Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:7(1), July 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

डिजिटल बैंकिंग के युग में साइबर सुरक्षा : भारतीय परिप्रेक्ष्य में चुनौतियाँ और समाधान

❖ **Dr.Gaganpreet Singh Saini[1]**
Assistant Professor, Department of Commerce
Government Degree College, Gururabanj - 263623 (Almora)
Email address: sdrgaganpreet@gmail.com
❖ **Dr. Manpreet Singh[2]**
Assistant Professor, Department of Commerce
Government Degree college, Bhikiyasain - 263667 (Almora)
Email: drmanpreetsinghsaini@gmail.com

सारांश

21वीं सदी के तीसरे दशक में भारत ने डिजिटल परिवर्तन के क्षेत्र में उल्लेखनीय प्रगति की है, जिसमें बैंकिंग क्षेत्र अग्रणी भूमिका निभा रहा है। पारंपरिक बैंकिंग प्रणाली, जो कभी कागजी दस्तावेजों, सीमित शाखाओं और धीमी प्रक्रियाओं पर आधारित थी, आज डिजिटल प्लेटफॉर्म, मोबाइल एप्लिकेशन और क्लाउड–आधारित सेवाओं के माध्यम से संचालित हो रही है। यूनिफाइड पेमेंट्स इंटरफेस (UPI), इंटरनेट बैंकिंग, मोबाइल वॉलेट और डिजिटल भुगतान प्रणालियों ने न केवल बैंकिंग सेवाओं को सरल और सुलभ बनाया है बल्कि वित्तीय समावेशन को भी नई दिशा प्रदान की है।

हालांकि, इस तीव्र डिजिटलीकरण के साथ साइबर सुरक्षा के खतरे भी तेजी से बढ़े हैं। साइबर हमले अब केवल तकनीकी समस्या तक सीमित नहीं हैं बल्कि वे आर्थिक, सामाजिक और मनोवैज्ञानिक स्तर पर गहरा प्रभाव डालते हैं। बैंकिंग क्षेत्र में साइबर अपराधों के कारण न केवल ग्राहकों की वित्तीय सुरक्षा खतरे में पड़ती है अपितु बैंकिंग संस्थानों की विश्वसनीयता और देश की वित्तीय स्थिरता भी प्रभावित होती है। यही कारण है इस मुद्दे पर अध्ययन समय की प्रासंगिकता बन गयी है। विषय की इसी प्रासंगिकता के कारण प्रस्तुत शोध पत्र विषय का चयन किया गया है।

यह शोध पत्र भारतीय बैंकिंग क्षेत्र में उभरते साइबर खतरों का विश्लेषण करता है तथा उनके प्रभावों का अध्ययन करता है। इसके साथ ही, यह अध्ययन ग्राहक विश्वास, वित्तीय स्थिरता और नियामक ढांचे के बीच संबंधों को समझने का प्रयास करता है। शोध का उद्देश्य यह स्पष्ट करना है कि साइबर सुरक्षा केवल तकनीकी उपायों तक सीमित नहीं है। यह एक व्यापक सामाजिक और आर्थिक चुनौती बन है, जिसके समाधान के लिए बहुआयामी दृष्टिकोण आवश्यक है।

शब्द–कुंजी साइबर सुरक्षा, डिजिटल बैंकिंग, UPI, ग्राहक विश्वास, वित्तीय स्थिरता, फिशिंग, डेटा संरक्षण।

प्रस्तावना

वर्तमान समय में डिजिटल तकनीक ने मानव जीवन के लगभग हर क्षेत्र को प्रभावित किया है। बैंकिंग क्षेत्र जो मानव समाज की विविध जीवनगत परिस्थितियों में महत्वपूर्ण सहायक की भूमिका अदा करती है, में परिवर्तन इसी का एक प्रमुख उदाहरण है। भारत में बैंकिंग प्रणाली ने पिछले कुछ दशकों में जो परिवर्तन देखा है, वह कुछ समय पूर्व तक अकल्पनीय प्रतीत होती थी। 1980 के दशक में जहाँ बैंकिंग सेवाएँ मुख्यतः मैन्युअल प्रक्रियाओं पर आधारित थीं, वहीं आज यह पूरी तरह डिजिटल नेटवर्क पर निर्भर हो चुकी हैं।

डिजिटल इंडिया अभियान, प्रधानमंत्री जन धन योजना और UPI जैसी पहलों ने न केवल बैंकिंग सेवाओं को सरल बनाया है, बल्कि उन्हें समाज के अंतिम व्यक्ति तक पहुँचाने में भी महत्वपूर्ण भूमिका निभाई है। आज एक ग्रामीण किसान भी अपने मोबाइल फोन के माध्यम से पैसे का लेन–देन कर सकता है, जो पहले संभव नहीं था। लेकिन इसका उपयोग जितना सरल दिखाई देता है, उतना ही चुनौतियों एवं खतरों से भरा है। साइबर सुरक्षा का विचार, उनके लिए निरंतर प्रयास एवं संभावित समस्याओं का आकलन इन्हीं खतरों एवं चुनौतियों की देन है। जैसे–जैसे बैंकिंग सेवाएं ऑनलाइन होती गईं, वैसे–वैसे साइबर अपराधियों के लिए नए अवसर उत्पन्न हुए। पहले जहाँ बैंक डकैती या धोखाधड़ी भौतिक रूप में होती थी, अब वही

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:7(1), July 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

अपराध डिजिटल माध्यमों से होने लगे हैं। साइबर अपराधी अत्यंत परिष्कृत तकनीकों का उपयोग करके ग्राहकों और बैंकों दोनों को निशाना बना रहे हैं। फिशिंग, डेटा चोरी आदि जैसे खतरे अब आम हो गए हैं। इन हमलों का प्रभाव केवल आर्थिक नुकसान तक सीमित नहीं है, बल्कि यह ग्राहकों के मन में भय और असुरक्षा की भावना भी उत्पन्न करता है। और यही वह वजह है, जिसके कारण साइबर सुरक्षा का महत्व अत्यंत बढ़ जाता है। यह केवल तकनीकी सुरक्षा का प्रश्न नहीं है, बल्कि यह बैंकिंग प्रणाली की विश्वसनीयता, ग्राहक विश्वास और राष्ट्रीय आर्थिक स्थिरता का आधार बन चुका है। यदि साइबर सुरक्षा में चूक होती है, तो उसका प्रभाव व्यापक हो सकता है, जिससे पूरे वित्तीय तंत्र में अस्थिरता उत्पन्न हो सकती है।

अध्ययन का महत्व

प्रस्तुत अध्ययन वर्तमान समय में अत्यंत प्रासंगिक है क्योंकि डिजिटल बैंकिंग के विस्तार के साथ साइबर खतरों की संख्या और जटिलता दोनों बढ़ी हैं। इस शोध का महत्व निम्नलिखित बिंदुओं के माध्यम से समझा जा सकता है –

1. डिजिटल लेनदेन का तीव्र विस्तार होने के साथ–साथ साइबर अपराधियों के लिए नए अवसर का सृजन भी किया है जिससे समय रहते अवगत होना आवश्यक है।

2. बैंकिंग प्रणाली में ग्राहकों की संवेदनशील जानकारी जैसे बैंक खाता विवरण, आधार संख्या, मोबाइल नंबर और लेनदेन इतिहास संग्रहित होता है। यदि यह डेटा गलत हाथों में चला जाए, तो इसका दुरुपयोग गंभीर परिणाम उत्पन्न कर सकता है। इसलिए डेटा सुरक्षा आज बैंकिंग क्षेत्र की प्राथमिक आवश्यकता बन गई है।

3. साइबर हमले केवल व्यक्तिगत स्तर पर ही नहीं, बल्कि पूरे वित्तीय तंत्र को प्रभावित कर सकते हैं। यदि किसी बड़े बैंक या भुगतान प्रणाली पर हमला होता है, तो इससे व्यापक आर्थिक अस्थिरता उत्पन्न हो सकती है। जिससे आज के युवा वर्ग का अवगत होना महत्वपूर्ण है।

अध्ययन का उद्देश्य

वर्तमान डिजिटल युग में बैंकिंग प्रणाली तेजी से विकसित हो रही है, लेकिन इस विकास के साथ अनेक जोखिम भी जुड़े हुए हैं। ऐसे में यह आवश्यक हो जाता है कि इन जोखिमों की पहचान कर उनके प्रभावों का समुचित अध्ययन किया जाए। इसी आधार पर प्रस्तुत शोध पत्र हेतु निम्नलिखित उद्देश्यों का निर्धारण किया गया है –

1. भारतीय बैंकिंग क्षेत्र में साइबर खतरों की पहचान करना।

2. साइबर हमलों का ग्राहक विश्वास पर प्रभाव का अध्ययन करना।

3. वित्तीय स्थिरता पर साइबर सुरक्षा के प्रभाव को समझना।

4. नियामक ढांचे और सरकारी उपायों का मूल्यांकन करना।

5. भविष्य के लिए सुझाव प्रस्तुत करना।

शोध प्रविधि

प्रस्तुत शोध पत्र द्वितीयक तथ्यों पर आधारित एक मौलिक अध्ययन है। इस अध्ययन के सफल सम्पादन हेतु विभिन्न पुस्तकों, शोध पत्रों एवं वेबसाइट की सहायता ली गयी है। उक्त स्रोतों के माध्यम से संकलित तथ्यों का विश्लेषण कर निष्कर्ष का आलेखन किया गया है। साथ ही उक्त प्रक्रिया के दौरान प्राप्त अनुभव के आधार पर सुझावों का भी आलेखन किया गया है।

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:7(1), July 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

तथ्यों का विश्लेषण

डिजिटल बैंकिंग के विकास ने भारतीय वित्तीय प्रणाली को अभूतपूर्व गति प्रदान की है। भारतीय रिजर्व बैंक तथा राष्ट्रीय भुगतान निगम (NPCI) के आँकड़े दर्शाते हैं कि पिछले कुछ वर्षों में डिजिटल लेन–देन की संख्या में निरंतर वृद्धि हुई है। विशेष रूप से यूनिफाइड पेमेंट्स इंटरफेस (UPI) ने भुगतान प्रणाली में क्रांतिकारी परिवर्तन किया है। आज भारत विश्व के सबसे बड़े डिजिटल भुगतान बाजारों में शामिल हो चुका है। डिजिटल भुगतान की यह बढ़ती प्रवृत्ति एक ओर वित्तीय समावेशन को बढ़ावा दे रही है, वहीं दूसरी ओर साइबर अपराधियों के लिए नए अवसर भी उत्पन्न कर रही है। डिजिटल बैंकिंग के बढ़ते उपयोग के साथ साइबर सुरक्षा संबंधी चुनौतियाँ भी अधिक जटिल और व्यापक होती जा रही हैं।

भारतीय बैंकिंग क्षेत्र में साइबर खतरों का स्वरूप बहुआयामी है। फिशिंग, विशिंग, स्मिशिंग, मैलवेयर तथा पहचान चोरी जैसे साइबर अपराध वर्तमान समय में प्रमुख चुनौतियों के रूप में सामने आए हैं। फिशिंग के अंतर्गत अपराधी नकली ई–मेल, वेबसाइट अथवा संदेशों के माध्यम से ग्राहकों की गोपनीय जानकारी प्राप्त करने का प्रयास करते हैं। इसी प्रकार विशिंग में फोन कॉल के माध्यम से तथा स्मिशिंग में एसएमएस के माध्यम से ग्राहकों को धोखा दिया जाता है। इन तकनीकों का उद्देश्य ग्राहकों की बैंकिंग जानकारी, ओटीपी अथवा पासवर्ड प्राप्त करना होता है। डिजिटल साक्षरता की कमी तथा तकनीकी जानकारी का अभाव इन अपराधों को और अधिक प्रभावी बना देता है।

भारतीय समाज की विविध सामाजिक–आर्थिक परिस्थितियों का भी साइबर सुरक्षा पर प्रभाव पड़ता है। ग्रामीण क्षेत्रों में डिजिटल बैंकिंग का विस्तार तेजी से हुआ है, किन्तु वहाँ डिजिटल साक्षरता का स्तर अपेक्षाकृत कम है। अनेक उपयोगकर्ता मोबाइल बैंकिंग और ऑनलाइन भुगतान सेवाओं का उपयोग तो कर रहे हैं, लेकिन साइबर सुरक्षा के मूलभूत सिद्धांतों से परिचित नहीं हैं। परिणामस्वरूप वे आसानी से साइबर अपराधियों का शिकार बन जाते हैं। इससे स्पष्ट होता है कि साइबर सुरक्षा केवल तकनीकी विषय नहीं है, बल्कि इसका गहरा संबंध शिक्षा, सामाजिक जागरूकता और डिजिटल साक्षरता से भी है।

साइबर हमलों का सबसे प्रत्यक्ष प्रभाव ग्राहकों के विश्वास पर पड़ता है। बैंकिंग प्रणाली का आधार विश्वास है। ग्राहक यह मानकर अपनी धनराशि बैंक में जमा करते हैं कि उनकी पूँजी और व्यक्तिगत जानकारी सुरक्षित रहेगी। जब किसी बैंक अथवा भुगतान प्रणाली से संबंधित साइबर हमले की घटना सामने आती है, तब ग्राहकों में असुरक्षा की भावना उत्पन्न होती है। अनेक बार ग्राहक ऑनलाइन बैंकिंग सेवाओं के उपयोग से बचने लगते हैं अथवा डिजिटल लेन–देन के प्रति संदेहपूर्ण दृष्टिकोण अपनाते हैं। इससे डिजिटल बैंकिंग को बढ़ावा देने के सरकारी प्रयासों पर भी प्रतिकूल प्रभाव पड़ सकता है। ग्राहक विश्वास में कमी बैंकिंग संस्थानों की प्रतिष्ठा और विश्वसनीयता को भी प्रभावित करती है।

साइबर सुरक्षा का संबंध वित्तीय स्थिरता से भी अत्यंत महत्वपूर्ण है। आधुनिक बैंकिंग प्रणाली सूचना प्रौद्योगिकी पर आधारित है। यदि किसी बड़े बैंक, भुगतान नेटवर्क अथवा वित्तीय संस्था पर व्यापक साइबर हमला होता है, तो इसका प्रभाव केवल उस संस्था तक सीमित नहीं रहता बल्कि पूरे वित्तीय तंत्र पर पड़ सकता है। उदाहरण के लिए यदि किसी बैंक के सर्वर पर रैनसमवेयर हमला हो जाए और बैंकिंग सेवाएँ बाधित हो जाएँ, तो लाखों ग्राहकों के लेन–देन प्रभावित हो सकते हैं। इससे आर्थिक गतिविधियों में व्यवधान उत्पन्न हो सकता है। वित्तीय बाजारों में अनिश्चितता और अस्थिरता बढ़ सकती है। इसलिए साइबर सुरक्षा को आज राष्ट्रीय आर्थिक सुरक्षा के एक महत्वपूर्ण घटक के रूप में देखा जाने लगा है।

भारत सरकार तथा भारतीय रिजर्व बैंक ने साइबर सुरक्षा को सुदृढ़ बनाने के लिए अनेक कदम उठाए हैं। भारतीय रिजर्व बैंक द्वारा बैंकों के लिए साइबर सुरक्षा संबंधी दिशा–निर्देश जारी किए गए हैं। इसके अतिरिक्त बहु–स्तरीय प्रमाणीकरण (Multi-Factor Authentication), डेटा एन्क्रिप्शन, साइबर ऑडिट तथा जोखिम प्रबंधन प्रणालियों को बढ़ावा दिया गया है। भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In) तथा भारतीय साइबर अपराध समन्वय केंद्र जैसी संस्थाएँ भी साइबर खतरों से निपटने में महत्वपूर्ण भूमिका निभा रही हैं। हाल के वर्षों में डेटा संरक्षण और गोपनीयता के क्षेत्र में भी नीतिगत सुधार देखने को मिले हैं, जिनका उद्देश्य नागरिकों की व्यक्तिगत जानकारी की सुरक्षा सुनिश्चित करना है।

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:7(1), July 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

हालाँकि नियामक उपायों के बावजूद चुनौतियाँ बनी हुई हैं। साइबर अपराधियों द्वारा नई–नई तकनीकों का उपयोग किया जा रहा है। कृत्रिम बुद्धिमत्ता और मशीन लर्निंग जैसी उन्नत तकनीकों का प्रयोग अब अपराधी भी करने लगे हैं। डीपफेक तकनीक, स्वचालित फिशिंग अभियान तथा उन्नत मैलवेयर साइबर सुरक्षा के लिए नई चुनौतियाँ प्रस्तुत कर रहे हैं। इसके अतिरिक्त बैंकिंग संस्थानों के भीतर कार्यरत कर्मचारियों की लापरवाही अथवा आंतरिक सुरक्षा कमजोरियाँ भी जोखिम को बढ़ा सकती हैं। इसलिए साइबर सुरक्षा को केवल तकनीकी निवेश तक सीमित नहीं रखा जा सकता, बल्कि इसके लिए मानव संसाधन विकास, प्रशिक्षण तथा सतत निगरानी की आवश्यकता है।

उपर्युक्त तथ्यों के विश्लेषण से यह स्पष्ट होता है कि डिजिटल बैंकिंग के क्षेत्र में साइबर सुरक्षा एक बहुआयामी चुनौती है। यह केवल सूचना प्रौद्योगिकी से संबंधित विषय नहीं है, बल्कि इसका संबंध सामाजिक विश्वास, आर्थिक स्थिरता, प्रशासनिक दक्षता और नागरिक जागरूकता से भी है। डिजिटल बैंकिंग के विस्तार के साथ–साथ साइबर सुरक्षा को प्राथमिकता देना अनिवार्य हो गया है। यदि तकनीकी विकास और सुरक्षा उपायों के बीच संतुलन स्थापित नहीं किया गया, तो डिजिटल बैंकिंग की उपलब्धियाँ गंभीर जोखिमों का सामना कर सकती हैं। इसलिए एक समग्र और बहुस्तरीय दृष्टिकोण अपनाना समय की आवश्यकता है।

निष्कर्ष

प्रस्तुत अध्ययन से यह स्पष्ट होता है कि डिजिटल बैंकिंग ने भारतीय वित्तीय व्यवस्था में व्यापक परिवर्तन उत्पन्न किया है। डिजिटल तकनीकों के प्रयोग ने बैंकिंग सेवाओं को अधिक सरल, त्वरित और सुलभ बनाया है। यूनिफाइड पेमेंट्स इंटरफेस (UPI), इंटरनेट बैंकिंग, मोबाइल बैंकिंग तथा डिजिटल वॉलेट जैसी सेवाओं ने वित्तीय लेन–देन को नई गति प्रदान की है। इससे वित्तीय समावेशन को बढ़ावा मिला है और समाज के उन वर्गों तक भी बैंकिंग सेवाएँ पहुँची हैं जो पहले औपचारिक बैंकिंग व्यवस्था से पूर्णतः नहीं जुड़ पाए थे। डिजिटल इंडिया अभियान तथा विभिन्न सरकारी पहलों ने इस परिवर्तन को और अधिक प्रभावशाली बनाया है।

इस अध्ययन से यह भी स्पष्ट होता है कि डिजिटल बैंकिंग के विस्तार के साथ साइबर सुरक्षा संबंधी जोखिमों में भी उल्लेखनीय वृद्धि हुई है। साइबर अपराधियों द्वारा अपनाई जा रही नई तकनीकें और जटिल हमले बैंकिंग क्षेत्र के लिए गंभीर चुनौती बनते जा रहे हैं। फिशिंग, डेटा चोरी, पहचान की चोरी तथा ऑनलाइन धोखाधड़ी जैसी घटनाएँ यह संकेत देती हैं कि केवल तकनीकी प्रगति पर्याप्त नहीं है, बल्कि उसके साथ मजबूत सुरक्षा व्यवस्था भी अनिवार्य है। डिजिटल बैंकिंग का संपूर्ण ढाँचा ग्राहकों के विश्वास पर आधारित है और यदि यह विश्वास कमजोर होता है, तो डिजिटल अर्थव्यवस्था की प्रगति भी प्रभावित हो सकती है।

अध्ययन के दौरान यह तथ्य भी सामने आया कि साइबर सुरक्षा केवल तकनीकी समस्या नहीं है। इसका संबंध सामाजिक, आर्थिक तथा मनोवैज्ञानिक पहलुओं से भी है। अनेक मामलों में साइबर अपराध तकनीकी कमजोरी के कारण नहीं, बल्कि उपयोगकर्ताओं की जागरूकता की कमी के कारण सफल होते हैं। डिजिटल साक्षरता के अभाव में ग्राहक आसानी से फर्जी कॉल, संदेश या ई–मेल के माध्यम से धोखाधड़ी का शिकार हो जाते हैं। ग्रामीण क्षेत्रों और नव–डिजिटल उपयोगकर्ताओं में यह समस्या अपेक्षाकृत अधिक देखने को मिलती है। इसलिए साइबर सुरक्षा के क्षेत्र में मानव व्यवहार और जागरूकता का महत्व तकनीकी उपायों के समान ही है।

वित्तीय स्थिरता के दृष्टिकोण से भी साइबर सुरक्षा का महत्व अत्यंत अधिक है। आधुनिक बैंकिंग प्रणाली सूचना प्रौद्योगिकी नेटवर्क पर आधारित है। यदि किसी बड़े बैंक अथवा भुगतान प्रणाली पर गंभीर साइबर हमला होता है, तो उसका प्रभाव व्यापक आर्थिक गतिविधियों पर पड़ सकता है। इससे बैंकिंग सेवाएँ बाधित हो सकती हैं, ग्राहकों का विश्वास कम हो सकता है और वित्तीय बाजारों में अस्थिरता उत्पन्न हो सकती है। इस प्रकार साइबर सुरक्षा आज राष्ट्रीय आर्थिक सुरक्षा का एक अभिन्न अंग बन चुकी है।

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:7(1), July 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

अध्ययन से यह भी ज्ञात होता है कि भारत सरकार, भारतीय रिजर्व बैंक तथा अन्य नियामक संस्थाओं ने साइबर सुरक्षा को सुदृढ़ बनाने हेतु अनेक महत्वपूर्ण कदम उठाए हैं। बहु–स्तरीय प्रमाणीकरण, साइबर सुरक्षा दिशानिर्देश, डेटा संरक्षण नीतियाँ तथा साइबर अपराध नियंत्रण तंत्र इस दिशा में उल्लेखनीय प्रयास हैं। बावजूद इसके बदलती तकनीक और साइबर अपराधियों की नई रणनीतियों को देखते हुए सुरक्षा उपायों को निरंतर अद्यतन करना आवश्यक है।

निष्कर्षत: कहा जा सकता है कि डिजिटल बैंकिंग का भविष्य साइबर सुरक्षा की प्रभावशीलता पर निर्भर करता है। तकनीकी विकास और सुरक्षा उपायों के मध्य संतुलन स्थापित कर ही एक सुरक्षित, विश्वसनीय और समावेशी डिजिटल बैंकिंग व्यवस्था का निर्माण किया जा सकता है। इसके लिए सरकार, बैंकिंग संस्थान, तकनीकी विशेषज्ञ और ग्राहक सभी की साझी जिम्मेदारी है।

सुझाव

डिजिटल बैंकिंग प्रणाली को अधिक सुरक्षित और विश्वसनीय बनाने की दिशा में निम्नलिखित कदम महत्वपूर्ण हो सकते हैं–

- ❖ साइबर सुरक्षा के प्रति जन–जागरूकता को व्यापक स्तर पर बढ़ाया जाना चाहिए। बैंकों तथा सरकारी संस्थाओं को नियमित रूप से जागरूकता अभियान चलाने चाहिए ताकि ग्राहक फिशिंग, विशिंग, स्मिशिंग और अन्य ऑनलाइन धोखाधड़ी के तरीकों से परिचित हो सकें।
- ❖ डिजिटल साक्षरता कार्यक्रमों का विस्तार विशेष रूप से ग्रामीण क्षेत्रों और वरिष्ठ नागरिकों के लिए किया जाना चाहिए। इससे नए उपयोगकर्ता सुरक्षित डिजिटल व्यवहार अपनाने में सक्षम होंगे।
- ❖ बैंकों को अपने साइबर सुरक्षा ढाँचे को निरंतर अद्यतन करना चाहिए। कृत्रिम बुद्धिमत्ता आधारित सुरक्षा प्रणालियाँ, उन्नत खतरा पहचान तंत्र तथा वास्तविक समय निगरानी प्रणालियाँ विकसित की जानी चाहिए।
- ❖ ग्राहकों के लिए बहु–स्तरीय प्रमाणीकरण (Multi&Factor Authentication) को और अधिक प्रभावी बनाया जाना चाहिए। इससे अनधिकृत पहुँच की संभावना कम होगी।
- ❖ बैंकिंग संस्थानों में कार्यरत कर्मचारियों को नियमित साइबर सुरक्षा प्रशिक्षण प्रदान किया जाना चाहिए। अनेक साइबर घटनाएँ मानवीय त्रुटियों के कारण होती हैं, जिन्हें प्रशिक्षण के माध्यम से कम किया जा सकता है।
- ❖ डेटा संरक्षण कानूनों का कठोरता से अनुपालन सुनिश्चित किया जाना चाहिए। ग्राहकों की व्यक्तिगत और वित्तीय जानकारी को सुरक्षित रखने के लिए मजबूत कानूनी ढाँचे की आवश्यकता है।
- ❖ साइबर अपराधों की रिपोर्टिंग प्रक्रिया को सरल और त्वरित बनाया जाना चाहिए ताकि पीड़ित व्यक्ति षीघ्र सहायता प्राप्त कर सकें और अपराधियों के विरुद्ध समय पर कार्रवाई की जा सके।
- ❖ बैंकों, तकनीकी कंपनियों तथा सरकारी एजेंसियों के बीच समन्वय को और अधिक मजबूत किया जाना चाहिए। साइबर सुरक्षा एक साझा जिम्मेदारी है, जिसके लिए बहु–संस्थागत सहयोग आवष्यक है।
- ❖ षैक्षणिक संस्थानों में डिजिटल सुरक्षा और साइबर जागरूकता से संबंधित पाठ्यक्रमों को बढ़ावा दिया जाना चाहिए ताकि नई पीढ़ी प्रारंभ से ही सुरक्षित डिजिटल व्यवहार सीख सके।
- ❖ साइबर सुरक्षा के क्षेत्र में अनुसंधान और नवाचार को प्रोत्साहित किया जाना चाहिए, जिससे भविश्य की चुनौतियों का प्रभावी समाधान विकसित किया जा सके।

संदर्भ सूची (References)

- ➢ Agarwal, A. (2023). Cyber Security in Digital Banking: Challenges and Opportunities. New Delhi: Sage Publications.
- ➢ Reserve Bank of India. (2024). Report on Trend and Progress of Banking in India. Mumbai: RBI.
- ➢ National Payments Corporation of India. (2024). UPI Product Statistics and Digital Payment Trends. New Delhi: NPCI.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:7(1), July 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

- Ministry of Electronics and Information Technology. (2023). Digital India Annual Report. Government of India.
- CERT-In. (2024). Annual Cyber Security Incident Report. New Delhi: Indian Computer Emergency Response Team.
- Kumar, R., & Sharma, P. (2022). Cyber Threats in Indian Banking Sector: Issues and Challenges. Journal of Banking and Finance, 15(2), 45–58.
- Gupta, S. (2021). Information Security and Digital Banking in India. New Delhi: Atlantic Publishers.
- Reserve Bank of India. (2023). Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices. Mumbai: RBI.
- World Bank. (2023). Digital Financial Inclusion and Cyber Security in Emerging Economies. Washington DC: World Bank.
- United Nations Development Programme. (2022). Digital Transformation and Financial Security: Global Perspectives. New York: UNDP.
- Reserve Bank of India www-rbi-org-in
- National Payments Corporation of India- www-npci-org-in
- Indian Computer Emergency Response Team www-cert&in-org-in
- World Bank www-worldbank-org