

साइबर सुरक्षा को सुदृढ़ करने में बैंकों की भूमिका: एक अध्ययन

Hargovind Kharera*

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

*Corresponding Author: hgkharera@gmail.com

Citation: Kharera, H. (2026). साइबर सुरक्षा को सुदृढ़ करने में बैंकों की भूमिका: एक अध्ययन. *International Journal of Education, Modern Management, Applied Science & Social Science*, 08(03(III)), 57–68.

सार

वर्तमान डिजिटल युग में बैंकिंग प्रणाली में तीव्र गति से आधुनिक प्रौद्योगिकी के अनुसार परिवर्तन हो रहे हैं। इंटरनेट बैंकिंग, मोबाइल बैंकिंग, डिजिटल भुगतान, एटीएम, त्वरित भुगतान प्रणाली तथा अन्य इलेक्ट्रॉनिक बैंकिंग सेवाओं ने बैंकिंग कार्यों को अधिक सरल, तीव्र एवं सुविधाजनक बनाया है। लेकिन इसके विपरीत डिजिटल बैंकिंग के विस्तार के साथ साइबर अपराध, ऑनलाइन धोखाधड़ी, मुख्य पहचान की चोरी, फिशिंग, मैलवेयर, रैनसमवेयर, अनधिकृत लेन-देन तथा ग्राहक संबंधी संवेदनशील सूचनाओं के दुरुपयोग जैसे साइबर जोखिमों में भी वृद्धि हुई है। ऐसी स्थिति में बैंकों की भूमिका केवल वित्तीय सेवाएँ उपलब्ध कराने तक सीमित नहीं रह जाती है बल्कि उन्हें सुरक्षित एवं विश्वसनीय डिजिटल बैंकिंग वातावरण विकसित करने की महत्वपूर्ण जिम्मेदारी भी निभानी पड़ती है। भारतीय रिजर्व बैंक द्वारा बैंकों के लिए साइबर सुरक्षा एवं साइबर लचीलापन संबंधी आवश्यकताओं पर विशेष बल दिया जा रहा है। इनमें बोर्ड-स्तरीय निगरानी, वास्तविक अथवा लगभग वास्तविक समय में सुरक्षा घटनाओं की निगरानी, साइबर सुरक्षा संचालन केंद्र, जोखिम प्रबंधन तथा घटना की प्रतिक्रिया जैसे महत्वपूर्ण उपाय देखने को मिल रहे हैं। इसी के साथ-साथ भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) साइबर घटनाओं की सूचना, विश्लेषण, चेतावनी तथा साइबर घटना की प्रतिक्रिया के समन्वय में राष्ट्रीय स्तर पर महत्वपूर्ण भूमिका निभा रहा है। यह शोध-पत्र साइबर सुरक्षा को सुदृढ़ करने में बैंकों की भूमिका का विश्लेषण कर सकता है तथा तकनीकी सुरक्षा, जोखिम प्रबंधन, ग्राहक जागरूकता, कर्मचारी प्रशिक्षण, साइबर निगरानी, घटना प्रतिक्रिया और विनियामकीय अनुपालना के माध्यम से बैंकिंग क्षेत्र में साइबर लचीलापन विकसित करने के उपायों को प्रकाशित भी कर सकता है।

शब्दकोश: साइबर सुरक्षा, बैंकिंग क्षेत्र, डिजिटल बैंकिंग, साइबर अपराध, साइबर जोखिम, डिजिटल भुगतान, सूचना सुरक्षा, ग्राहक जागरूकता।

प्रस्तावना

बैंक किसी भी आधुनिक अर्थव्यवस्था की वित्तीय संरचना का महत्वपूर्ण आधार होते हैं। पारंपरिक बैंकिंग व्यवस्था में बैंक शाखाओं में नकद लेन-देन एवं भौतिक अभिलेखों पर अधिक निर्भर रहते थे लेकिन वर्तमान समय में सूचना एवं संचार प्रौद्योगिकी के विकास के कारण बैंकिंग सेवाएँ डिजिटल माध्यमों पर अत्यधिक निर्भर हो रही हैं। इसमें इंटरनेट बैंकिंग, मोबाइल बैंकिंग, एटीएम से लेन-देन, कार्ड से भुगतान, इलेक्ट्रॉनिक निधि अंतरण तथा त्वरित डिजिटल भुगतान ने बैंकिंग सेवाओं की प्रक्रिया को सरल एवं अधिक व्यापक बना दिया है। इसके परिणामस्वरूप ग्राहकों को 24/07 दिवस में बैंकिंग सेवाओं का लाभ प्राप्त हो रहा है। दूसरी ओर बैंकिंग

प्रणालियों के बढ़ते डिजिटलीकरण से साइबर अपराधियों के लिए भी नवीन अवसर उत्पन्न हो रहे हैं। इस परिस्थिति में साइबर सुरक्षा बैंकिंग क्षेत्र की मूलभूत आवश्यकता बनती जा रही है। बैंकों को ग्राहक की धन राशि के साथ-साथ उसकी व्यक्तिगत, वित्तीय एवं पहचान संबंधी सूचनाओं की भी सुरक्षा करनी पड़ती है।

साइबर सुरक्षा की अवधारणा

साइबर सुरक्षा की प्रभावी व्यवस्था मुख्यतः तीन आधारभूत सिद्धांतों पर आधारित है, जिन्हें सामान्यतः सी.आई.ए. त्रयी (CIA Triad) कहा जाता है। इसमें गोपनीयता, अखंडता तथा उपलब्धता को साइबर सुरक्षा के प्रमुख स्तंभ माना गया है। किसी भी सूचना प्रणाली की सुरक्षा सुनिश्चित करने के लिए इन तीनों तत्वों का संतुलित एवं प्रभावी होना आवश्यक है।

- **गोपनीयता (Confidentiality)**

गोपनीयता का तात्पर्य सूचना एवं आँकड़ों को अनधिकृत व्यक्तियों के नियंत्रण, उपयोग अथवा प्रकटीकरण से सुरक्षित रखना है। इसका उद्देश्य यह सुनिश्चित करना है कि संवेदनशील एवं महत्वपूर्ण सूचना केवल अधिकृत व्यक्तियों अथवा संस्थाओं तक ही सीमित रहे। इसकी गोपनीयता बनाए रखने के लिए पासवर्ड, बहु-स्तरीय प्रमाणीकरण, कूटलेखन तथा अन्य सुरक्षा उपायों का उपयोग किया जाता है।

- **अखंडता (Integrity)**

अखंडता का अर्थ सूचना की शुद्धता, विश्वसनीयता तथा पूर्णता को बनाए रखना है। इसके अंतर्गत यह सुनिश्चित किया जाता है कि किसी सूचना अथवा आँकड़े में अनधिकृत रूप से परिवर्तन, संशोधन, विलोपन अथवा छेड़-छाड़ न की जा सके। सूचना की अखंडता बनाए रखना विशेष रूप से बैंकिंग, वित्तीय लेन-देन तथा अन्य संवेदनशील डिजिटल सेवाओं के लिए अत्यंत आवश्यक होता है।

- **उपलब्धता (Availability)**

उपलब्धता का तात्पर्य यह सुनिश्चित करना है कि सूचना, डिजिटल प्रणाली एवं आवश्यक सेवाएँ अधिकृत उपयोगकर्ताओं को आवश्यकता पड़ने पर उचित समय पर उपलब्ध होती रहें। किसी तकनीकी खराबी, साइबर आक्रमण अथवा अन्य व्यवधान के कारण इन सेवाओं की निरंतरता बाधित न हो इसके लिए उपयुक्त सुरक्षा व्यवस्था, बैकअप, पुनर्प्राप्ति प्रणाली तथा वैकल्पिक व्यवस्थाओं का होना आवश्यक होता है।

बैंकिंग क्षेत्र में साइबर सुरक्षा का महत्व

वर्तमान समय में सूचना एवं संचार प्रौद्योगिकी के तीव्र विकास के परिणामस्वरूप बैंकिंग क्षेत्र में व्यापक परिवर्तन आया है। परंपरागत बैंकिंग व्यवस्था के स्थान पर इंटरनेट बैंकिंग, मोबाइल बैंकिंग, स्वचालित गणक मशीन (एटीएम), इलेक्ट्रॉनिक धन अंतरण, त्वरित भुगतान प्रणाली तथा अन्य डिजिटल बैंकिंग सेवाओं का व्यापक रूप से उपयोग किया जा रहा है। इन तकनीकी सुविधाओं ने बैंकिंग सेवाओं को अधिक सरल, तीव्र, सुलभ एवं सुविधाजनक बनाया है। किंतु दूसरी ओर, बैंकिंग गतिविधियों के बढ़ते डिजिटलीकरण ने साइबर अपराधों तथा डिजिटल धोखाधड़ी की संभावनाओं को भी बढ़ाया है। अतः वर्तमान बैंकिंग व्यवस्था में साइबर सुरक्षा का महत्व अत्यधिक बढ़ता जा रहा है।

- **ग्राहकों की गोपनीय सूचना का संरक्षण**

बैंकिंग संस्थानों में ग्राहकों से संबंधित अत्यंत संवेदनशील सूचनाएँ संग्रहीत रहती हैं। साइबर सुरक्षा का प्रमुख उद्देश्य इन सूचनाओं को अनधिकृत नियंत्रण, चोरी, प्रकटीकरण तथा दुरुपयोग से सुरक्षित रखना है। सुदृढ़ साइबर सुरक्षा व्यवस्था के माध्यम से यह सुनिश्चित किया जाता है कि ग्राहक की व्यक्तिगत एवं वित्तीय जानकारी केवल अधिकृत व्यक्ति या अधिकृत प्रणाली द्वारा ही प्राप्त की जा सके। इससे ग्राहकों की निजता की रक्षा होती है तथा बैंकिंग व्यवस्था के प्रति उनका विश्वास बना रहता है।

- **वित्तीय लेन-देन की सुरक्षा**

डिजिटल बैंकिंग के विस्तार के कारण वित्तीय लेन-देन का एक बड़ा भाग इलेक्ट्रॉनिक माध्यमों से संपन्न हो रहा है। धन अंतरण, बिल भुगतान, ऑनलाइन खरीदारी तथा अन्य वित्तीय गतिविधियाँ डिजिटल प्रणालियों के माध्यम से की जाती हैं। ऐसी स्थिति में प्रत्येक लेन-देन की सुरक्षा अत्यंत आवश्यक हो गई है। साइबर सुरक्षा उपाय अनधिकृत लेन-देन, धन की चोरी तथा डिजिटल धोखाधड़ी की संभावनाओं को कम करने में सहायता करते हैं।

- **साइबर धोखाधड़ी की रोकथाम**

बैंकिंग क्षेत्र में फिशिंग, पहचान की चोरी, सामाजिक अभियांत्रिकी, दुर्भावनापूर्ण सॉफ्टवेयर, नकली वेबसाइट तथा अन्य डिजिटल माध्यमों से धोखाधड़ी की जा सकती है। साइबर अपराधी प्रायः ग्राहकों की गोपनीय जानकारी प्राप्त करके उनके बैंक खातों से धन निकालने का प्रयास करते हैं। प्रभावी साइबर सुरक्षा प्रणाली संदिग्ध गतिविधियों की पहचान करने, अनधिकृत नियंत्रण को रोकने तथा संभावित साइबर धोखाधड़ी के विरुद्ध समय पर कार्रवाई करने में सहायक होती है।

- **बैंकिंग सेवाओं की निरंतर उपलब्धता**

बैंकिंग व्यवस्था में सेवाओं की निरंतर उपलब्धता अत्यंत महत्वपूर्ण है। यदि किसी साइबर आक्रमण, तकनीकी विफलता अथवा अन्य कारण से बैंक की डिजिटल प्रणाली बाधित होती है तो ग्राहकों को धन अंतरण, भुगतान, निकासी तथा अन्य आवश्यक सेवाओं में कठिनाई हो सकती है। इसलिए साइबर सुरक्षा का एक महत्वपूर्ण उद्देश्य बैंकिंग प्रणालियों को ऐसे व्यवधानों से सुरक्षित रखना तथा किसी आकस्मिक घटना के पश्चात सेवाओं को शीघ्र पुनः सामान्य करना है।

- **बैंक एवं ग्राहक के मध्य विश्वास का संरक्षण**

बैंकिंग व्यवस्था का मूल आधार विश्वास है। ग्राहक अपनी धनराशि एवं व्यक्तिगत जानकारी बैंक को इस विश्वास के साथ सौंपता है कि बैंक उसका सुरक्षित संरक्षण करेगा। यदि बैंकिंग प्रणाली में बार-बार साइबर धोखाधड़ी अथवा सूचना के उल्लंघन की घटनाएँ होती हैं तो ग्राहकों का बैंक के प्रति विश्वास कमजोर हो सकता है। अतः प्रभावी साइबर सुरक्षा बैंक एवं ग्राहक के मध्य विश्वास को बनाए रखने का महत्वपूर्ण साधन है।

साइबर सुरक्षा को सुदृढ़ करने में बैंकों की भूमिका

वर्तमान में बैंकिंग व्यवस्था का तीव्र गति से डिजिटलीकरण होने के कारण बैंकिंग सेवाएँ सूचना एवं संचार प्रौद्योगिकी पर अत्यधिक निर्भर हो रही हैं। इंटरनेट बैंकिंग, मोबाइल बैंकिंग, इलेक्ट्रॉनिक धन अंतरण, त्वरित भुगतान प्रणाली तथा स्वचालित बैंकिंग सेवाओं के विस्तार ने बैंकिंग कार्यों को अधिक सुविधाजनक और सुलभ बनाया है। इसके साथ ही बैंकिंग संस्थानों के सूचना-तंत्र, ग्राहक संबंधी आँकड़ों तथा वित्तीय लेन-देन पर साइबर आक्रमणों का जोखिम भी बढ़ रहा है। ऐसी परिस्थितियों में साइबर सुरक्षा को सुदृढ़ करना बैंकों की महत्वपूर्ण जिम्मेदारी बन गई है।

- **ग्राहकों के वित्तीय एवं व्यक्तिगत आँकड़ों की सुरक्षा करना**

बैंकों की प्रथम भूमिका ग्राहकों के वित्तीय एवं व्यक्तिगत आँकड़ों की सुरक्षा सुनिश्चित करना है। बैंक ग्राहकों की पहचान, खाते से संबंधित विवरण, संपर्क संबंधी जानकारी तथा वित्तीय लेन-देन से संबंधित अत्यंत संवेदनशील आँकड़ों का संधारण करते हैं। इन आँकड़ों तक अनधिकृत पक्षकारों की सेंदमारी को रोकने के लिए बैंकों द्वारा सुरक्षित सूचना-तंत्र, कूटलेखन, प्रवेश नियंत्रण तथा प्रभावी प्रमाणीकरण जैसी सुरक्षा व्यवस्थाओं को अपनाना आवश्यक है। इससे ग्राहकों की गोपनीय जानकारी के दुरुपयोग और अनधिकृत लेन-देन की संभावना को कम किया जा सकता है।

- **साइबर जोखिमों की पहचान एवं निरंतर निगरानी करना**

बैंकों की दूसरी महत्वपूर्ण भूमिका साइबर जोखिमों की पहचान एवं निरंतर निगरानी करना है। साइबर अपराधी समय के साथ नवीन तकनीकों और विधियों का उपयोग कर रहे हैं। इसलिए केवल एक बार सुरक्षा व्यवस्था स्थापित कर देना पर्याप्त नहीं है। बैंकों को अपने सूचना-तंत्र की नियमित निगरानी, सुरक्षा परीक्षण तथा जोखिम मूल्यांकन करते रहना चाहिए। संदिग्ध गतिविधियों की शीघ्र पहचान करके उन पर समय पर आवश्यक कार्रवाई करने से साइबर घटनाओं के प्रभाव को सीमित किया जा सकता है।

- **सुरक्षित प्रमाणीकरण एवं अभिगम नियंत्रण**

सुरक्षित प्रमाणीकरण एवं अभिगम नियंत्रण भी साइबर सुरक्षा को सुदृढ़ करने में बैंकों की महत्वपूर्ण भूमिका है। बैंकिंग प्रणालियों में यह सुनिश्चित किया जाना आवश्यक है कि केवल अधिकृत ग्राहक और कर्मचारी ही संबंधित खातों एवं प्रणालियों को नियंत्रित कर सकें। इसके लिए बहु-स्तरीय प्रमाणीकरण, सुरक्षित संकेत-पद, एक बार उपयोग होने वाला संकेतांक तथा अन्य उपयुक्त सुरक्षा उपायों का प्रयोग किया जा सकता है। इसी के साथ बैंक कर्मचारियों को उनके कार्य की आवश्यकता के अनुसार ही सूचना-तंत्र तक नियंत्रण की जानी चाहिए।

- **साइबर धोखाधड़ी की रोकथाम**

बैंकों की एक महत्वपूर्ण जिम्मेदारी साइबर धोखाधड़ी की रोकथाम तथा ग्राहकों में जागरूकता उत्पन्न करना भी है। अनेक साइबर अपराधों में अपराधी ग्राहकों को छलपूर्ण संदेश, दूरभाष, इलेक्ट्रॉनिक डाक अथवा अन्य माध्यमों से भ्रमित करके गोपनीय बैंकिंग जानकारी प्राप्त करने का प्रयास करते हैं। बैंक ग्राहकों को नियमित रूप से यह जानकारी प्रदान कर सकते हैं कि वे अपने संकेत-पद, एक बार उपयोग होने वाले संकेतांक, व्यक्तिगत पहचान संबंधी विवरण तथा अन्य गोपनीय जानकारी किसी अनधिकृत व्यक्ति के साथ साझा न करें।

- **साइबर घटनाओं की पहचान**

साइबर घटनाओं की पहचान की प्रतिक्रिया और पुनर्प्राप्ति के क्षेत्र में भी बैंकों की महत्वपूर्ण भूमिका है। साइबर आक्रमण होने की स्थिति में बैंक के पास पूर्वनिर्धारित प्रतिक्रिया व्यवस्था होनी चाहिए जिससे प्रभावित प्रणाली की पहचान, जोखिम को सीमित करने, आवश्यक सेवाओं को सुरक्षित रखने तथा सामान्य बैंकिंग कार्यों को पुनः शीघ्र स्थापित करने में सहायता मिले। नियमित रूप से आँकड़ों का सुरक्षित प्रतिरक्षण तथा आपातकालीन पुनर्स्थापना व्यवस्था विकसित करना भी बैंकिंग सेवाओं की निरंतरता के लिए आवश्यक है।

साइबर सुरक्षा संचालन में केंद्र की भूमिका

वर्तमान डिजिटल युग में बैंकिंग एवं वित्तीय संस्थानों की सूचना-प्रौद्योगिकी प्रणालियाँ निरंतर साइबर खतरों के संपर्क में रहती हैं। साइबर अपराधों की बढ़ती जटिलता, विभिन्न प्रकार के दुर्भावनापूर्ण सॉफ्टवेयर, छलपूर्ण गतिविधियों, अनधिकृत प्रवेश तथा आँकड़ों की चोरी जैसी घटनाओं को देखते हुए ऐसी सुरक्षा व्यवस्था आवश्यक है जो सूचना-तंत्र की निरंतर निगरानी कर सके और संभावित खतरों की समय रहते उनकी पहचान करके उचित कार्रवाई कर सके। इस संदर्भ में साइबर सुरक्षा संचालन केंद्र (SOC) की भूमिका अधिक महत्वपूर्ण हो जाती है। यह केंद्र किसी संस्था के सूचना-तंत्र, नेटवर्क, उपकरणों तथा सुरक्षा प्रणालियों से प्राप्त गतिविधियों की निरंतर निगरानी और विश्लेषण करने वाली एक संगठित सुरक्षा व्यवस्था है। साइबर सुरक्षा संचालन केंद्र का प्रमुख उद्देश्य साइबर खतरों की शीघ्र पहचान कर के उनका विश्लेषण तथा उनके प्रति समयबद्ध प्रतिक्रिया सुनिश्चित करना है। यह केंद्र विभिन्न सूचना-तंत्रों और सुरक्षा उपकरणों से प्राप्त घटनाओं एवं संकेतों का निरंतर निरीक्षण करता है। यदि किसी प्रणाली में असामान्य गतिविधि दिखाई देती है तो उसका विश्लेषण करके यह निर्धारित करने का प्रयास किया जाता है कि वह सामान्य गतिविधि है अथवा संभावित साइबर सुरक्षा घटना। इस प्रकार संभावित खतरे की प्रारंभिक अवस्था में पहचान करके उसके व्यापक प्रभाव को कम करने में सहायता मिलती है।

- **सूचना-तंत्र की निरंतर निगरानी**

साइबर सुरक्षा संचालन केंद्र की प्रमुख भूमिका बैंक के नेटवर्क, सर्वर, अनुप्रयोगों, सुरक्षा उपकरणों तथा अन्य डिजिटल संसाधनों की निरंतर निगरानी करना है। बैंकिंग व्यवस्था में बड़ी संख्या में प्रतिदिन वित्तीय लेन-देन होते हैं। ऐसी स्थिति में किसी असामान्य गतिविधि को शीघ्र पहचानना अत्यंत आवश्यक है। निरंतर निगरानी के माध्यम से संदिग्ध गतिविधियों का पता लगाकर आवश्यक सुरक्षा कार्रवाई की जा सकती है।

- **साइबर खतरों की पहचान**

साइबर सुरक्षा संचालन केंद्र विभिन्न स्रोतों से प्राप्त सुरक्षा संबंधी सूचनाओं का विश्लेषण करके संभावित साइबर खतरों की पहचान करता है। किसी खाते में असामान्य प्रवेश, नेटवर्क में संदिग्ध गतिविधि, अनधिकृत प्रणालीगत परिवर्तन अथवा दुर्भावनापूर्ण कार्यक्रम की उपस्थिति जैसे संकेत संभावित साइबर आक्रमण की ओर संकेत कर सकते हैं।

- **सुरक्षा घटनाओं का विश्लेषण**

प्रत्येक संदिग्ध गतिविधि साइबर आक्रमण नहीं होती। इसलिए सुरक्षा संचालन केंद्र का कार्य केवल चेतावनी प्राप्त करना ही नहीं बल्कि उसका विश्लेषण और सत्यापन करना भी है। विभिन्न स्रोतों से प्राप्त सुरक्षा घटनाओं को एक साथ देखकर घटना की प्रकृति, संभावित स्रोत, प्रभाव तथा गंभीरता का आकलन किया जाता है। इससे वास्तविक साइबर खतरे और सामान्य गतिविधि के मध्य अंतर करने में सहायता मिलती है।

- **साइबर आक्रमण के प्रति त्वरित प्रतिक्रिया**

किसी साइबर सुरक्षा घटना की पुष्टि होने पर साइबर सुरक्षा संचालन केंद्र संबंधित सुरक्षा दल के साथ मिलकर त्वरित प्रतिक्रिया की व्यवस्था करता है। आवश्यकता के अनुसार प्रभावित प्रणाली को अलग करना, संदिग्ध गतिविधि को रोकना, संबंधित खातों या अभिगम को अस्थायी रूप से प्रतिबंधित करना तथा सुरक्षित प्रणाली को पुनः स्थापित करना जैसी कार्यवाही की जा सकती है। शीघ्र प्रतिक्रिया से साइबर आक्रमण से होने वाली संभावित वित्तीय एवं परिचालन क्षति को सीमित करने में सहायता मिलती है।

- **साइबर जोखिमों की रोकथाम**

साइबर सुरक्षा संचालन केंद्र केवल घटित घटनाओं पर प्रतिक्रिया देने तक सीमित नहीं रहता है बल्कि संभावित खतरों की पहचान करके भविष्य में होने वाली घटनाओं की रोकथाम में भी योगदान देता है। पूर्व में घटित साइबर घटनाओं, सुरक्षा चेतावनियों और संदिग्ध गतिविधियों का अध्ययन करके सुरक्षा व्यवस्था में आवश्यक सुधार किए जा सकते हैं। इस प्रकार यह केंद्र बैंक की समग्र साइबर सुरक्षा क्षमता को निरंतर सुदृढ़ करने में सहायक होता है।

ग्राहक जागरूकता में बैंकों की भूमिका

वर्तमान डिजिटल युग में बैंकिंग सेवाओं का तीव्र गति से डिजिटलीकरण हुआ है। इंटरनेट बैंकिंग, मोबाइल बैंकिंग, एटीएम, त्वरित भुगतान प्रणाली तथा अन्य इलेक्ट्रॉनिक भुगतान माध्यमों ने बैंकिंग सेवाओं को सरल, तीव्र और सुविधाजनक बनाया है। किंतु डिजिटल बैंकिंग के बढ़ते उपयोग के साथ-साथ ग्राहकों के समक्ष छलपूर्ण संदेश, पहचान की चोरी, अनधिकृत लेन-देन, छलपूर्ण दूरभाष, संदिग्ध संकेतस्थल तथा अन्य साइबर अपराधों का जोखिम भी बढ़ा है। ऐसी परिस्थितियों में ग्राहक जागरूकता साइबर सुरक्षा की एक महत्वपूर्ण कड़ी बन जाती है। ग्राहकों को सुरक्षित डिजिटल बैंकिंग व्यवहार के प्रति जागरूक करने में बैंकों की भूमिका अत्यंत महत्वपूर्ण है।

- **साइबर अपराधों के प्रति जागरूकता**

बैंकों की प्रमुख जिम्मेदारी ग्राहकों को विभिन्न प्रकार के साइबर अपराधों के संबंध में सरल एवं स्पष्ट जानकारी उपलब्ध कराना है। ग्राहकों को छलपूर्ण दूरभाष, छलपूर्ण संदेश, संदिग्ध इलेक्ट्रॉनिक डाक, जाली

संकेतस्थल, पहचान की चोरी तथा अनधिकृत वित्तीय लेन-देन जैसी गतिविधियों के संबंध में जागरूक किया जाना चाहिए। इससे ग्राहक संभावित धोखाधड़ी के संकेतों को समय रहते पहचान सकता है।

- **गोपनीय बैंकिंग जानकारी की सुरक्षा**

बैंकों को ग्राहकों को यह स्पष्ट रूप से समझाना चाहिए कि संकेत-पद एक बार उपयोग होने वाला संकेतांक, व्यक्तिगत पहचान संख्या, कार्ड संबंधी गोपनीय विवरण तथा अन्य संवेदनशील जानकारी किसी अनधिकृत व्यक्ति के साथ साझा नहीं करनी चाहिए। बैंक यह भी स्पष्ट कर सकते हैं कि बैंक के प्रतिनिधि के रूप में स्वयं को प्रस्तुत करने वाला कोई व्यक्ति यदि ऐसी जानकारी माँगता है तो ग्राहक को सावधानी बरतनी चाहिए।

- **सुरक्षित डिजिटल बैंकिंग व्यवहार**

ग्राहकों को सुरक्षित डिजिटल बैंकिंग व्यवहार अपनाने के लिए प्रोत्साहित करना बैंकों की महत्वपूर्ण भूमिका है। ग्राहकों को केवल विश्वसनीय माध्यमों से बैंकिंग सेवाओं का उपयोग करने, अपने उपकरणों एवं अनुप्रयोगों को अद्यतन रखने तथा संदिग्ध संदेशों में दिए गए संकेतस्थल पर प्रवेश न करने जैसी सावधानियों की जानकारी दी जानी चाहिए। इससे डिजिटल बैंकिंग के दौरान होने वाले जोखिमों को कम करने में सहायता मिलती है।

- **नियमित सूचना एवं चेतावनी संदेश**

बैंक समय-समय पर अपने ग्राहकों को साइबर सुरक्षा संबंधी चेतावनी संदेश भेज सकते हैं। इन संदेशों के माध्यम से ग्राहकों को नवीन साइबर धोखाधड़ी की विधियों तथा उनसे बचाव के उपायों की जानकारी दी जा सकती है। नियमित सूचना-प्रसार से ग्राहकों में साइबर सुरक्षा के प्रति निरंतर सजगता बनी रहती है।

- **वित्तीय लेन-देन की निगरानी के प्रति जागरूकता**

बैंकों को ग्राहकों को अपने खातों में होने वाले लेन-देन की नियमित जाँच करने के लिए प्रेरित करना चाहिए। यदि किसी ग्राहक को ऐसा लेन-देन दिखाई देता है जिसे उसने स्वयं नहीं किया है तो उसे तत्काल बैंक को सूचित करना चाहिए। समय पर सूचना मिलने से बैंक आवश्यक सुरक्षा कार्रवाई कर सकता है तथा संभावित वित्तीय क्षति को सीमित करने में सहायता मिल सकती है।

साइबर आक्रमणों की रोकथाम के लिए बैंक कर्मचारियों का प्रशिक्षण

वर्तमान डिजिटल बैंकिंग व्यवस्था में बैंक कर्मचारियों की भूमिका केवल ग्राहकों को बैंकिंग सेवाएँ उपलब्ध कराने तक सीमित नहीं है बल्कि वे बैंक की सूचना प्रणाली, ग्राहक संबंधी आँकड़ों तथा वित्तीय लेन-देन की सुरक्षा में भी महत्वपूर्ण भूमिका निभाते हैं। साइबर अपराधी अनेक बार कर्मचारियों को छलपूर्ण संदेश, जाली इलेक्ट्रॉनिक डाक, संदिग्ध संकेतस्थल, दुर्भावनापूर्ण सॉफ्टवेयर अथवा अन्य सामाजिक अभियांत्रिकी तकनीकों के माध्यम से लक्ष्य बनाते हैं। ऐसी परिस्थितियों में बैंक कर्मचारियों को साइबर सुरक्षा के प्रति प्रशिक्षित करना साइबर आक्रमणों की रोकथाम की एक महत्वपूर्ण आवश्यकता है।

- **साइबर खतरों की पहचान संबंधी प्रशिक्षण**

बैंक कर्मचारियों को विभिन्न प्रकार के साइबर खतरों की पहचान करने का व्यावहारिक प्रशिक्षण दिया जाना चाहिए। इसमें छलपूर्ण इलेक्ट्रॉनिक डाक, संदिग्ध संदेश, जाली संकेतस्थल, अनधिकृत दूरभाष, पहचान की चोरी, दुर्भावनापूर्ण सॉफ्टवेयर तथा सामाजिक अभियांत्रिकी जैसी गतिविधियों की पहचान प्रमुख है। कर्मचारियों को वास्तविक उदाहरणों के माध्यम से यह समझाया जाना चाहिए कि संदिग्ध गतिविधि दिखाई देने पर उसकी पहचान कैसे की जाए और किस प्रकार उसकी सूचना संबंधित सुरक्षा विभाग को दी जाए।

- **गोपनीय सूचना की सुरक्षा**

बैंक कर्मचारियों के पास ग्राहकों तथा बैंक की महत्वपूर्ण सूचनाएँ होती हैं। इसलिए उन्हें ग्राहक की व्यक्तिगत एवं वित्तीय जानकारी की गोपनीयता बनाए रखने के संबंध में विशेष प्रशिक्षण दिया जाना आवश्यक है।

कर्मचारियों को यह स्पष्ट रूप से बताया जाना चाहिए कि गोपनीय संकेत-पद, व्यक्तिगत पहचान संख्या, प्रमाणीकरण संबंधी जानकारी अथवा अन्य संवेदनशील विवरण अनधिकृत व्यक्ति के साथ साझा नहीं किए जाने चाहिए। इसी प्रकार बैंक के आंतरिक अभिलेखों एवं सूचना-तंत्र का उपयोग केवल अधिकृत कार्यों के लिए किया जाना चाहिए।

- **सुरक्षित संकेत-पद एवं प्रमाणीकरण का प्रशिक्षण**

कर्मचारियों को सुरक्षित संकेत-पद बनाने, उन्हें गोपनीय रखने तथा समय-समय पर आवश्यकतानुसार परिवर्तित करने की जानकारी दी जानी चाहिए। साथ ही बहु-स्तरीय प्रमाणीकरण तथा अन्य सुरक्षा प्रक्रियाओं के उचित उपयोग का प्रशिक्षण दिया जाना चाहिए। कर्मचारियों को यह भी समझना चाहिए कि किसी अन्य कर्मचारी के अभिगम अधिकार या प्रमाणीकरण साधनों का अनधिकृत उपयोग नहीं किया जाना चाहिए।

- **सामाजिक अभियांत्रिकी से बचाव**

साइबर अपराधी कई बार तकनीकी सुरक्षा को सीधे भेदने के बजाय कर्मचारियों को मनोवैज्ञानिक रूप से प्रभावित करके गोपनीय सूचना प्राप्त करने का प्रयास करते हैं। इसे सामाजिक अभियांत्रिकी कहा जाता है। प्रशिक्षण के माध्यम से कर्मचारियों को ऐसे छलपूर्ण व्यवहार की पहचान करना सिखाया जाना चाहिए।

- **संदिग्ध गतिविधियों की सूचना देने का प्रशिक्षण**

किसी कर्मचारी को यदि सूचना-तंत्र में असामान्य गतिविधि, संदिग्ध संदेश, अनधिकृत प्रवेश या अन्य सुरक्षा संबंधी घटना दिखाई देती है तो उसे तत्काल संबंधित अधिकारी या साइबर सुरक्षा दल को सूचित करना चाहिए। इसलिए कर्मचारियों को बैंक की साइबर घटना की सूचना एवं प्रतिक्रिया प्रक्रिया का स्पष्ट ज्ञान होना आवश्यक है।

साइबर सुरक्षा के संबंध में समंक संरक्षण एवं एन्क्रिप्शन

साइबर सुरक्षा के क्षेत्र में समंक संरक्षण एवं एन्क्रिप्शन अत्यंत महत्वपूर्ण सुरक्षा उपाय हैं। वर्तमान डिजिटल युग में बैंकिंग संस्थानों द्वारा ग्राहकों की व्यक्तिगत जानकारी, खाता विवरण, पासवर्ड, लेन-देन संबंधी अभिलेख तथा वित्तीय सूचनाओं का बड़ी मात्रा में डिजिटल रूप से संग्रहण एवं प्रसंस्करण किया जाता है। ऐसी सूचनाओं की अनधिकृत नियंत्रण, चोरी, दुरुपयोग अथवा उनमें अनधिकृत परिवर्तन को रोकने के लिए प्रभावी समंक संरक्षण व्यवस्था आवश्यक है। समंक संरक्षण का मुख्य उद्देश्य सूचना की गोपनीयता, अखंडता और उपलब्धता को बनाए रखना है। इसके अंतर्गत सुरक्षित भंडारण, नियमित बैकअप, अभिगम नियंत्रण, पहचान एवं प्रमाणीकरण, सुरक्षा निगरानी तथा समंक के सुरक्षित हस्तांतरण जैसी व्यवस्थाएँ सम्मिलित होती हैं।

साइबर घटना की स्थिति में बैंक की भूमिका

डिजिटल बैंकिंग के बढ़ते विस्तार के साथ साइबर घटनाओं की संभावना भी बढ़ी है। ऐसी स्थिति में बैंक की भूमिका केवल घटना को रोकने तक सीमित नहीं रहती है बल्कि घटना की पहचान, प्रभाव को सीमित करना, संबंधित पक्षों को सूचना देना, प्रणाली की पुनर्बहाली तथा भविष्य में ऐसी घटनाओं की पुनरावृत्ति रोकना भी बैंक की महत्वपूर्ण जिम्मेदारी होती है। भारतीय रिजर्व बैंक के वर्तमान साइबर सुरक्षा निर्देशों में भी साइबर घटना के प्रति प्रतिक्रिया एवं पुनर्बहाली के लिए स्पष्ट प्रक्रियाएँ, उत्तरदायित्व और संचार व्यवस्था स्थापित करने पर बल दिया गया है।

- **घटना की शीघ्र पहचान एवं मूल्यांकन**

साइबर घटना की शीघ्र पहचान एवं मूल्यांकन बैंक की प्रमुख जिम्मेदारी है। बैंक को अपने सुरक्षा संचालन केंद्र, नेटवर्क निगरानी प्रणालियों, अभिलेखों तथा अन्य सुरक्षा साधनों के माध्यम से असामान्य गतिविधियों की निरंतर निगरानी करनी चाहिए। घटना का पता लगने के बाद उसके स्वरूप, गंभीरता, प्रभावित प्रणालियों तथा संभावित प्रभाव का तत्काल मूल्यांकन किया जाना आवश्यक है। इससे बैंक को यह निर्धारित करने में सहायता मिलती है कि घटना से ग्राहक खातों, भुगतान प्रणालियों अथवा बैंक की महत्वपूर्ण सूचना-प्रौद्योगिकी सेवाओं पर कितना प्रभाव पड़ा है।

• साइबर आक्रमण के प्रभाव को सीमित करना

प्रभावित कंप्यूटर, सर्वर, नेटवर्क अथवा अन्य प्रणालियों को आवश्यकता के अनुसार अलग करके बैंक को आक्रमण के विस्तार को रोकना चाहिए। इसके साथ ही संदिग्ध नियंत्रण को समाप्त करना, प्रभावित खातों अथवा सेवाओं पर आवश्यक सुरक्षा नियंत्रण लागू करना तथा महत्वपूर्ण आँकड़ों और प्रणालियों को सुरक्षित रखना आवश्यक होता है। वर्तमान RBI निर्देशों में प्रभावित उपकरणों या प्रणालियों को पृथक करने तथा आक्रमण के स्तर को नियंत्रित करने के लिए आवश्यक सुरक्षा उपाय करने का उल्लेख है।

- संबंधित संस्थाओं को समय पर सूचना देना साइबर घटना प्रबंधन का महत्वपूर्ण भाग है। बैंक को नियामकीय आवश्यकताओं के अनुसार भारतीय रिजर्व बैंक तथा भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In) को साइबर घटना की सूचना देनी होती है। 2026 के RBI के निर्देशों के अनुसार वाणिज्यिक बैंकों को साइबर घटना की पहचान के छह घंटे के मध्य RBI के DAKSH मंच पर रिपोर्ट करना तथा CERT-In को भी नियमानुसार सूचित करना है।
- ग्राहकों एवं अन्य संबंधित पक्षों के साथ उचित संचार आवश्यक है। यदि साइबर घटना से ग्राहकों के खातों, व्यक्तिगत आँकड़ों अथवा डिजिटल लेन-देन पर प्रभाव पड़ता है तो बैंक को परिस्थितियों के अनुरूप ग्राहकों को आवश्यक सूचना एवं सुरक्षा संबंधी निर्देश उपलब्ध कराने चाहिए। बैंक के निदेशक मंडल एवं वरिष्ठ प्रबंधन को भी घटना की जानकारी देकर आवश्यक निर्णय लेने की व्यवस्था होनी चाहिए। RBI के निर्देशों में साइबर घटना के संबंध में स्पष्ट संचार योजना तथा निदेशक मंडल, वरिष्ठ प्रबंधन और आवश्यकता पड़ने पर ग्राहकों को सूचना देने की व्यवस्था पर बल दिया गया है।

बैंक द्वारा साइबर जोखिम प्रबंधन

बैंकिंग क्षेत्र में सूचना प्रौद्योगिकी और डिजिटल बैंकिंग सेवाओं के बढ़ते उपयोग के साथ साइबर जोखिम प्रबंधन बैंकिंग व्यवस्था का एक अत्यंत महत्वपूर्ण अंग बन गया है। साइबर जोखिम प्रबंधन से आशय ऐसी व्यवस्थित प्रक्रिया से है जिसके माध्यम से बैंक अपने सूचना प्रौद्योगिकी तंत्र, डिजिटल सेवाओं, ग्राहक संबंधी आँकड़ों, भुगतान प्रणालियों तथा अन्य महत्वपूर्ण संसाधनों को साइबर आक्रमण, अनधिकृत नियंत्रण, समंक चोरी, धोखाधड़ी और अन्य डिजिटल खतरों से सुरक्षित रखने के लिए जोखिमों की पहचान, आकलन, नियंत्रण, निगरानी तथा उनके प्रभाव को कम करने की व्यवस्था करता है। भारतीय रिजर्व बैंक ने भी बैंकों के लिए साइबर सुरक्षा एवं साइबर प्रत्यास्थता को सुदृढ़ करने हेतु व्यापक नियामकीय व्यवस्था निर्धारित की है।

बैंक द्वारा साइबर जोखिम प्रबंधन की प्रक्रिया जोखिम की पहचान एवं आकलन से प्रारम्भ होती है। बैंक को अपने सूचना-प्रौद्योगिकी तंत्र, नेटवर्क, समंक-संग्रहण प्रणालियों, डिजिटल भुगतान माध्यमों, मोबाइल बैंकिंग, इंटरनेट बैंकिंग तथा बाहरी सेवा प्रदाताओं से जुड़े संभावित साइबर जोखिमों का नियमित रूप से मूल्यांकन करना आवश्यक है। वर्तमान नियामकीय व्यवस्था के अनुसार बैंक की जोखिम प्रबंधन नीति में सूचना-प्रौद्योगिकी तथा साइबर सुरक्षा से संबंधित जोखिमों को सम्मिलित किया जाना तथा उनका नियमित पुनरावलोकन किया जाना अपेक्षित है।

बैंकिंग क्षेत्र में साइबर सुरक्षा की प्रमुख चुनौतियाँ

वर्तमान समय में बैंकिंग क्षेत्र में सूचना एवं संचार प्रौद्योगिकी का तीव्र विस्तार हुआ है। इंटरनेट बैंकिंग, मोबाइल बैंकिंग, डिजिटल भुगतान तथा अन्य इलेक्ट्रॉनिक बैंकिंग सेवाओं ने बैंकिंग व्यवस्था को अधिक तीव्र एवं सुविधाजनक बनाया है। इसके साथ ही बैंकिंग संस्थाएँ साइबर आक्रमणों के लिए अधिक संवेदनशील भी हुई हैं। भारतीय रिजर्व बैंक ने समय-समय पर यह रेखांकित किया है कि साइबर घटनाओं की संख्या, आवृत्ति और प्रभाव में वृद्धि के कारण बैंकों के लिए निरंतर साइबर सुरक्षा एवं साइबर प्रत्यास्थता बनाए रखना आवश्यक है। शोध-पत्र की दृष्टि से बैंकिंग क्षेत्र में साइबर सुरक्षा की प्रमुख चुनौतियों को निम्नलिखित रूप में स्पष्ट किया जा सकता है।

- **साइबर आक्रमणों की बढ़ती जटिलता**

बैंकिंग क्षेत्र के समक्ष सबसे प्रमुख चुनौती साइबर आक्रमणों की निरंतर बदलती प्रकृति है। साइबर अपराधी नई तकनीकों का उपयोग करके बैंक की सूचना-प्रणाली, नेटवर्क और डिजिटल सेवाओं को लक्ष्य बनाते हैं। दुर्भावनापूर्ण सॉफ्टवेयर, फ़िशिंग के लिए ऑकड़ों को बंधक बनाना, सेवा-अस्वीकार आक्रमण, भ्रामक संदेश, पहचान की चोरी तथा अन्य प्रकार के आक्रमण बैंकिंग संस्थानों की सुरक्षा को प्रभावित कर सकते हैं। भारतीय रिजर्व बैंक ने भी बैंकों को उभरते साइबर खतरों के अनुरूप अपनी नीतियों, प्रक्रियाओं और प्रौद्योगिकी में निरंतर सुधार करने की आवश्यकता पर बल दिया है।

- **ग्राहक संबंधी संवेदनशील ऑकड़ों की सुरक्षा**

ग्राहकों की सूचनाओं की अनधिकृत नियंत्रण, चोरी अथवा दुरुपयोग से ग्राहक की वित्तीय सुरक्षा तथा गोपनीयता प्रभावित हो सकती है। इसलिए ऑकड़ों की गोपनीयता, अखंडता और उपलब्धता सुनिश्चित करना बैंकिंग संस्थानों के लिए एक महत्वपूर्ण चुनौती है। तत्प के साइबर सुरक्षा ढाँचे में ग्राहक सूचना की सुरक्षा को विशेष महत्व दिया गया है, चाहे ऑकड़े बैंक के भीतर संग्रहीत हों या किसी तृतीय-पक्ष सेवा प्रदाता के पास हों।

- **डिजिटल बैंकिंग एवं भुगतान संबंधी जोखिम**

ग्राहकों को भ्रामक संदेश, नकली दूरभाष, जालसाजीपूर्ण वेबसाइट तथा अन्य माध्यमों से प्रभावित करके गोपनीय जानकारी प्राप्त करने का प्रयास किया जाता है। इस प्रकार डिजिटल लेन-देन की सुरक्षा बनाए रखना बैंकों के लिए निरंतर चुनौती है।

- **मानवीय त्रुटि एवं जागरूकता का अभाव**

साइबर सुरक्षा केवल तकनीकी साधनों पर निर्भर नहीं करती। बैंक कर्मचारियों या ग्राहकों की असावधानी भी साइबर जोखिम का कारण बन सकती है। संदिग्ध संदेशों पर प्रतिक्रिया देना, असुरक्षित कूटशब्द का प्रयोग करना अथवा निर्धारित सुरक्षा प्रक्रियाओं का पालन न करना बैंक की सुरक्षा को प्रभावित कर सकता है। इसलिए कर्मचारियों के नियमित प्रशिक्षण तथा ग्राहकों में साइबर सुरक्षा के प्रति जागरूकता उत्पन्न करना आवश्यक है।

वैचारिक मॉडल (Conceptual Model)

इस शोध के लिए निम्न वैचारिक मॉडल प्रस्तावित किया जा सकता है:

- तकनीकी सुरक्षा
- साइबर जोखिम प्रबंधन
- साइबर निगरानी एवं घटना-प्रतिक्रिया
- ग्राहक एवं कर्मचारी जागरूकता
- नियामकीय अनुपालन
- सुदृढ़ बैंकिंग साइबर सुरक्षा
- ग्राहक विश्वास एवं डिजिटल बैंकिंग सुरक्षा

इस मॉडल में यह माना जाता है कि तकनीकी सुरक्षा, मानव जागरूकता, जोखिम प्रबंधन तथा नियामकीय अनुपालन संयुक्त रूप से बैंक की साइबर सुरक्षा क्षमता को प्रभावित करते हैं।

निष्कर्ष

डिजिटल बैंकिंग के तीव्र विस्तार के वर्तमान दौर में साइबर सुरक्षा बैंकिंग क्षेत्र की अनिवार्य आवश्यकता बन चुकी है। बैंक केवल वित्तीय मध्यस्थ के रूप में कार्य नहीं करते, बल्कि वे ग्राहकों की वित्तीय एवं व्यक्तिगत सूचनाओं के संरक्षक भी हैं। इसलिए साइबर सुरक्षा को बैंक की मूलभूत संस्थागत जिम्मेदारी के रूप में देखा

जाना चाहिए। बैंकों द्वारा उन्नत तकनीकी सुरक्षा, बहु कारक प्रमाणीकरण, साइबर निगरानी, कृत्रिम बुद्धिमत्ता, समंक एन्क्रिप्शन, साइबर जोखिम प्रबंधन, कर्मचारी प्रशिक्षण तथा ग्राहक जागरूकता को एकीकृत रूप से अपनाया जाना आवश्यक है। साथ ही बैंकिंग संस्थानों को भारतीय रिजर्व बैंक तथा CERT-In जैसे संस्थानों द्वारा निर्धारित सुरक्षा आवश्यकताओं एवं दिशा-निर्देशों का प्रभावी अनुपालन करना चाहिए। RBI के साइबर सुरक्षा ढाँचे में बोर्ड स्तरीय भागीदारी और सुरक्षा घटनाओं की प्रभावी निगरानी जैसे उपायों पर विशेष बल दिया गया है।

अतः यह निष्कर्ष निकाला जा सकता है कि साइबर सुरक्षा केवल सूचना-प्रौद्योगिकी विभाग की जिम्मेदारी नहीं है बल्कि यह बैंक के प्रबंधन, कर्मचारियों, ग्राहकों, प्रौद्योगिकी प्रदाताओं तथा नियामकीय संस्थाओं की सामूहिक जिम्मेदारी है। एक समन्वित, सक्रिय एवं जोखिम-आधारित साइबर सुरक्षा व्यवस्था ही सुरक्षित, विश्वसनीय और सुदृढ़ डिजिटल बैंकिंग प्रणाली का आधार बन सकती है।

शोध अंतराल (Research Gape)

वर्तमान डिजिटल युग में बैंकिंग सेवाओं का तीव्र डिजिटलीकरण हुआ है। इंटरनेट बैंकिंग, मोबाइल बैंकिंग, एटीएम, यूपीआई तथा अन्य डिजिटल भुगतान प्रणालियों के विस्तार ने बैंकिंग को अधिक सुविधाजनक बनाया है। इसके विपरीत साइबर धोखाधड़ी, फिशिंग, पहचान की चोरी, समंक चोरी, मैलवेयर तथा अनधिकृत लेन-देन जैसी चुनौतियाँ भी बढ़ी हैं। इस संदर्भ में बैंकों की साइबर सुरक्षा व्यवस्था का अध्ययन अत्यंत महत्वपूर्ण हो जाता है। इस विषय से संबंधित पूर्व अध्ययनों का अवलोकन करने पर निम्नलिखित शोध-अंतराल दिखाई देते हैं।

- **बैंक की भूमिका पर समग्र अध्ययन का अभाव:** अनेक अध्ययनों में साइबर अपराधों के प्रकार, डिजिटल बैंकिंग के जोखिम अथवा ग्राहकों की साइबर जागरूकता पर अलग-अलग चर्चा की गई है। किंतु साइबर सुरक्षा को सुदृढ़ करने में बैंक की समग्र भूमिका तकनीकी सुरक्षा, कर्मचारी प्रशिक्षण, ग्राहक जागरूकता, जोखिम प्रबंधन तथा घटना प्रतिक्रिया का एकीकृत अध्ययन अपेक्षाकृत कम दिखाई देता है।
- **ग्राहक और बैंक के मध्य साझा उत्तरदायित्व का सीमित अध्ययन:** साइबर सुरक्षा केवल बैंक की तकनीकी व्यवस्था पर निर्भर नहीं करती है जबकि ग्राहक की सावधानी, पासवर्ड सुरक्षा, ओटीपी की गोपनीयता और संदिग्ध संदेशों की पहचान भी महत्वपूर्ण हैं। फिर भी बैंक और ग्राहक के मध्य साइबर सुरक्षा के साझा उत्तरदायित्व को लेकर पर्याप्त समग्र अध्ययन की आवश्यकता है।
- **तकनीकी उपायों की प्रभावशीलता का मूल्यांकन आवश्यक:** बैंक बहु-स्तरीय प्रमाणीकरण, कृत्रिम बुद्धिमत्ता, व्यवहार आधारित निगरानी, एन्क्रिप्शन तथा संदिग्ध लेन-देन की पहचान जैसी तकनीकों का प्रयोग करते हैं। शोध में यह जानना आवश्यक है कि ये उपाय वास्तविक साइबर जोखिमों को कम करने में कितने प्रभावी हैं तथा इनके कार्यान्वयन में कौन-कौन सी व्यावहारिक कठिनाइयाँ आती हैं।
- **मानवीय पक्ष पर अपेक्षाकृत कम ध्यान:** साइबर सुरक्षा में तकनीक के साथ-साथ बैंक कर्मचारियों और ग्राहकों का व्यवहार भी महत्वपूर्ण है। कर्मचारियों की साइबर जागरूकता, प्रशिक्षण, सुरक्षा संबंधी कार्यप्रणाली तथा ग्राहकों की डिजिटल साक्षरता के बीच संबंध का पर्याप्त अध्ययन किया जाना आवश्यक है।
- **ग्रामीण और शहरी क्षेत्रों के मध्य अंतर का अध्ययन:** डिजिटल बैंकिंग का विस्तार ग्रामीण क्षेत्रों तक हो रहा है लेकिन ग्रामीण और शहरी ग्राहकों में डिजिटल साक्षरता, साइबर जागरूकता तथा बैंकिंग सुविधाओं के उपयोग में अंतर हो सकता है। इसलिए विभिन्न क्षेत्रों के ग्राहकों के संदर्भ में बैंकों की साइबर सुरक्षा भूमिका का तुलनात्मक अध्ययन एक महत्वपूर्ण शोध-अंतराल है।

- **साइबर घटनाओं के बाद बैंक की प्रतिक्रिया पर सीमित अध्ययन:** साइबर धोखाधड़ी की रोकथाम के साथ-साथ घटना घटित होने के बाद बैंक कितनी शीघ्रता से शिकायत दर्ज करता है, खाते को सुरक्षित करता है, ग्राहक को सहायता देता है और घटना से सीख लेकर सुरक्षा व्यवस्था में सुधार करता है, इस घटना-प्रतिक्रिया व्यवस्था का अध्ययन भी आवश्यक है।

भविष्य की संभावनाएँ (Use in Future)

शोध-विषय: "साइबर सुरक्षा को सुदृढ़ करने में बैंकों की भूमिका: एक अध्ययन"

भविष्य में बैंकिंग क्षेत्र में डिजिटल तकनीकों का विस्तार और अधिक तीव्र होने की संभावना है। कृत्रिम बुद्धिमत्ता, मशीन अधिगम, क्लाउड तकनीक, जैवमितीय प्रमाणीकरण तथा डिजिटल भुगतान प्रणालियों के बढ़ते प्रयोग के साथ साइबर सुरक्षा की चुनौतियाँ भी अधिक जटिल हो सकती हैं। अतः बैंकों की भूमिका केवल साइबर अपराधों की रोकथाम तक सीमित न रहकर एक व्यापक और सक्रिय सुरक्षा व्यवस्था विकसित करने की होगी। इस शोध-विषय के संदर्भ में भविष्य की प्रमुख संभावनाएँ निम्नलिखित हैं:-

- **कृत्रिम बुद्धिमत्ता का बढ़ता प्रयोग:** भविष्य में बैंक कृत्रिम बुद्धिमत्ता और मशीन अधिगम के माध्यम से संदिग्ध लेन-देन तथा असामान्य गतिविधियों की पहचान अधिक प्रभावी ढंग से कर सकेंगे। इससे साइबर धोखाधड़ी की रोकथाम और त्वरित कार्रवाई में सहायता मिलेगी।
- **उन्नत प्रमाणीकरण व्यवस्था:** भविष्य में पारंपरिक पासवर्ड और एकबारगी पासवर्ड के साथ जैवमितीय पहचान, व्यवहार-आधारित प्रमाणीकरण तथा बहु-स्तरीय प्रमाणीकरण का प्रयोग बढ़ सकता है। इससे अनधिकृत व्यक्तियों द्वारा बैंक खातों तक नियंत्रण प्राप्त करना कठिन होगा।
- **ग्राहक साइबर-जागरूकता में वृद्धि:** बैंक भविष्य में ग्राहकों को फिशिंग, संदिग्ध संदेशों, नकली बैंकिंग अनुप्रयोगों और ऑनलाइन धोखाधड़ी के प्रति अधिक जागरूक बनाने के लिए नियमित प्रशिक्षण एवं जागरूकता कार्यक्रम चला सकते हैं। इससे बैंक और ग्राहक दोनों की संयुक्त सुरक्षा व्यवस्था मजबूत होगी।
- **साइबर सुरक्षा में निवेश में वृद्धि:** साइबर खतरों के बढ़ते स्वरूप को देखते हुए बैंक आधुनिक सुरक्षा प्रणालियों, सुरक्षित सर्वर, समंक संरक्षण, निरंतर निगरानी तथा प्रशिक्षित साइबर सुरक्षा विशेषज्ञों में अधिक निवेश कर सकते हैं।
- **साइबर अपराध की त्वरित पहचान और प्रतिक्रिया:** भविष्य में बैंकों के लिए ऐसी प्रणालियाँ विकसित करना महत्वपूर्ण होगा, जो साइबर हमले या संदिग्ध लेन-देन की पहचान तत्काल कर सकें और आवश्यक सुरक्षा कार्रवाई शीघ्र आरंभ कर सकें।
- **बैंकों और सरकारी संस्थाओं के बीच सहयोग:** साइबर अपराध की प्रकृति व्यापक होने के कारण भविष्य में बैंक, नियामक संस्थाएँ, कानून-प्रवर्तन एजेंसियाँ तथा प्रौद्योगिकी संस्थाएँ आपसी समन्वय से साइबर सुरक्षा व्यवस्था को अधिक मजबूत कर सकती हैं।
- **ग्रामीण एवं कम डिजिटल-साक्षर ग्राहकों पर विशेष ध्यान:** भविष्य के अध्ययनों में ग्रामीण क्षेत्रों तथा कम डिजिटल-साक्षर ग्राहकों की साइबर सुरक्षा आवश्यकताओं पर विशेष ध्यान दिया जा सकता है। इससे डिजिटल बैंकिंग का सुरक्षित और समावेशी विस्तार संभव होगा।

संदर्भ ग्रन्थ सूची

1. National Institute of Standards and Technology. (2024). The NIST Cyber Security Framework (CSF) 2.0.
2. National Institute of Standards and Technology. (2024). NIST Cyber Security Framework 2.0: Resource & Overview Guide.

- 68 International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASS) July-September(III), 2026
3. Reserve Bank of India. Cyber Security Framework in Banks: Baseline Cyber Security and Resilience Requirements.
 4. Indian Computer Emergency Response Team. Cyber Security advisories and incident response guidance.
 5. Indian Computer Emergency Response Team. (2026). Digital Threat Report 2025–26.
 6. Official website of RBI (https://www.rbi.org.in/?utm_source=chatgpt.com) [CERT-In](https://www.cert-in.org.in/?utm_source=chatgpt.com) [NIST Cyber security Framework](https://www.nist.gov/cyberframework?utm_source=chatgpt.com)
 7. Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2(1), 4-27.
 8. Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behaviour, 48, 51-61. DOI: 10.1016/j.chb.2015.01.039.
 9. Broadhurst, R., & Grabosky, P. (2005). Cyber-crime: The Challenge in Asia. Hong Kong University Press.
 10. Shackleford, D. (2015). Cyber Threat Intelligence: How to Get Ahead of Cybercrime. SANS Institute. Retrieved from <https://www.sans.org/reading-room/whitepapers/threats/cyber-threat-intelligence-get-ahead-cybercrime-36362>

