International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
An International Quarterly bi-lingual Multidisciplinary Double Blind Open Access Peer Reviewed Refereed Journal
ISSN:2581-9925, Impact Factor (Cosmos: 7.555 & I2OR: 5.105), Volume 08, No. 03(II), July-September, 2026, pp. 110-119

ऑनलाइन बैंकिंग और लेन–देन को प्रभावित करने वाले साइबर हमलों के कारण और निवारण

Hargovind Kharera*

Assistant Professor Department of EAFM, Government Commerce College, Alwar, Rajasthan.

*Corresponding Author: hgkharera@gmail.com

Citation: Kharera, H. (2026). ऑनलाइन बैंकिंग और लेन–देन को प्रभावित करने वाले साइबर हमलों के कारण और निवारण. International Journal of Education, Modern Management, Applied Science & Social Science, 08(03(II)), 110–119.

सार

वित्तीय सेवाओं के तेजी से बढ़ते डिजिटलीकरण ने बैंकिंग क्षेत्र को महत्वपूर्ण रूप से परिवर्तित किया है, जिससे ऑनलाइन बैंकिंग और डिजिटल लेन–देन को व्यापक रूप से अपनाया जा रहा है। ग्राहक सुविधा, इंटरनेट बैंकिंग की गति और अपनी डिजिटलीकरण की आव कता की पूर्ति, मोबाइल एप्लिकेशन और डिजिटल भुगतान प्लेटफॉर्म पर तीव्र गति से भरोसा करने लगे हैं। हालांकि, इस बदलाव ने वित्तीय प्रणालियों को साइबर सुरक्षा के खतरों की एक विस्तृत श्रृंखला के तरीकों को भी उजागर किया है। यह शोध अध्ययन ऑनलाइन बैंकिंग और डिजिटल लेन–देन को प्रभावित करने वाले विभिन्न साइबर सुरक्षा उपकरणों की भी जांच करता है, जिसमें फिशिंग, मैलवेयर हमले, ग्राहक पहचान की चोरी और समंक उल्लंघन सम्मिलित हैं। यह अध्ययन ग्राहकों की जागरूकता के स्तर, बैंकों द्वारा अपनाए गए सुरक्षा के प्रभावसाली उपायों और सुरक्षित वित्तीय लेन–देन सुनिश्चित करने में विभिन्न विनियामक अधिकारियों की भूमिका का भी मूल्यांकन करता है। कुछ निष्कर्षों से पता चलता है कि बैंक उन्नत तकनीकी समाधान लागू कर रहे हैं, लेकिन उपयोगकर्ताओं की लापरवाही और जागरूकता की कमी साइबर जोखिमों में प्रमुख योगदानकर्ता बनी हुई है। यह अध्ययन डिजिटल बैंकिंग पारिस्थितिकी तंत्र में साइबर सुरक्षा को मजबूत करने के लिए प्रौद्योगिकी, उपयोगकर्ता, शिक्षा और विभिन्न विनियामक अधिकारियों की सहायता से जुड़े एक संयुक्त दृष्टिकोण की आवश्यकता पर जोर रहा है।

शब्दकोशः *साइबर सुरक्षा, ऑनलाइन बैंकिंग, फिशिंग, मैलवेयर, पहचान की चोरी, डिजिटल लेनदेन, डेटा उल्लंघन।*

प्रस्तावना

सूचना प्रौद्योगिकी और डिजिटल संचार में प्रगति के कारण बैंकिंग क्षेत्र ने एक महत्वपूर्ण परिवर्तन का अनुभव किया रहा है। ऑनलाइन बैंकिंग और डिजिटल भुगतान प्रणालियां वित्तीय लेनदेन के लिए आवश्यक उपकरण बन गई हैं जिससे ग्राहक कभी भी और कहीं भी बैंकिंग गतिविधियां कर सकते हैं। मोबाइल बैंकिंग, यूनिफाइड पेमेंट्स इंटरफेस और डिजिटल वॉलेट जैसी सेवाओं की शुरुआत ने वित्तीय संचालन की दक्षता बढ़ा दी है। विकास की इन चुनौतियाँ से साइबर सुरक्षा के क्षेत्र में अनेक नवीन समस्याएं भी उत्पन्न हो रही हैं। तीव्र गति से बढ़ते हुए साइबर खतरों वित्तीय संस्थानों और व्यक्तिगत उपयोगकर्ताओं को निशाना बनाया जा रहा है। साइबर ठगी करने वाले हैकर्स अनधिकृत रूप से वित्तीय समंक की चौरी करके ऑनलाइन प्रणाली सिस्टम की

* *Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.*

कमजोरियों, खराब सुरक्षा प्रणालियों और उपयोगकर्ताओं में लेन–देन के प्रति जागरूकता की कमी का फायदा उठाते हैं। उक्त शोध अध्ययन ऑनलाइन बैंकिंग को प्रभावित करने वाले साइबर सुरक्षा के कारन एवं परिणाम का विश्लेषण करने और सुरक्षा बढ़ाने व जोखिमों को कम करने के उपायों की पहचान करने पर केंद्रित है।

वैचारिक पृष्ठभूमि (Conceptual Background)

ऑनलाइन बैंकिंग और डिजिटल लेनदेन में साइबर सुरक्षा से संबंधित प्रमुख अवधारणाओं की एक सैद्धांतिक समझ प्रदान करती है। यह डिजिटल बैंकिंग पारिस्थितिकी तंत्र की संरचना, विभिन्न हितधारकों की भूमिका और वित्तीय प्रणालियों में सुरक्षा तंत्र के महत्व को समझाती है।

- **ऑनलाइन बैंकिंग प्रणाली (Online Banking System):** ऑनलाइन बैंकिंग प्रणाली में इंटरनेट आधारित प्लेटफॉर्मों के उपयोग ग्राहकों को किसी भौतिक बैंकिंग की शाखा में जाए बिना वित्तीय लेन–देन में फंड ट्रांसफर, बिल भुगतान, बैलेंस पूछताछ, खाता प्रबंधन और निवेश गतिविधियां सम्मिलित होती हैं। ऑनलाइन बैंकिंग के विकास ने वित्तीय सेवाओं की दक्षता और पहुंच में बहुत अधिक सुधार हुआ है। ग्राहक कंप्यूटर या मोबाइल उपकरणों का उपयोग करके 24/7 लेन–देन कर सकते हैं। बैंकों ने इन सेवाओं को डिजिटल प्लेटफॉर्म पर स्थानांतरित करके परिचालन लागत को भी कम किया है। डिजिटल बुनियादी ढांचे पर निर्भरता ऑनलाइन बैंकिंग को साइबर खतरों के प्रति अत्यधिक संवेदनशील बनाती है।
- **डिजिटल लेनदेन पारिस्थितिकी तंत्र (Digital Transactions Ecosystem):** डिजिटल लेन–देन पारिस्थितिकी तंत्र में परस्पर अनेक इकाइयाँ सम्मिलित होती हैं जो इलेक्ट्रॉनिक वित्तीय लेन–देन को सुविधा जनक बनाती हैं। इनमें बैंक, ग्राहक, फिनटेक कंपनियां, भुगतान गेटवे, दूरसंचार सेवा प्रदाता और नियामक प्राधिकरण सम्मिलित होती हैं। ग्राहक द्वारा लेन–देन की इस पारिस्थितिकी तंत्र की प्रक्रिया में अनेक जोखिमें हो सकती हैं। किसी भी घटक में एक कमजोरी पूरे सिस्टम को प्रभावित कर सकती है। इसलिए इस पारिस्थितिकी तंत्र की समस्त स्तरों पर सुरक्षा बनाए रखना अति आवश्यक हैं।
- **बैंकिंग में साइबर सुरक्षा (Cyber Security in Banking):** बैंक के ग्राहक समंक और लेन–देन की सुरक्षा के लिए विभिन्न सुरक्षा उपाय लागू रहे हैं। इनमें एन्क्रिप्शन, फायरवॉल, घुसपैठ का पता लगाने वाली प्रणालियाँ और मल्टी–फैक्टर प्रमाणिकता सम्मिलित हैं। धोखाधड़ी वाली गतिविधियों का पता लगाने और उन्हें रोकने के लिए आर्टिफिशियल इंटेलिजेंस और मशीन लर्निंग जैसी उन्नत तकनीकों का भी उपयोग किया जाता है।
- **डिजिटल बैंकिंग सुरक्षा में फिनटेक की भूमिका (Role of FinTech in Digital Banking Security):** फिनटेक कंपनियां डिजिटल बैंकिंग सेवा और सुरक्षा को बढ़ाने में महत्वपूर्ण भूमिका निभाती हैं। वे डिजिटल वॉलेट, यूपीआई प्लेटफॉर्म, भुगतान ऐप और रीयल–टाइम लेन–देन प्रणाली जैसे अभिनव समाधान प्रदान करती हैं। फिनटेक कंपनियां लेन–देन सुरक्षा में सुधार के लिए समंक एनालिटिक्स, आर्टिफिशियल इंटेलिजेंस और ब्लॉकचेन जैसी उन्नत तकनीकों का उपयोग करती हैं।
- **डिजिटल बैंकिंग में साइबर खतरों के प्रकार (Types of Cyber Threats in Digital Banking):** डिजिटल बैंकिंग में साइबर खतरों को उनकी प्रकृति और हमले की विधि के आधार पर विभिन्न श्रेणियों में वर्गीकृत किया जा सकता है। इनमें फिशिंग हमले, मैलवेयर संक्रमण, समंक पहचान की चोरी, समंक उल्लंघन और नेटवर्क आधारित हमले सम्मिलित हैं। बढ़ते हुए साइबर हमलों के कारण बैंकों के लिए अपनी सुरक्षा प्रणालियों को लगातार अपडेट करना और सक्रिय उपाय अपनाना आवश्यक हो गया है।
- **प्रमाणीकरण और सुरक्षा तंत्र (Authentication and Security Mechanisms):** प्रमाणीकरण ऑनलाइन बैंकिंग में साइबर सुरक्षा का एक प्रमुख घटक है। यह सुनिश्चित करता है कि केवल अधिकृत उपयोगकर्ता ही बैंकिंग सेवाओं तक पहुँच सकें। सामान्य प्रमाणीकरण विधियों में पासवर्ड, ओटीपी

(वन–टाइम पासवर्ड), बायोमेट्रिक सत्यापन और मल्टी–फैक्टर ऑथेंटिकेशन शामिल हैं। सुरक्षा तंत्रों में एन्क्रिप्शन तकनीक, फायरवॉल और मॉनिटरिंग सिस्टम भी शामिल हैं।

- **साइबर सुरक्षा में उपयोगकर्ताओं की भूमिका (Role of Users in Cyber Security):** ऑनलाइन बैंकिंग में साइबर सुरक्षा बनाए रखने में इसके उपयोगकर्ता महत्वपूर्ण भूमिका निभाते हैं। उपयोगकर्ता संबंधित लालच में आकर या अग्यांतावस लेन–देन करते समय साइबर जोखिमों को बढ़ावा देने के लिए अनावश्यक कार्य जैसे– आसान अथवा सुविधाजनक पासवर्ड का उपयोग करना, गोपनीय जानकारी साझा करना, संदिग्ध लिंक पर क्लिक करना और असुरक्षित नेटवर्क का उपयोग करना एवं अन्य कार्य कर देते हैं। इसलिए उपयोगकर्ताओं को साइबर सुरक्षा प्रणालियों के बारे में शिक्षित करना आवश्यक है।
- **नियामक ढांचा और साइबर कानून (Regulatory Framework and Cyber Laws):** नियामक प्राधिकरण बैंकिंग क्षेत्र में साइबर सुरक्षा सुनिश्चित करने में महत्वपूर्ण भूमिका निभाते हैं। भारत में भारतीय रिजर्व बैंक जैसी संस्थाएं डिजिटल बैंकिंग सुरक्षा से संबंधित दिशानिर्देश और नीतियां जारी करती हैं। ये नियम समंक सुरक्षा, धोखाधड़ी की रोकथाम, ग्राहक जागरूकता और जोखिम प्रबंधन पर ध्यान केंद्रित करते रहते हैं लेकिन फिर भी हेकर्स लेन–देनों को हैक करने में सफल हो रहे हैं और आए दिन ग्राहक इनके शिकार हो रहे हैं।
- **डिजिटल अर्थव्यवस्था में साइबर सुरक्षा का महत्व (Importance of Cyber Security in Digital Economy):** डिजिटल अर्थव्यवस्था की सफलता में साइबर सुरक्षा एक महत्वपूर्ण कारक है। एक सुरक्षित डिजिटल वातावरण उपयोगकर्ताओं को ऑनलाइन बैंकिंग सेवाओं को अपनाने के लिए प्रोत्साहित करते हुए आर्थिक विकास में वृद्धि करता है। डिजिटल वित्तीय प्रणालियों के सतत विकास के लिए सरकार एवं सम्बंधित संस्था द्वारा साइबर सुरक्षा में निवेश करना अति आवश्यक हो गया है।

साहित्य समीक्षा (Review of Literature)

बैंकिंग लेन–देन में साइबर सुरक्षा पर समय–समय पर किये जाने वाले अध्ययन डिजिटल प्रणालियों की बढ़ती संवेदनशीलता को प्रकाशित करते रहते हैं। इस शोध अध्यन से पूर्व अनेक शोधार्थियों ने समय– समय पर समय की मांग के अनुकूल फिशिंग और मैलवेयर के परिणामस्वरूप बैंकिंग लेन–देन करने वाले उपयोगकर्ताओं पर पड़ने वाले भौतिक एवं अभौतिक प्रभाव की विश्त्रित व्याख्या की है। पूर्व के अनेक शोध प्रतिवेदनों से यह भी संकेत मिलता है कि साइबर धोखाधड़ी को रोकने में ग्राहक जागरूकता महत्वपूर्ण भूमिका निभाती है। कुच्छ उपयोगकर्ताओं में ज्ञान की कमी और लापरवाही के कारण वे स्वयं वित्तीय जोखिमों के शिकार हो जाते हैं लेकिन वर्तमान में आर्टिफिशियल इंटेलिजेंस, एन्क्रिप्शन और बायोमेट्रिक ऑथेंटिकेशन जैसी आधुनिक तकनीकी प्रगति में होने वाले नवाचारों ने सुरक्षा प्रणालियों में अधिक से अधिक सुधार करने का प्रयास किया है। फिर भी समंक गोपनीयता की चिंताएं और विकसित होते साइबर खतरे जैसी चुनौतियाँ बनी ही रहती हैं अर्थात यह देखा गया है कि साइबर सुरक्षा की घटनाओं को रोकने में इसके उपयोगकर्ताओं के व्यवहार और जागरूकता की कमी सब से बड़ी इम्मेदारी रही है।

साइबर सुरक्षा में शोध अंतर (Research Gap)

साइबर सुरक्षा के क्षेत्र में अभी भी कई ऐसे विषय हैं जिन पर पर्याप्त शोध नहीं हुआ है जो प्रमुख शोध अंतर इस प्रकार हैं:

- **आर्टिफिशियल इंटेलिजेंस आधारित साइबर हमलों से सुरक्षाः** कृत्रिम बुद्धिमत्ता से होने वाले फिशिंग, डीपफेक और मालवेयर हमलों से बचाने के लिए प्रभावी तरीकों पर भविष्य में शोध अध्ययन की और भी आवश्यकता है।

- **उपकरणों की सुरक्षा IOT (Internet of Things):** उपयोग में लिए जाने वाले आधुनिक उपकरणों के लिए कम लागत वाली और सुद्रड सुरक्षा प्रणाली विकसित करने पर भी शोध की आवश्यकता है।
- **क्लाउड सुरक्षा (Cloud Security):** मल्टी–क्लाउड और हाइब्रिड क्लाउड वातावरण में समंक सुरक्षा और गोपनीयता बनाए रेखाने पर शोध करने की अधिक आवश्यकता है।
- **रैनसमवेयर (Ransom ware) की शीघ्र पहचानः** वास्तविक समय में रैनसमवेयर का पता लगाने और उसे रोकने की तकनीकों पर शोध करने की अधिक आवश्यकता है।
- **क्वांटम कंप्यूटिंग और एन्क्रिप्शनः** भविष्य में क्वांटम कंप्यूटर्स से वर्तमान एन्क्रिप्शन तकनीकों को खतरा होने की संभावना अधिक रहती है। इस कारण नई सुरक्षित क्रिप्टोग्राफी पर और शोध करने की अधिक आवश्यकता है।
- **मानवीय व्यवहार (Human Factor):** उपयोगकर्ताओं की जागरूकता, साइबर सुरक्षा प्रशिक्षण और लेन–देन मे होने वाली मानवीय गलतियों को कम करने के प्रभावी तरीकों पर शोध करने की अधिक आवश्यकता है।
- **5जी नेटवर्क सुरक्षाः** 5जी नेटवर्क में समंक सुरक्षा, नेटवर्क स्लाइसिंग और एज कंप्यूटिंग से संबन्धित सुरक्षा जोखिमों पर शोध करने की अधिक आवश्यकता है।
- **ब्लॉकचेन सुरक्षाः** स्मार्ट कॉन्ट्रैक्ट की कमजोरियों और ब्लॉकचेन आधारित साइबर हमलों से सुरक्षा पर अभी भी पर्याप्त शोध नहीं हुआ है।

अनुसंधान के उद्देश्य (Research Objectives)

- ऑनलाइन बैंकिंग में साइबर सुरक्षा की जोखिमें की जांच करना,
- साइबर खतरों के बारे में ग्राहकों की जागरूकता का विश्लेषण करना,
- साइबर हमलों के प्रभाव का मूल्यांकन करना,
- बैंकों द्वारा अपनाए गए आवश्यक उपायों का अध्ययन करना,
- सुरक्षित लेन–देन के लिए सुधारों का सुझाव देना।

अनुसंधान पद्धति (Research Methodology)

अनुसंधान पद्धति किसी भी विषय पर शोध अध्ययन करने की एक वैज्ञानिक और व्यवस्थित प्रक्रिया है। सामान्यतः यह वह ब्लूप्रिंट या ढांचा है जिसके अनुसार शोधार्थी अपने प्रश्नों के उत्तर खोजने, समस्याओं को हल करने या नए ज्ञान की खोज के लिए समंक (समंक या जानकारी) कैसे एकत्र करने, उसका विश्लेषण करने और सम्बंधित निष्कर्ष प्राप्त करने की प्रक्रिया।

विश्लेषण के उपकरण (Tools for Analysis)

- प्रतिशत विश्लेषण (Percentage analysis),
- ग्राफिकल प्रतिनिधित्व (Graphical representation)

अनुसंधान डिजाइन (Research Design)

अनुसंधान प्रारूप शोध कार्य को पूरा करने की एक रूपरेखा है। जिस तरह एक घर बनाने से पहले उसका नक्शा तैयार किया जाता है ताकि मकान के सम्पूर्ण ढांचे की जानकारी जैसे कमरों की वास्तु स्थिति, उचित स्थान, विनिर्माण की गुणवत्ता, आवश्यक सामग्री, इसमें लगाने वाले समय और सामग्री कहाँ लेनी है, नींव कैसी होगी और सामग्री कितनी लगेगी इसी प्रकार अनुसंधान प्रारूप यह तय करता है कि शोध के प्रारंभ से लेकर अंतिम निष्कर्ष तक की प्रक्रिया क्या होगी। यह अध्ययन ऑनलाइन बैंकिंग और डिजिटल लेन–देन को

प्रभावित करने वाले साइबर सुरक्षा जोखिमों की जांच और विश्लेषण करने के लिए एक वर्णनात्मक अनुसंधान दृष्टिकोण अपनाता है।

समंक स्रोत (Data Sources)

- **प्राथमिक समंकः** ऑनलाइन बैंकिंग उपयोगकर्ताओं के बीच आयोजित प्रश्नावली आधारित सर्वेक्षण।
- **माध्यमिक समंकः** जर्नल, आरबीआई की रिपोर्ट और प्रकाशित शोध लेख से समंक प्राप्त किए गए हैं।

नमूनाकरण तकनीक (Sampling Technique)

नियमित रूप से ऑनलाइन बैंकिंग सेवाओं का उपयोग करने वाले उत्तरदाताओं से समंक एकत्र करने के लिए सुविधा नमूनाकरण तकनीक का उपयोग किया गया है।

ऑनलाइन बैंकिंग सेवाओं के प्रकार (Types of Online Banking Services)

निम्नलिखित प्रकार की ऑनलाइन बैंकिंग सेवाओं का व्यापक रूप से उपयोग किया जाता है और ये साइबर सुरक्षा खतरों के अधीन हैंः–

- इंटरनेट बैंकिंग,
- मोबाइल बैंकिंग,
- एटीएम सेवाएं,
- यूपीआई लेन–देन,
- डिजिटल वॉलेट।

ये सेवाएँ सुविधाओं के साथ–साथ साइबर जोखिमों के प्रति जोखिम भी बढ़ाती रहती हैं।

प्रमुख साइबर सुरक्षा की समस्या (Major Cyber Security Issues)

- **फिशिंग (Phishing):** यह ऑनलाइन बैंकिंग लेन–देन में उपयोगकर्ताओं को नकारात्मक रूप से सबसे अधिक प्रभावित करने वाले उपकरणों में आता है और इसकी पृक्राति अधिक खतरनाक है। इसमें धोखाधड़ी करने वाले संचार के साधन जैसे ईमेल, एसएमएस (संदेश) एवं नकली वेबसाइट के रूप में होते हैं जिन्हें उपयोगकर्ताओं को लॉगिन क्रेडेंशियल, ओटीपी, डेबिट कार्ड विवरण एवं पिन जैसी संवेदनशील जानकारी प्राप्त करने के लिए डिजाइन किया गया है। साइबर अपराधी पीड़ित का विश्वास जीतने के लिए विश्वसनीय बैंकों भुगतान प्लेटफार्मों अधिकारिक सदस्य बनकर अपने जाल में फंसाकर ऑनलाइन ठगी को अंजाम देने के लिए जालसाज आसानी से बैंक खातों को अपने नियंत्रण मे लेकर अनधिकृत लेन–देन कर सकते हैं।
- **मैलवेयर (Malware):** यह ऑनलाइन बैंकिंग में असुरक्षित डाउनलोड, ईमेल अटैचमेंट या दुर्भावनापूर्ण लिंक के माध्यम से उपयोगकर्ता के उपकरण में प्रवेश कर सकता है और यह उपभोगता के उपकरण में एक बार इंस्टॉल होने के पश्चात् उपयोगकर्ता की समस्त गतिविधियों को ट्रैक करने, लॉगिन विवरण कैप्चर करने और सम्बंधित उपकरण को दूरस्थ रूप से नियंत्रित भी करके अनधिकृत लेन–देन कर सकते हैं और ग्राहक को इसकी कार्यप्रणाली का एहसास भी नहीं होता है क्योंकि ये अक्सर चुपचाप काम करते हैं।
- **पहचान की चोरी (Identity Theft):** जब साइबर अपराधी किसी व्यक्ति का रूप धारण करने के लिए नाम, आधार नंबर, फोन नंबर या बैंक विवरण जैसी व्यक्तिगत जानकारी चुरा लेते हैं तब वह पहचान की चोरी होती हैद्य ऑनलाइन बैंकिंग में पहचान की चोरी एक खतरनाक समस्या है क्योंकि डिजिटल प्लेटफॉर्म प्रमाणीकरण के लिए व्यक्तिगत समंक पर बहुत अधिक निर्भर करते हैं। इससे न केवल वित्तीय नुकसान होता है बल्कि पीड़ित के लिए दीर्घकालिक जटिलताएं भी उत्पन्न होती हैं जिसके

परिणामस्वरूप कानूनी प्रक्रियाओं में उलझना, उपभोक्ता का मानसिक रूप से टूटना और क्रेडिट स्कोर खराब होना आदि समस्याओं का सामना करना पड़ता है।

- **समंक सेंधमारी (Data Breaches):** दुर्बल सुरक्षा प्रणालियों, सॉफ्टवेयर की कमियों एवं संथागत संस्थाओं में अंदरूनी जान पहचान के कारण बैंकिंग प्रणालियों या डिजिटल प्लेटफार्मों में संग्रहीत संवेदनशील जानकारी तक अनधिकृत रूप से पड़ताल करने के कारण बैंकिंग प्रणालियों या डिजिटल प्लेटफार्मों में संग्रहीत संवेदनशील जानकारी अनधिकृत रूप से अपने अधिकार में लेकर लेन–देन करते समंक सेंधमारी करते हैंद्य इस प्रक्रिया में एक नहीं बल्कि लाखों या करोड़ों उपयोगकर्ता प्रभावित होते हैं। इस प्रकार लीक हुए समंक का उपयोग फिशिंग, पहचान की चोरी और वित्तीय धोखाधड़ी जैसे अन्य साइबर अपराधों के लिए किया जा सकता है।
- **मैन–इन–द–मिडिल हमले (Man-in-the-Middle Attacks):** यदि कोई साइबर अपराधी उपयोगकर्ता और बैंकिंग प्रणाली के मध्य संचार को बीच में ही रोक कर यह सामान्यतः सार्वजनिक वाई–फाई जैसे असुरक्षित नेटवर्क के माध्यम से जाल्साझ किसी भी पक्ष की जानकारी के बिना गुप्त रूप से संचार की निगरानी करके उसे परवर्तित करके इस प्रक्रिया को अंतिम रूप देता सकता है।
- **सिम स्वैप धोखाधड़ी (SIM Swap Fraud):** यह ऑनलाइन बैंकिंग के क्षेत्र में बढ़ता हुआ साइबर सुरक्षा को चुनौती देने वाला एक उपकरण है। इसमे हमलावर पीड़ित का रूप धारण करके दूरसंचार प्रदाता को पीड़ित का फोन नंबर एक नए सिम पर स्थानांतरित करने के लिए मनाकर एक प्रतिलिपि (डुप्लिकेट) सिम कार्ड प्राप्त कर लेते हैं। जालसाज एक बार पीड़ित के मोबाइल नंबर पर नियंत्रण प्राप्त कर लेते है तो वे बैंकिंग लेन–देन से संबंधित ओटीपी और अन्य एस एम् एस प्राप्त कर के धोखाधड़ी सकते हैं।
- **पासवर्ड हमले (Password Attacks):** पासवर्ड हमलों में साइबर अपराधियों द्वारा पासवर्ड का अनुमान लगाकर या उन्हें क्रैक करके उपयोगकर्ता के खातों से सम्बंधित जानकारी प्राप्त करने के प्रयास करते हैं। इस प्रक्रिया में ब्रूट फोर्स (Brute force) उपकरण आता है इसमें अनेक पासवर्ड संयोजनों का प्रयास किया जाता है और क्रेडेंशियल स्टफिंग (Credential stuffing), जिसमें अन्य प्लेटफार्मों से चुराए गए पासवर्ड का पुनः उपयोग किया जाता है। यह ऑनलाइन बैंकिंग के लिए पासवर्ड का उपयोग करने का प्रमुख और सटीक तरीका है।
- **सोशल इंजीनियरिंग हमले (Social Engineering Attacks):** सोशल इंजीनियरिंग हमले तकनीकी कमजोरियों का फायदा उठाने के स्थान पर मानवीय व्यवहार में परिवर्तन करने पर निर्भर करते हैं। जालसाज फोन कॉल, संदेश या ईमेल के माध्यम से पीड़ितों के साथ सीधे बात करते हुए बैंक अधिकारी या सेवा प्रदाता होने का नाटक करते हैं। वे उपयोगकर्ताओं को गोपनीय जानकारी साझा करने के लिए राजी करने के लिए तात्कालिकता या डर की भावना पैदा करते हैं। ऑनलाइन बैंकिंग धोखाधड़ी में साइबर अपराधियों द्वारा उपयोग की जाने वाली यह सबसे अधिक प्रभावी विधियों में से एक है।

साइबर सुरक्षा मुद्दों के कारण (Causes of Cyber Security Issues)

- उपयोगकर्ताओं में जागरूकता की कमी होना,
- आसान एवं सुविधाजनक पासवर्ड का उपयोग करना,
- सार्वजनिक वाई–फाई नेटवर्क का उपयोग करना,
- व्यक्तिगत और बैंकिंग जानकारी साझा करना,
- उपयोग में लिए जाने वाले पुराने सॉफ्टवेयर और सुरक्षा प्रणालियों का उपयोग करना।

साइबर सुरक्षा जोखिमों का प्रभाव (Impact of Cyber Security Issues)

साइबर सुरक्षा खतरों के उपयोगकर्ताओं और वित्तीय संस्थानों दोनों के लिए गंभीर परिणाम होते हैंः–

- ग्राहकों और बैंकों को वित्तीय हानि होना,
- डिजिटल बैंकिंग प्रणालियों में उपयोगकर्ता के विश्वास की कमी होना,
- वित्तीय संस्थानों की प्रतिष्ठा में कमी होना,
- कानूनी परिणाम और नियामक दंड का सामना करना,
- बैंकिंग और डिजिटल भुगतान सेवाओं में व्यवधान उत्पन्न होना।

परिणाम (Findings)

- विभिन्न प्रयासों से उपयोगकर्ता समयानुसार जागरूक तो हो रहे हैं लेकिन साइबर धोखाधड़ी को रोकने के लिए ये प्रयास अपर्याप्त हो सकते हैं।
- ऑनलाइन बैंकिंग में फिशिंग सबसे अधिक और प्रभावशाली खतरा है।
- अधिकतम उपयोगकर्ता लेन–देन में ऑनलाइन बैंकिंग की असुरक्षित प्रणालियों का उपयोग करते हैं।
- उपयोगकर्ता समय–समय पर बैंक द्वारा दिए जाने वाले दिशानिर्सेशों की अनुपालना नहीं करते हैं।

सुझाव (Suggestions)

- बैंकों और विनियामक निकायों द्वारा आधुनिक एवं वैश्विक स्तर के जागरूकता कार्यक्रम आयोजित करने चाहिए।
- उपयोगकर्ताओं को सुद्रढ़ और सटीक पासवर्ड का उपयोग करने के लिए प्रोत्साहित करना चाहिए।
- उपयोगकर्ताओं को सार्वजनिक वाई–फाई के माध्यम से बैंकिंग सेवाओं का उपयोग करने से बचने की सलाह देनी चाहिए।
- एआई–आधारित धोखाधड़ी का पता लगाने वाली प्रणाली के साथ बैंक की सुरक्षा प्रणालियों में सुधार करना चाहिए।
- नियमित सॉफ्टवेयर अपडेट करना और ग्राहकों को सुरक्षा अलर्ट भेजते रहना चाहिए।

प्रबंधकीय निहितार्थ (Managerial Implications)

- **बैंकों और वित्तीय संस्थानों के लिए निहितार्थ (Implications for Banks and Financial Institutions):** बैंकों को आर्टिफिशियल इंटेलिजेंस, मशीन लर्निंग और रीयल–टाइम धोखाधड़ी की पहचान की प्रणालियों में उन्नत तकनीकों को अपनाकर अपने साइबर सुरक्षा के परम्परागत ढांचे को लगातार अधतन करना चाहिए। बैंकों को ग्राहक शिक्षा और जागरूकता कार्यक्रमों पर भी ध्यान केंद्रित करना चाहिए, उपयोगकर्ता के अनुकूल सुरक्षा प्रणालियां लागू करननी चाहिए, निरंतर निगरानी और जोखिम मूल्यांकन करना चाहिए।
- **ग्राहकों के लिए निहितार्थ (Implications for Customers):** साइबर सुरक्षा बनाए रखने के लिए ग्राहक भी समान रूप से जिम्मेदार हैं। उपयोगकर्ताओं को ओटीपी, पासवर्ड और बैंकिंग विवरण जैसी गोपनीय जानकारी साझा करने से बचना चाहिए। ग्राहकों को सुद्रड और अद्वितीय पासवर्ड का उपयोग करना चाहिए, मल्टी–फैक्टर ऑथेंटिकेशन प्रणाली को लागू करना चाहिए, नियमित रूप से अपने उपकरणों को अपडेट करना चाहिए, और सार्वजनिक या असुरक्षित नेटवर्क के माध्यम से बैंकिंग सेवाओं के उपयोग से बचना चाहिए।

- **फिनटेक कंपनियों के लिए निहितार्थ (Implications for FinTech Companies):** फिनटेक कंपनियों को सुरक्षित सिस्टम, डिजाइन और समंक सुरक्षा को प्राथमिकता देनी चाहिए। उन्हें एकीकृत सुरक्षा समाधान विकसित करने के लिए बैंकों के साथ सहयोग करना चाहिए और उपयोगकर्ता आधारित सुरक्षात्मक सुविधाएँ विक्सित करनी चाहिए जो सरल और सुरक्षित प्रमाणीकरण तंत्र प्रदान कर सकती हैं।
- **नियामक अधिकारियों के लिए निहितार्थ (Implications for Regulatory Authorities):** नियामक निकायों को साइबर सुरक्षा मानकों का सख्त दिशानिर्देश लागू करने चाहिए, नवीन जोखिमों से निपटने के लिए दिशानिर्देशों को नियमित रूप से अपडेट करना चाहिए और डिजिटल साक्षरता व जागरूकता कार्यक्रमों को बढ़ावा देना चाहिए। उन्हें साइबर सुरक्षा में उन्नत तकनीकों को अपनाने और नवाचार को भी प्रोत्साहित करना चाहिए।
- **डिजिटल अर्थव्यवस्था के लिए निहितार्थ (Implications for the Digital Economy):** साइबर सुरक्षा में सुधार से ग्राहकों का विश्वास बढ़ सकता है, डिजिटल भागीदारी बढ़ सकती है और आर्थिक विकास में वृद्दि हो सकती है, बार–बार होने वाले साइबर हमले विश्वास को कम कर सकते हैं जिससे लेन–देन की डिजिटल प्रणाली को अपनाने की गति धीमी हो सकती है। क्योंकि अर्थव्यवस्था के सतत विकास के लिए एक सुरक्षित डिजिटल वातावरण आवश्यक है।

अध्ययन की सीमाएँ (Limitations of the Study)

- यह अध्ययन एक सीमित नमूना प्रणाली पर आधारित है जो ऑनलाइन बैंकिंग के उपयोगकर्ताओं की सम्पूर्ण जनसँख्या का पूर्णतया प्रतिनिधित्व नहीं कर सकता है।
- यह शोध अध्ययन आंशिक रूप से एकत्रित समंकों की व्यक्तिगत धारणाओं पर आंशिक परिवर्तित हो सकता है जो पूर्वाग्रह से ग्रसित भी हो सकता है।
- शोधकर्ता समयाभाव के कारण इस अध्ययन को व्यापक भौगोलिक क्षेत्र के अनुसार पूर्णतया समाविष्ट नहीं कर सका या अधिक संख्या में उत्तरदाताओं को सम्मिलित नहीं करने से परिणामों में भिन्नता हो सकती है।
- इस अध्ययन में उन्नत सांख्यिकीय उपकरणों को लागू करने के पश्चात् भी सांख्यिकीय विश्लेषण विभिन्न विधियों पर केंद्रित होने से सांख्यिकीय विभ्रमों के कारण परिणामों में भिन्नता हो सकती है।
- यह अनुसंधान मुख्य रूप से उपयोगकर्ताओं के जागरूकता और सामान्य साइबर जोखिमों पर अधिक बल देता है लेकिन एन्क्रिप्शन एल्गोरिदम या नेटवर्क सुरक्षा ढांचा जैसी तकनीकी पहलुओं का उचित विश्लेषण नहीं कर पता है।
- साइबर जोखिमों में तीव्र गति से परिवर्तित होती हुई प्रकृति का तात्पर्य यह है कि यदि नियमित रूप से इसे अदधानता अपडेट न किया जाए तो निष्कर्ष समय के साथ पुराने हो सकते हैं।
- अध्ययन में बैंकों या वित्तीय संस्थानों के विस्तृत मामलों के विशिष्ट समंक सम्मिलित नहीं होने से परिणामों में भिन्नता हो सकती है क्योंकि कुछ समंक गोपनीय होते हैं।

भविष्य में अध्ययन का दायरा (Future Scope of the Study)

- अधिक व्यापक और सामान्यीकरण योग्य परिणाम प्रदान करने के लिए भविष्य के अध्ययन बड़े नमूना आकार और व्यापक भौगोलिक समाविष्ट करने के साथ आयोजित किए जा सकते हैं।
- शोधकर्ता विभिन्न चरों के मध्य संबंधों के परिक्षण में प्रतीपगमन विश्लेषण, कारक विश्लेषण, और परिकल्पना परीक्षण जैसे उन्नत सांख्यिकीय उपकरणों को लागू कर सकते हैं।

- विभिन्न बैंकिंग प्रणालियों जैसे सार्वजनिक क्षेत्र के बैंकों, निजी बैंकों और फिनटेक प्लेटफॉर्मों के मध्य परसपर तुलनात्मक विश्लेषण किया जा सकता है।
- यह अध्ययन भविष्य में साइबर सुरक्षा में उभरती प्रौद्योगिकियों पर ध्यान केंद्रित कर सकता हैद्य जैसे कि आर्टिफिशियल इंटेलिजेंस, ब्लॉकचेन, बायोमेट्रिक प्रामाणिकता और मशीन लर्निंग–आधारित धोखाधड़ी का पता लगाना।
- उपयोगकर्ताओं के व्यवहार संबंधी पहलुओं और जोखिम भरे ऑनलाइन व्यवहार को प्रभावित करने वाले मनोवैज्ञानिक कारकों पर शोध आधारित प्रभावशाली जागरूकता कार्यक्रम तैयार करने में मदद कर सकता है।
- साइबर सुरक्षा प्रणालियों में सुधारने पर सरकारी नीतियों और नियामक ढांचों के प्रभाव की और जांच की जा सकती है।
- वास्तविक साइबर धोखाधड़ी की घटनाओं से जुड़े मामलों के अध्ययन पर आधारित शोध अध्ययन व्यावहारिक पक्ष प्रदान कर सकते हैं जिससे यह जानकारी मिल सके कि साइबर हमले कैसे होते हैं और उन्हें कैसे रोका जाना चाहिए।

संभावित शोध विषय (Research Topics)

- आर्टिफिशियल इंटेलिजेंस आधारित फिशिंग हमलों की पहचान और रोकथाम।
- इंटरनेट आधारित उपकरणों के लिए सुरक्षित प्रमाणीकरण मॉडल।
- क्लाउड कंप्यूटिंग में समंक गोपनीयता और सुरक्षा प्रणाली।
- रैनसमवेयर की रियल–टाइम पहचान के लिए मशीन लर्निंग आधारित मॉडल।
- क्वांटम युग के लिए सुरक्षित एन्क्रिप्शन तकनीकों का अध्ययन।
- साइबर सुरक्षा जागरूकता का उपयोगकर्ताओं के व्यवहार पर प्रभाव।
- ये विषय एम.टेक., एमसीए., बी.टेक., एमबीए (आईटी) और पीएचडी स्तर के शोध के लिए उपयुक्त हैं।

निष्कर्ष (Conclusion)

ऑनलाइन बैंकिंग और ऑनलाइन लेन–देन को प्रभावित करने वाले साइबर सुरक्षा मामलों पर अध्ययन वर्तमान समय में वित्तीय लेन–देन के वातावरण में डिजिटल सुरक्षा के बढ़ते महत्व पर प्रकाश डालता है। डिजिटल बैंकिंग सेवाओं के बढ़ते उपयोग के साथ ग्राहकों को 24/7 लेन–देन की सुविधा, लेन–देन की तीव्र गति और आवश्यक आने लाभ मिलते हैं। इस शोध अध्ययन में विभिन्न साइबर सुरक्षा मामलों जैसे फिशिंग हमलों, मैलवेयर, पहचान की चोरी और समंक उल्लंघन की पहचान करने,वग्राहकों और वित्तीय संस्थानों के लिए गंभीर जोखिम पैदा करने और फिशिंग व उपयोगकर्ता से जुड़ी कमियां सबसे अधिक मात्रा में और प्रभावशाली खतरों के रूप में सामने आई हैं। यह अध्ययन इस बात पर भी जोर देता है कि साइबर सुरक्षा केवल एक तकनीकी मुद्दा नहीं है बल्कि बैंकों, ग्राहकों और नियामक अधिकारियों की एक संयुक्त जिम्मेदारी है। बैंकों को अपनी सुरक्षा प्रणालियों को लगातार अधत्तन और ग्राहकों को शिक्षित करना चाहिए, जबकि उपयोगकर्ताओं को सुरक्षित बैंकिंग प्रणालियों को अपनाते हुए ऑनलाइन लेन–देन के दौरान सतर्क रहना चाहिए। ऑनलाइन बैंकिंग में साइबर सुरक्षा सुनिश्चित करने के लिए प्रौद्योगिकी, जागरूकता और विनियमन को मिलाने वाले एक संतुलित दृष्टिकोण की आवश्यकता है। इन तीनों स्तंभों को मजबूत करने से साइबर जोखिमों को बहुत अधिक मात्रा में कम किया जा सकता है जिससे डिजिटल वित्तीय प्रणालियों में विश्वास उत्पन्न किया जा सकता है। अर्थात ऑनलाइन बैंकिंग और डिजिटल लेन–देन के लिए एक सुरक्षित, विश्वसनीय और संरक्षित वातावरण बनाने के साथ–साथ सक्रिय और सहयोगात्मक प्रयास आवश्यक होता है।

आभार (Acknowledgment)

लेखक इस शोध अध्ययन को पूर्ण करने में समस्त सहयोगी उत्तरदाताओं और इससे संबन्धित पक्षकारों के प्रति भी आभार व्यक्त करता हैं जिन्होंने इस सर्वेक्षण में भाग लेकर अपने कीमती सुझावा दिए।

संदर्भ ग्रन्थ सूची (References)

1. Symantec Corporation. Internet Security Threat Report. Symantec, 2022.
2. NASSCOM. Cyber Security in India – Perspectives, Priorities, and Considerations. NASSCOM, 2021.
3. Shey, H.G., et al. "Understanding Cyber Security Challenges in Online Banking and Financial Transactions." Journal of Cyber Security Research, Vol. 3, No. 1, 2020.
4. Kumar, S. and Sinha, R. "Phishing Attacks and Online Banking: A Study of User Awareness." International Journal of Information Security, 2019
5. Reserve Bank of India (RBI). Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. RBI, 2011.
6. Aimé, F. (2022). SpyGuard. https://github.com/SpyGuard/SpyGuard
7. Althouse, J. B., Atkinson, J., & Atkins, J. (2017–2025). JA3: A standard for creating SSL client fingerprints (Computer software). GitHub. https://github.com/salesforce/ja3
8. Amnesty International Security Lab. (2021, July 18). Forensic methodology report: How to catch NSO Group's Pegasus. Amnesty International.

   https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Websites

9. https://sansorg.egnyte.com/dl/KPgmR663V6km
10. https://www.sans.edu/cyber-research/entra-id-governance-insta-iamiga-solution
11. https://journal.cisse.info/jcisse
12. https://academic.oup.com/cybersecurity
13. https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

❑❑❑