संदर्भ में पुस्तकालयों की कानूनी और नैतिक जिम्मेदारियों की समीक्षा करते हुए सुरक्षा के तकनीकी एवं नीतिगत समाधान प्रस्तावित करता है।

मूल शब्द: साइबर सुरक्षा, डेटा गोपनीयता, डिजिटल लॉग, पाठक डेटा (Patron Data), पुस्तकालय प्रबंधन प्रणाली (LMS), DPDP अधिनियम 2023।

प्रस्तावना

ऐतिहासिक रूप से, पुस्तकालयों ने हमेशा पाठकों की बौद्धिक स्वतंत्रता (Intellectual Freedom) और गोपनीयता की रक्षा की है। पारंपरिक युग में, पाठक ने कौन सी पुस्तक पढ़ी या खोजी, इसका रिकॉर्ड रजिस्टर तक ही सीमित रहता था। लेकिन आज के डिजिटल युग में, जब कोई पाठक पुस्तकालय की वेबसाइट, वाई-फाई (Wi-Fi), ओपेक (OPAC), या क्लाउड-आधारित लाइब्रेरी मैनेजमेंट सिस्टम (LMS) का उपयोग करता है, तो उसके हर कदम का एक डिजिटल पदचिह्न (Digital Footprint) या लॉग (Log) बनता है।

यह डिजिटल लॉग न केवल यह बताता है कि पाठक क्या पढ़ रहा है, बल्कि उसकी आईपी एड्रेस (IP Address), डिवाइस की जानकारी, और लॉग-इन समय जैसी संवेदनशील जानकारी को भी सहेजता है। यदि यह डेटा सुरक्षित नहीं है, तो यह पाठकों की निजता के अधिकार का सीधा उल्लंघन है। इसलिए, पुस्तकालयों के लिए 'साइबर सुरक्षा' और 'डेटा गोपनीयता' अब वैकल्पिक नहीं, बल्कि अनिवार्य परिचालन आवश्यकता बन गई है।

पुस्तकालयों द्वारा प्रबंधित डिजिटल डेटा के प्रकार (Types of Digital Data Managed by Libraries)

पुस्तकालय मुख्य रूप से दो प्रकार के संवेदनशील डेटा का संकलन और प्रसंस्करण (Processing) करते हैं

1. **पाठक डेटा (Patron Data):** इसमें पाठक का नाम, आधार/पहचान पत्र संख्या, ईमेल आईडी, फोन नंबर, घर का पता, और वित्तीय लेनदेन (जुर्माना या सदस्यता शुल्क का ऑनलाइन भुगतान) की जानकारी शामिल होती है।

2. **डिजिटल और परिचालन लॉग (Digital & Operational Logs)**

■ **सर्च लॉग (Search Logs):** ओपेक (OPAC) या डिस्कवरी टूल्स पर पाठकों द्वारा खोजे गए कीवर्ड।

■ **एक्सेस लॉग (Access Logs):** ई-बुक्स, ऑनलाइन जर्नल्स और डेटाबेस (जैसे- Scopus, IEEE) को एक्सेस करने का समय और आईपी एड्रेस।

■ **नेटवर्क लॉग (Network Logs):** पुस्तकालय के फ्री वाई-फाई या कंप्यूटर लैब का उपयोग करने वाले उपयोगकर्ताओं का ट्रैफिक डेटा।

प्रमुख साइबर सुरक्षा चुनौतियाँ और खतरे (Major Cyber security Challenges and Threats)

1. **रैनसमवेयर और मैलवेयर हमले (Ransom ware and Malware Attacks)**

हाल के वर्षों में शैक्षणिक और सार्वजनिक पुस्तकालयों के सर्वरों पर रैनसमवेयर हमले तेजी से बढ़े हैं। हैकर्स पुस्तकालय के सर्वर और डिजिटल लॉग्स को एन्क्रिप्ट (लॉक) कर देते हैं और डेटा वापस करने के बदले मोटी फिरोती की मांग करते हैं। इससे पुस्तकालय की सेवाएं हफ्तों तक ठप हो जाती हैं।

2. **थर्ड-पार्टी वेंडर और प्रकाशक (Third Party Vendors Risk)**

अधिकांश पुस्तकालय ई-संसाधनों के लिए बाहरी प्रकाशकों (जैसे- Elsevier, Springer) और सॉफ्टवेयर प्रदाताओं पर निर्भर हैं। यदि इन थर्ड-पार्टी वेंडर्स के सिस्टम में सुरक्षा चूक होती है, तो पुस्तकालय के पाठकों का डेटा भी सीधे खतरे में पड़ जाता है। अक्सर ये वेंडर लक्षित विज्ञापनों (Targeted Ads) के लिए पाठकों के पढ़ने की आदतों का डेटा ट्रैक करते हैं।

3. **असुरक्षित वाई-फाई और नेटवर्क (Unsecured Wi-Fi Networks)**

पुस्तकालयों में आने वाले उपयोगकर्ता अक्सर वहां के खुले और मुफ्त वाई-फाई नेटवर्क का उपयोग करते हैं। सुरक्षा प्रोटोकॉल

(जैसे WPA3) न होने पर साइबर अपराधी 'मैन-इन-द-मिडल (MitM)' हमलों के जरिए उपयोगकर्ताओं के उपकरणों में सेंध लगा सकते हैं और उनके डेटा लॉग चुरा सकते हैं।

विनियामक ढांचा: भारत का DPDP अधिनियम, 2023 और पुस्तकालय

भारत सरकार द्वारा पारित डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 (DPDP Act 2023) के बाद अब पुस्तकालयों की कानूनी जिम्मेदारी अत्यधिक बढ़ गई है। इस कानून के तहत पुस्तकालयों को 'डेटा फिड्यूसियरी (Data Fiduciary)' माना जाएगा। पुस्तकालयों को अब निम्नलिखित नियमों का पालन करना अनिवार्य है

- **स्पष्ट सहमति (Notice & Consent):** किसी भी पाठक का डेटा या डिजिटल लॉग सहेजने से पहले उसे सरल भाषा (हिंदी/अंग्रेजी या क्षेत्रीय भाषा) में बताना होगा कि डेटा क्यों लिया जा रहा है।
- **डेटा न्यूनीकरण (Data Minimization):** पुस्तकालय केवल उतना ही डेटा एकत्र कर सकते हैं जो उनकी सेवाओं के लिए अत्यंत आवश्यक हो। अनावश्यक डिजिटल लॉग्स को लंबे समय तक स्टोर नहीं किया जा सकता।
- **मिटाने का अधिकार (Right to Erasure):** यदि कोई पाठक पुस्तकालय की सदस्यता छोड़ता है, तो पुस्तकालय को उसका सारा व्यक्तिगत डेटा और डिजिटल लॉग स्थायी रूप से हटाना होगा।

सुरक्षा और गोपनीयता सुनिश्चित करने के उपाय (Solutions and Mitigation Strategies)

1. तकनीकी समाधान (Technical Solutions)

- **डेटा एन्क्रिप्शन (Encryption):** सर्वर और डेटाबेस में संग्रहीत सभी पाठक डेटा को 'एईएस-256 (AES-256)' जैसे मजबूत एन्क्रिप्शन मानकों के साथ सुरक्षित किया जाना चाहिए।
- **लॉग अनामितीकरण (Log Anonymization):** सिस्टम एडमिनिस्ट्रेटर को सर्वर और एक्सेस लॉग्स से पाठकों की व्यक्तिगत पहचान (जैसे नाम या रोल नंबर) को अलग कर देना चाहिए, ताकि डेटा लीक होने पर भी यह पता न चले कि वह किस विशिष्ट व्यक्ति का है।
- **बहु-स्तरीय प्रमाणीकरण (Multi-Factor Authentication & MFA):** पुस्तकालय के कर्मचारियों और एडमिनिस्ट्रेटर के खातों के लिए MFA अनिवार्य होना चाहिए ताकि अनधिकृत पहुंच को रोका जा सके।

2. प्रशासनिक और नीतिगत समाधान (Administrative Policies)

- **डेटा प्रतिधारण नीति (Data Retention Policy):** पुस्तकालयों को एक सख्त नीति बनानी चाहिए जिसके तहत वाई-फाई लॉग और सर्वर लॉग को एक निश्चित समय (जैसे 30 या 90 दिन) के बाद स्वचालित रूप से नष्ट (Auto-delete) कर दिया जाए।
- **नियमित सुरक्षा ऑडिट (VAPT):** पुस्तकालय के डिजिटल बुनियादी ढांचे का वर्ष में कम से कम एक बार

'वलनरेबिलिटी असेसमेंट एंड पेनिट्रेशन टेस्टिंग (VAPT)' कराया जाना चाहिए।

- **डिजिटल साक्षरता अभियान:** पाठकों और पुस्तकालय कर्मियों को 'साइबर हाइजीन' (जैसे मजबूत पासवर्ड बनाना, फिशिंग ईमेल से बचना) के बारे में शिक्षित किया जाना चाहिए।

निष्कर्ष

डिजिटल युग में पुस्तकालयों का दायित्व केवल ज्ञान का प्रसार करना नहीं, बल्कि उस ज्ञान को प्राप्त करने वाले पाठकों की डिजिटल सुरक्षा करना भी है। व्यापक डिजिटल लॉग और संवेदनशील पाठक डेटा का प्रबंधन करने के लिए पुस्तकालयों को अपनी पारंपरिक मानसिकता से बाहर निकलकर उन्नत साइबर सुरक्षा तकनीकों को अपनाना होगा। भारत के DPDP अधिनियम 2023 जैसे कड़े कानूनों के लागू होने के बाद, डेटा गोपनीयता का उल्लंघन पुस्तकालयों के लिए गंभीर कानूनी और वित्तीय संकट पैदा कर सकता है। अतः एक मजबूत तकनीकी सुरक्षा चक्र और पारदर्शी गोपनीयता नीति को लागू करके ही पुस्तकालय आधुनिक समाज में एक सुरक्षित, विश्वसनीय और लोकतांत्रिक संस्थान के रूप में अपनी पहचान बनाए रख सकते हैं।

संदर्भ

1. भारत सरकार. (2023). डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (DPDP Act), 2023. इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय।
2. इंटरनेशनल फेडरेशन ऑफ लाइब्रेरी एसोसिएशंस एंड इंस्टीट्यूशंस (IFLA). (2025). स्टेटमेंट ऑन लाइब्रेरी प्राइवेसी एंड डेटा प्रोटेक्शन इन द डिजिटल एरा.
3. कुमार, आर., एवं सिंह, पी. (2026). भारतीय शैक्षणिक पुस्तकालयों में क्लाउड कंप्यूटिंग और साइबर सुरक्षा चुनौतियाँ। जर्नल ऑफ लाइब्रेरी एंड इंफॉर्मेशन टेक्नोलॉजी, 46(1), 34–45।
4. अमेरिकन लाइब्रेरी एसोसिएशन (ALA). (2024). प्राइवेसी फील्ड गाइड फॉर लाइब्रेरी एडमिनिस्ट्रेटर्स.