Vol 7, Issue 11, 2024 **Impact Factor: 5.355** DOI: https://doi.org/10.31426/ijamsr.2024.7.11.7915

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा खतरे: चुनौतियाँ, प्रभाव और सुरक्षा उपायों का विश्लेषण

राकेश कुमार राय

सहायक प्रोफेसर, भारथी कॉलेज ऑफ एजुकेशन, कंदरी, मांडर, रांची, झारखंड

ईमेल आईडी: rkrai23284@gmail.com

सार:

यह पत्र भारतीय बैंकिंग क्षेत्र के सामने आने वाले साइबर सुरक्षा खतरों के उभरते परिदृश्य की जांच करता है, प्रमुख चुनौतियों, प्रभावों और मौजूदा सुरक्षा उपायों की प्रभावशीलता की पहचान करता है। -2015 और 2024 के बीच प्रकाशित 20 सहकर्मी समीक्षा अध्ययनों की एक व्यवस्थित समीक्षा पर आधारित, यह बड़े पैमाने पर उपभोक्ता सर्वेक्षणों से लेकर केंद्रित संस्थागत आकलन तक के मात्रात्मक निष्कर्षों को संश्लेषित करता है ताकि प्रचलित हमले के वैक्टर (फ़िशिंग, मैलवेयर, रैनसमवेयर), छोटे बैंकों के बीच संसाधन की कमी और लगातार मानवीय कमज़ोरियों को उजागर किया जा सके। विश्लेषण से विनियामक अनुपालन और व्यावहारिक लचीलेपन के बीच महत्वपूर्ण अंतर का पता चलता है, जिसमें उन्नत खतरे का पता लगाने और सक्रिय जोखिम प्रबंधन का अभी भी कम उपयोग किया जाता है। अनुभवजन्य साक्ष्य डिजिटल बैंकिंग प्रदर्शन को बेहतर बनाने में निरंतर निगरानी, पता लगाने और भेद्यता प्रबंधन की महत्वपूर्ण भूमिका को रेखांकित करते हैं, साथ ही यह भी प्रदर्शित करते हैं कि बुनियादी सुरक्षा नियंत्रण अकेले सीमित लाभ देते हैं। पेपर एक बहुस्तरीय साइबर सुरक्षा ढांचे का प्रस्ताव देकर समाप्त होता है जो तकनीकी सुरक्षा, हितधारक शिक्षा और क्रॉससेक्टर सहयोग को एकीकृत करता है। इसमें भारत में टिकाऊ, सुरक्षित डिजिटल बैंकिंग विकास सुनिश्चित करने के लिए सुरक्षा परिचालन क्षमताओं में लक्षित निवेश, तीसरे पक्ष की निगरानी को मजबूत करने और उभरते खतरों पर निरंतर अनुसंधान की सिफारिश की गई है।

कीवर्ड: साइबर सुरक्षा खतरे, बहुस्तरीय -साइबर सुरक्षा ढांचा, भारतीय बैंकिंग क्षेत्र.

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

I. परिचय

पिछले दो दशकों में भारतीय बैंकिंग क्षेत्र में तेजी से बदलाव आया है, जो डिजिटल तकनीकों के व्यापक रूप से अपनाए जाने और तेजी से आपस में जुड़े वित्तीय पारिस्थितिकी तंत्र के कारण हुआ है। कोर बैंकिंग समाधान, इंटरनेट बैंकिंग और मोबाइल बैंकिंग प्लेटफ़ॉर्म के आगमन ने बैंकों को विविध सामाजिक-आर्थिक क्षेत्रों में वित्तीय समावेशन का विस्तार करते हुए कुशल, ग्राहक-केंद्रित सेवाएँ देने में सक्षम बनाया है। 2023 तक, भारत में 900 मिलियन से अधिक सक्रिय डिजिटल बैंकिंग उपयोगकर्ता हैं, जो आधुनिक वित्तीय सेवाओं को आकार देने में प्रौद्योगिकी की महत्वपूर्ण भूमिका को दर्शाता है। हालाँकि, इस डिजिटल प्रसार ने बैंकिंग उद्योग को फ़िशिंग और मैलवेयर हमलों से लेकर उन्नत लगातार खतरों (APT) और रैनसमवेयर तक साइबर सुरक्षा खतरों के व्यापक स्पेक्ट्रम के सामने उजागर किया है। साइबर हमलों की बढ़ती आवृत्ति और परिष्कार भारतीय बैंकिंग संदर्भ में मौजूदा सुरक्षा उपायों की चुनौतियों, प्रभावों और प्रभावकारिता की व्यापक समझ की तत्काल आवश्यकता को उजागर करते हैं। वैश्विक स्तर पर, वित्तीय सेवा क्षेत्र साइबर अपराधियों के लिए एक प्राथमिक लक्ष्य रहा है, क्योंकि बैंकों द्वारा संसाधित उच्च मौद्रिक मूल्य और संवेदनशील डेटा है। सर्विडियो और टेलर (2015) ने सामुदायिक बैंकों के खिलाफ साइबर हमलों की आवृत्ति, दायरे और परिष्कार में क्रमिक वृद्धि देखी, यह देखते हुए कि छोटे संस्थानों में अक्सर मजबूत साइबर सुरक्षा बचाव ***(सर्विडियो और टेलर, 2015) को लागू करने के लिए संसाधनों की कमी होती है***। भारत में, इसी तरह के रुझान सामने आए हैं, सभी आकार के बैंकों ने डेटा उल्लंघन, अनधिकृत लेनदेन और मैलवेयर संक्रमण की घटनाओं की रिपोर्ट की है। भारत में नियामक परिदृश्य इन खतरों के जवाब में विकसित हुआ है, जिसमें भारतीय रिजर्व बैंक (RBI) साइबर सुरक्षा दिशानिर्देश जारी करता है और समय-समय पर भेद्यता आकलन अनिवार्य करता है। फिर भी, तकनीकी नवाचार की गति अक्सर सुरक्षा ढांचे के विकास से आगे निकल जाती है, जिससे महत्वपूर्ण अंतराल पैदा होते हैं जिनका विरोधी फायदा उठा सकते हैं।

प्रदीप (2015) ने इस बात पर जोर दिया कि 1990 के बाद भारत के वित्तीय क्षेत्र के उदारीकरण ने सूचना प्रौद्योगिकी में महत्वपूर्ण निवेश को उत्प्रेरित किया, जिससे मोबाइल वॉलेट, इंटरनेट बैंकिंग और इलेक्ट्रॉनिक फंड ट्रांसफर जैसे इलेक्ट्रॉनिक बैंकिंग चैनलों का प्रसार संभव हुआ ***(प्रदीप, 2015) /*** जबकि इन प्रगति ने परिचालन दक्षता और ग्राहक सुविधा में सुधार किया है, उन्होंने साइबर विरोधियों के लिए हमले की सतह को भी बढ़ाया है। भारत में साइबर अपराध फ़िशिंग, पहचान की चोरी और परिष्कृत मैलवेयर अभियानों सहित विभिन्न रूपों में प्रकट हुआ है, जिसके परिणामस्वरूप पर्याप्त वित्तीय नुकसान और ग्राहक विश्वास में कमी आई है। दीप

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

और शर्मा (2018) ने आगे उल्लेख किया कि बैंकिंग क्रेडेंशियल्स को लक्षित करने वाली फ़िशिंग वेबसाइटों और मैलवेयर के प्रसार ने पारंपरिक परिधि-आधारित सुरक्षा की अपर्याप्तता को रेखांकित किया है ***(दीप और शर्मा, 2018) /***

भारतीय बैंकों के सामने सबसे बड़ी चुनौतियों में से एक साइबर खतरों की गतिशील प्रकृति है, जो जटिलता और पैमाने में इतनी तेजी से विकसित होते हैं कि अक्सर संगठनों की प्रभावी ढंग से प्रतिक्रिया करने की क्षमता से आगे निकल जाते हैं। कुशवाह एट अल. (2016) ने बैंकिंग में साइबर सुरक्षा के मुख्य स्तंभों के रूप में गोपनीयता, अखंडता और उपलब्धता की पहचान की, इस बात पर प्रकाश डाला कि दूरस्थ पहुँच और सार्वजनिक नेटवर्क का उपयोग कमज़ोरियों को काफी हद तक बढ़ाता है ***(कुशवाहा एट अल., 2016) /*** इसके अलावा, बैंकों के आईटी इन्फ्रास्ट्रक्चर के भीतर विरासत प्रणालियों और तीसरे पक्ष के एकीकरण की विविधता मानकीकृत सुरक्षा प्रोटोकॉल के कार्यान्वयन को जटिल बनाती है। कर्मचारियों और ग्राहकों के बीच अपर्याप्त साइबर सुरक्षा जागरूकता जैसे मानवीय कारक - एक व्यापक चिंता का विषय बने हुए हैं, जो सामाजिक इंजीनियरिंग हमलों और अंदरूनी खतरों की सफलता में योगदान करते हैं।

भारतीय बैंकिंग क्षेत्र में साइबर घटनाओं का प्रभाव तत्काल वित्तीय नुकसान से कहीं अधिक है, जिसमें प्रतिष्ठा को नुकसान, विनियामक दंड और ग्राहकों के विश्वास में दीर्घकालिक कमी शामिल है। हाई-प्रोफाइल डेटा उल्लंघन और एटीएम धोखाधड़ी अक्सर सुर्खियाँ बनती हैं, जो साइबर सुरक्षा चूक से उत्पन्न प्रणालीगत जोखिमों को रेखांकित करती हैं। अल्ज़ौबी एट अल. (2022) की एक रिपोर्ट ने निष्कर्ष निकाला कि उभरती अर्थव्यवस्थाओं में डिजिटल बैंकिंग प्लेटफ़ॉर्म महत्वपूर्ण सुरक्षा चुनौतियों का सामना करते हैं, जिसमें अपर्याप्त मल्टी-फ़ैक्टर प्रमाणीकरण, कमज़ोर एन्क्रिप्शन प्रथाएँ और सीमित उपभोक्ता जागरूकता को प्राथमिक जोखिम कारकों के रूप में पहचाना जाता है ***(अल्ज़ौबी एट अल., 2022) /***

इन खतरों के जवाब में, भारतीय बैंकों ने कई तरह के सुरक्षा उपाय अपनाए हैं, जिनमें एंड-टू-एंड एन्क्रिप्शन, मल्टी-फैक्टर ऑथेंटिकेशन, घुसपैठ का पता लगाना और रोकथाम प्रणाली, और मजबूत घटना प्रतिक्रिया ढांचे शामिल हैं। RBI के साइबर सुरक्षा ढांचे और सूचना प्रौद्योगिकी अधिनियम, 2000 जैसे विनियामक अधिदेशों में समय-समय पर सुरक्षा ऑडिट, साइबर घटनाओं की रिपोर्टिंग और न्यूनतम सुरक्षा मानकों के कार्यान्वयन की आवश्यकता होती है। हालाँकि, अनुभवजन्य साक्ष्य बताते हैं कि केवल अनुपालन ही लचीलेपन की गारंटी नहीं है; सक्रिय खतरे की खुफिया जानकारी, निरंतर निगरानी और अनुकूली जोखिम प्रबंधन रणनीतियाँ उभरते हमले के वैक्टर का मुकाबला करने के लिए आवश्यक हैं।

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

मौजूदा सुरक्षा उपायों के एक महत्वपूर्ण विश्लेषण से खतरे की दृश्यता, विसंगति का पता लगाने और प्रतिक्रिया समन्वय जैसे क्षेत्रों में लगातार अंतराल का पता चलता है। जबकि बड़े बैंकों के भीतर उन्नत सुरक्षा संचालन केंद्र (एसओसी) स्थापित किए गए हैं, छोटे संस्थानों में अक्सर ऐसी क्षमताओं को प्रभावी ढंग से संचालित करने के लिए अपेक्षित प्रतिभा और वित्तीय संसाधनों की कमी होती है। इसके अलावा, क्लाउड कंप्यूटिंग और फिनटेक साझेदारी को तेजी से अपनाने से डेटा गोपनीयता, तीसरे पक्ष के जोखिम प्रबंधन और नियामक अनुपालन से संबंधित अतिरिक्त जटिलताएं सामने आई हैं। ग्राहक जागरूकता और व्यवहार भी बैंकिंग प्रणालियों की साइबर सुरक्षा स्थिति में महत्वपूर्ण भूमिका निभाते हैं। अध्ययनों से पता चला है कि साइबर सुरक्षा पर बढ़ते नियामक जोर के बावजूद, फ़िशिंग प्रयासों को पहचानने और मोबाइल उपकरणों को सुरक्षित करने जैसे सर्वोत्तम तरीकों की उपभोक्ता समझ असंगत बनी हुई है। इस अंतर को पाटने के लिए बैंकों, नियामकों और शैक्षणिक संस्थानों के बीच साइबर सुरक्षा साक्षरता को बढ़ावा देने और हितधारकों के बीच सतर्कता की संस्कृति विकसित करने के लिए सहयोगात्मक प्रयासों की आवश्यकता है। भारतीय बैंकिंग क्षेत्र में साइबर सुरक्षा चुनौतियों की बहुमुखी प्रकृति, इस अध्ययन का उद्देश्य वर्तमान खतरे के परिदृश्य की व्यापक जांच प्रदान करना, सुरक्षा उपायों की प्रभावशीलता का आकलन करना और सुधार के लिए प्रमुख क्षेत्रों की पहचान करना है। विनियामक दिशा-निर्देशों, उद्योग प्रथाओं और अकादमिक शोध से प्राप्त अंतर्दृष्टि को संश्लेषित करके, शोध साइबर खतरों के खिलाफ लचीलापन बढ़ाने और भारत में डिजिटल बैंकिंग के सतत विकास का समर्थन करने के लिए कार्रवाई योग्य सिफारिशें प्रदान करेगा। तेजी से डिजिटल परिवर्तन और बढ़ते साइबर खतरों का मिलन भारतीय बैंकों के लिए एक महत्वपूर्ण मोड़ प्रस्तुत करता है। वित्तीय स्थिरता और ग्राहक विश्वास की रक्षा के लिए साइबर सुरक्षा ढांचे को मजबूत करना, हितधारक सहयोग को बढ़ावा देना और अत्याधुनिक रक्षा तंत्र में निवेश करना अनिवार्य है। यह परिचय भारतीय बैंकिंग प्रणाली के साइबर सुरक्षा परिदृश्य को परिभाषित करने वाली चुनौतियों, प्रभावों और सुरक्षा रणनीतियों की गहन खोज के लिए मंच तैयार करता है।

II. संबंधित समीक्षाएँ

सर्विडियो और टेलर (2015) ने देखा कि साइबर हमलों की आवृत्ति, परिष्कार और दायरा धीरे-धीरे बढ़ रहा है, जिससे वे अधिक व्यापक हो रहे हैं। उन्होंने उल्लेख किया कि कई सामुदायिक बैंकों ने हाल के वर्षों में साइबर घटनाओं का अनुभव किया है, जिसमें मैलवेयर हमले और क्लाइंट डेटा प्राप्त करने के उद्देश्य से फ़िशिंग प्रयास शामिल हैं। जबकि प्रमुख वित्तीय संस्थानों और बड़े खुदरा विक्रेताओं ने सबसे अधिक मीडिया का ध्यान आकर्षित किया था, कई सामुदायिक बैंकों और वित्तीय संस्थानों ने भी साइबर खतरों का सामना किया था। इन

IJAMSR
International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

बैंकों के खिलाफ धोखाधड़ी की गतिविधियाँ, जैसे कि स्वचालित टेलर मशीनों से अनधिकृत नकद निकासी और खाता अधिग्रहण चोरी, की गई थीं। उन्होंने इस बात पर प्रकाश डाला कि कई छोटे और मध्यम आकार के बैंकों के पास साइबर हमलों से खुद को बचाने के लिए आवश्यक संसाधनों की कमी है। उनके लेख में बताया गया है कि कैसे सामुदायिक बैंक बैंकिंग एजेंसी की सिफारिशों के साथ संरेखित साइबर सुरक्षा रणनीति विकसित कर सकते हैं, जो साइबर सुरक्षा तैयारी के पाँच प्रमुख स्तंभों के आसपास संरचित है। उनके अनुसार, यह दृष्टिकोण सामुदायिक बैंकों को साइबर खतरों को रोकने, कम करने और प्रभावी ढंग से जवाब देने में मदद करेगा।

प्रदीप (2015) ने कहा कि 1990 के बाद, भारत सरकार ने निवेश क्षेत्र को उदार बनाने के उपायों को लागू किया था, जिससे वित्तीय संस्थानों के भीतर सेवा की गुणवत्ता और परिचालन दक्षता में महत्वपूर्ण प्रगति हुई, जिसने भारतीय अर्थव्यवस्था में बहुत योगदान दिया। उन्होंने इस बात पर जोर दिया कि 21वीं सदी में प्रौद्योगिकी एक महत्वपूर्ण प्रेरक शक्ति बन गई है, जिससे सूचना प्रौद्योगिकी के बिना दुनिया की कल्पना करना असंभव हो गया है। वैश्विक बाजार में प्रतिस्पर्धी बने रहने के लिए, वित्तीय संस्थानों ने अपनी बैंकिंग सेवाओं के तकनीकी पहलुओं को उन्नत करना शुरू कर दिया है। उन्होंने इस बात पर प्रकाश डाला कि इंटरनेट बैंकिंग, इलेक्ट्रॉनिक बैंकिंग, केंद्रीकृत कोर बैंकिंग, प्लास्टिक मनी के माध्यम से इलेक्ट्रॉनिक कॉमर्स और ग्राहक सेवा प्रमुख प्रौद्योगिकी-संचालित क्षेत्रों में से हैं, जिन्हें पर्याप्त पूंजी निवेश प्राप्त हुआ है। इसके अलावा, बैंकों की जांच की जा रही थी कि कौन सी ग्राहक-आधारित सेवाएँ विकसित हो रहे सेवा मॉडल में सफल होंगी। भविष्य को देखते हुए, बैंकिंग उद्योग से सर्वव्यापी बैंकिंग प्रथाओं को अपनाकर स्थिरता प्राप्त करने पर ध्यान केंद्रित करने की उम्मीद की गई थी। हालांकि, उन्होंने कहा कि साइबर अपराध एक अप्रत्याशित और चुनौतीपूर्ण खतरे के रूप में उभरा है जिसका पता लगाना और उसे कम करना मुश्किल है। बैंकिंग चैनलों की सुरक्षा, व्यक्तिगत डेटा की सुरक्षा और प्रौद्योगिकी-संचालित वाणिज्यिक लेनदेन की सुरक्षा ने महत्वपूर्ण जोखिम उत्पन्न किए हैं। अध्ययन का उद्देश्य विभिन्न बैंकिंग सेवाओं का पता लगाना था जो सूचना प्रौद्योगिकी का उपयोग करती हैं और बैंकिंग में आईटी के विनियामक पहलुओं की जांच करती हैं। इसके अतिरिक्त, इसने 2010 और 2013 के बीच भारत में किए गए साइबर अपराधों की गंभीरता को दर्शाते हुए साइबर सुरक्षा की आवश्यकता का आकलन किया।

मल्होत्रा (2015) ने देखा कि संयुक्त राज्य अमेरिका के कॉर्पोरेट और सरकारी दोनों क्षेत्रों में साइबर सुरक्षा व्यवसायी अपना ध्यान साइबर जोखिम प्रबंधन की ओर केंद्रित कर रहे हैं। परिणामस्वरूप, उभरते अनुप्रयोगों से जुड़े प्रशिक्षण पाठ्यक्रमों के साथ आईटी-साइबर सुरक्षा पेशेवर संगठनों के अनुप्रयोग मानकों को संरेखित करना महत्वपूर्ण हो गया था। उन्होंने नोट किया कि नेटवर्क प्रोटोकॉल और विश्लेषण उपकरण, सिस्टम और

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

नेटवर्क इंफ्रास्ट्रक्चर और जोखिम प्रबंधन नीतियों से संबंधित रूपरेखा मौजूदा शैक्षिक पाठ्यक्रमों और मानकों के भीतर खंडित प्रतीत होती है। अध्ययन का उद्देश्य लागू जोखिम प्रबंधन प्रथाओं की आवश्यकताओं को बेहतर ढंग से पूरा करने के लिए इन मानकों को संरेखित, एकीकृत और सरल बनाने के लिए एक लागू रूपरेखा प्रदान करना था। वॉयस ओवर इंटरनेट प्रोटोकॉल (वीओआईपी) नेटवर्क पर विशेष ध्यान देने के साथ, जिसने वैश्विक बैंकिंग और वित्त सहित विभिन्न उद्योगों में महत्वपूर्ण महत्व प्राप्त किया था, साइबर जोखिम प्रबंधन रूपरेखा विकसित की जा रही थी। तकनीकी और आर्थिक रूप से उनकी महत्वपूर्ण भूमिका के बावजूद, इन नेटवर्क में प्रमुख कमजोरियों - जिन्हें अक्सर वैश्विक वित्तीय प्रणालियों में "सबसे कमजोर लिंक" के रूप में संदर्भित किया जाता है, पर कम से कम ध्यान दिया गया था, जैसा कि साइबर सुरक्षा और पैठ परीक्षण परिणामों से स्पष्ट होता है। लेख में दर्शाया गया है कि प्रस्तावित साइबर जोखिम प्रबंधन ढांचे ने बैंकिंग और वित्त उद्योग के भीतर इन सुरक्षा अंतरालों को संबोधित करने में महत्वपूर्ण भूमिका निभाई है। इसके अलावा, इसने इस बात पर प्रकाश डाला कि साइबर सुरक्षा और सूचना आश्वासन की तकनीकें, वित्तीय अनुप्रयोगों के माध्यम से उदाहरण के रूप में, स्वास्थ्य सेवा जैसे अन्य क्षेत्रों में भी लागू होती हैं।

मबेली और ड्वोलट्स्की (2016) ने दक्षिण अफ़्रीका में ऑनलाइन बैंकिंग से जुड़े साइबर सुरक्षा जोखिमों की जांच की, जिसमें पाया गया कि हाल के वर्षों में वित्तीय सूचना प्रणालियों के खिलाफ़ साइबर हमले अधिक बार हुए हैं। उन्होंने देखा कि इस घटना के जवाब में, दक्षिण अफ़्रीकी वित्तीय संस्थानों ने जोखिम प्रबंधन को अपनी व्यावसायिक रणनीति के एक महत्वपूर्ण पहलू के रूप में मानना शुरू कर दिया है। साइबर हमलों के कारण होने वाले बड़े वित्तीय और सूचनात्मक नुकसान को रोकने के लिए, नवीनतम सुरक्षा उपायों और प्रौद्योगिकियों में निरंतर निवेश लाभदायक साबित हुआ है। उन्होंने इस बात पर प्रकाश डाला कि साइबर अपराध का बढ़ना दक्षिण अफ़्रीकी संगठनों और पूरे देश के लिए एक महत्वपूर्ण आर्थिक चुनौती बन गया है। उनके अध्ययन ने पहले ऑनलाइन बैंकिंग से संबंधित विभिन्न साइबर खतरों का विश्लेषण किया और बाद में सीमा और एप्लिकेशन सुरक्षा दोनों को शामिल करते हुए एक साइबर-बैंकिंग सुरक्षा वास्तुकला का प्रस्ताव रखा। उन्होंने बताया कि दोनों सुरक्षा परतें कमज़ोरियों को कम करने की तकनीकें प्रदान करती हैं, जिसमें सीमा सुरक्षा वास्तुकला में चार मुख्य घटक शामिल हैं। निष्कर्ष में, उन्होंने वित्तीय संस्थानों के लिए कार्यान्वयन के लिए एक साइबर-बैंकिंग सुरक्षा ढाँचे की सिफारिश की।

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

कुशवाह एट अल. (2016) ने कहा कि इंटरनेट सेवाओं का उपयोग करने वाले बैंकिंग अनुप्रयोगों के लिए सूचना सुरक्षा बैंक की सूचना और सूचना प्रणाली परिसंपत्तियों की सुरक्षा में एक आवश्यक घटक रही है। उन्होंने नोट किया कि सॉफ़्टवेयर प्रोग्राम और नेटवर्किंग घटकों सहित परिसंपत्तियों की सुरक्षा, उनके साथ जुड़े तरीकों और उपकरणों और प्रौद्योगिकियों दोनों पर निर्भर करती है। आवश्यक बैंकिंग कार्यों को करने के लिए दूरस्थ उपयोगकर्ताओं और कर्मचारियों द्वारा खुले सार्वजनिक नेटवर्क के उपयोग के कारण, ऑनलाइन बैंकिंग प्रणाली संभावित साइबर खतरों के प्रति अधिक संवेदनशील हो गई थी। सबसे महत्वपूर्ण सुरक्षा चिंताओं में गोपनीयता, अखंडता, उपलब्धता और सटीकता थी। उन्होंने कार्यों के डोमेन का उपयोग करके इन सुरक्षा चुनौतियों का विश्लेषण किया और बैंकिंग परिसंपत्तियों से जुड़े जोखिमों को कम करने के लिए कुशल प्रक्रियाएँ विकसित कीं। इसके अतिरिक्त, उन्होंने उन विधायी कानूनों और विनियमों पर प्रकाश डाला, जिन्होंने साइबर अपराधियों और हैकर्स को बैंक की सूचना परिसंपत्तियों से समझौता करने से रोकने में महत्वपूर्ण भूमिका निभाई है। उनके विचार में, एक सक्रिय सुरक्षा तंत्र को एप्लिकेशन की अखंडता और इसकी समग्र सुरक्षा दोनों को बनाए रखने के लिए सबसे प्रभावी समाधान माना गया था। उन्होंने वित्तीय सेवाओं से जुड़े नैतिक विचारों पर भी जोर दिया, जिसमें कहा गया कि कार्यस्थल में नैतिक व्यवहार को तकनीकी प्लेटफ़ॉर्म के भीतर सिस्टम की भूमिका के साथ रचनात्मक रूप से संरेखित करने की आवश्यकता है।

गुप्ता एट अल. (2016) ने कहा कि इंटरनेट का उपयोग अभूतपूर्व दर से बढ़ रहा है, इसके अनुप्रयोग दैनिक जीवन में तेजी से एकीकृत हो रहे हैं। उन्होंने इस बात पर जोर दिया कि इंटरनेट विभिन्न व्यवसायों के व्यक्तियों के लिए आवश्यक हो गया है, चाहे वह व्यक्तिगत, पेशेवर या सरकारी उपयोग के लिए हो। उन्होंने आगे बताया कि ऑनलाइन शॉपिंग, वित्तीय लेनदेन, शिक्षा और सार्वजनिक सेवाओं जैसे अनुप्रयोगों को सुरक्षा की आवश्यकता है, क्योंकि इंटरनेट के उपयोग में वृद्धि के साथ-साथ साइबर सुरक्षा संबंधी चिंताएँ भी बढ़ गई हैं। उन्होंने उल्लेख किया कि इंटरनेट में कई कमजोरियाँ हैं जिन्हें संबोधित करने की आवश्यकता है, जिसमें धोखाधड़ी वाले वित्तीय लेनदेन (फ़िशिंग), HTML इंजेक्शन, SQL इंजेक्शन और इसी तरह के अन्य हमले जैसे विभिन्न साइबर खतरे शामिल हैं। चूंकि सुरक्षा खतरे तेजी से विकसित हो रहे थे, इसलिए उन्होंने बताया कि साइबर सुरक्षा एक बढ़ती हुई चिंता बन गई है। संभावित समाधानों के रूप में, उन्होंने एक्सेस कंट्रोल, मैसेज एन्क्रिप्शन और घुसपैठ का पता लगाने जैसे उपायों पर चर्चा की। इसके अतिरिक्त, उन्होंने उल्लेख किया कि जानकारी को सुरक्षित रखने के लिए उसे चुराया जा सकता है, और बिना पता लगाए संशोधन किए जाने से पहले कमजोर डेटा को निकाला जा सकता है।

IJAMSR
International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

अलगाज़ो एट अल. (2017) ने कहा कि इंटरनेट बैंकिंग सबसे सुविधाजनक और सबसे तेज़ बैंकिंग विधियों में से एक के रूप में उभरी है, लेकिन साइबर सुरक्षा खतरों ने इंटरनेट बैंकिंग और ई-कॉमर्स व्यवसायों दोनों के लिए एक बड़ी चुनौती पेश की है। उन्होंने तीन विकासशील देशों में इंटरनेट बैंकिंग साइबर सुरक्षा का गहन विश्लेषण किया और बैंकों और उपभोक्ताओं के बीच की खाई को पाटने के उद्देश्य से साइबर जोखिमों को कम करने के लिए एक अनूठा दृष्टिकोण प्रस्तावित किया। उनका मॉडल सऊदी अरब, पाकिस्तान और भारत में इंटरनेट बैंकिंग की आदतों से संबंधित सर्वेक्षण निष्कर्षों के आधार पर विकसित किया गया था। अध्ययन में मुख्य रूप से साइबर सुरक्षा के बारे में उपयोगकर्ताओं की समझ और इंटरनेट बैंकिंग में आम खतरों के बारे में उनकी जागरूकता पर ध्यान केंद्रित किया गया, जिसमें उनके ज्ञान का आकलन करने के लिए प्रश्न तैयार किए गए थे।

एम्बोरे एट अल. (2017) ने कहा कि साइबर अपराध में तेजी से वृद्धि तकनीकी प्रगति और साइबरस्पेस में उपलब्ध वित्तीय अवसरों से जुड़ी हुई है। उन्होंने कहा कि साइबर अपराध शीर्ष दस वैश्विक खतरों में से एक बन गया है, जिससे संगठनों को इसके जोखिमों को कम करने के लिए नियंत्रण और प्रतिवाद में निवेश करने के लिए प्रेरित किया जा रहा है। हालाँकि, इन प्रयासों के बावजूद, सफल साइबर हमलों की आवृत्ति में वृद्धि जारी रही। उन्होंने देखा कि मोबाइल उपकरणों के आगमन ने दुनिया भर में दो अरब से अधिक लोगों को पारंपरिक बैंकिंग प्रणालियों के माध्यम से पहले से उपलब्ध नहीं होने वाली वित्तीय सेवाओं तक पहुँचने में सक्षम बनाया है। इसके अतिरिक्त, बैंकों और वित्तीय संस्थानों ने वित्तीय लेनदेन के लिए वैकल्पिक चैनल के रूप में मोबाइल प्लेटफ़ॉर्म का उपयोग तेज़ी से किया है। हालाँकि, उन्होंने बताया कि मोबाइल उपकरणों ने नई साइबर सुरक्षा कमज़ोरियों को भी पेश किया है, जिसने सिस्टम में विश्वास को नकारात्मक रूप से प्रभावित किया है और मोबाइल वित्तीय सेवाओं (MFS) को अपनाने की गति को धीमा कर दिया है। उनके अध्ययन ने मोबाइल प्लेटफ़ॉर्म द्वारा बिना बैंक वाले लोगों को दिए जाने वाले लाभों का विस्तृत विश्लेषण प्रदान किया और जाँच की कि कैसे साइबर सुरक्षा चिंताओं ने MFS को व्यापक रूप से अपनाने में बाधा उत्पन्न की है। इसके अलावा, उन्होंने अपने शोध से प्रारंभिक निष्कर्ष प्रस्तुत किए और जटिल MFS पारिस्थितिकी तंत्र के भीतर साइबर अपराध को कम करने की रणनीति प्रस्तावित की।

हुसैन एट अल. (2017) ने कहा कि इलेक्ट्रॉनिक बैंकिंग में उपयोग किए जाने वाले प्रदाता नेटवर्क में बैंकों द्वारा पहले किए गए विभिन्न कार्यों को बदलने और दोहराने की क्षमता थी। उन्होंने नोट किया कि इलेक्ट्रॉनिक बैंकिंग व्यक्तियों और निगमों दोनों के लिए वित्तीय लेनदेन को निष्पादित करने के लिए एक आवश्यक उपकरण बन गया है, जिससे संचार, वितरण और लेनदेन चैनलों की सुरक्षा सुनिश्चित करना आवश्यक हो गया है। इसमें बैंकों

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

के स्वामित्व वाले इंटरनेट या वर्चुअल प्राइवेट नेटवर्क पर आधारित इलेक्ट्रॉनिक बैंकिंग गतिविधियाँ शामिल थीं। उनके अध्ययन ने ई-बैंकिंग क्रांति में नवीनतम रुझानों की जांच की, जिसका उद्देश्य पाकिस्तानी बैंकिंग ग्राहकों के लिए एक सरल इंटरफ़ेस प्रदान करना था, जिससे उन्हें भौतिक बैंक शाखा में जाने की आवश्यकता के बिना सेवाओं तक पहुँचने की अनुमति मिल सके। उनके अनुभवजन्य शोध का उद्देश्य पाकिस्तान में विभिन्न वित्तीय क्षेत्रों में इलेक्ट्रॉनिक बैंकिंग को लागू करने में आने वाली चुनौतियों की पहचान करना था। उनके निष्कर्षों ने संकेत दिया कि बैंकिंग क्षेत्र में इंटरनेट की पहुँच संबंधी समस्याओं के कारण ग्राहक अपने बैंक खातों को ऑनलाइन एक्सेस करने में झिझक रहे थे। इसके अतिरिक्त, उन्होंने पाया कि साइबर सुरक्षा की कमी का इलेक्ट्रॉनिक बैंकिंग सेवाओं में ग्राहकों के विश्वास पर महत्वपूर्ण प्रभाव पड़ा।

दीप और शर्मा (2018) ने कहा कि भारत में साइबर अपराध में वृद्धि देश के बढ़ते डिजिटलीकरण और आर्थिक विकास से प्रेरित थी। उन्होंने नोट किया कि फ़िशिंग, जिसमें वेबसाइट हैकिंग और मैलवेयर डाउनलोड शामिल थे, ने महत्वपूर्ण जानकारी के विरूपण और रिसाव को जन्म दिया था। कई घटनाओं ने भारत की बिगड़ती साइबर सुरक्षा स्थिति को उजागर किया था। उनके अध्ययन ने इलेक्ट्रॉनिक सिस्टम, फ़िशिंग वेबसाइट और साइबरबुलिंग पर हमलों के साथ-साथ मैलवेयर के प्रसार, निर्माण और संचालन पर ध्यान केंद्रित किया। उन्होंने विभिन्न साइबर अपराध मामलों पर विस्तार से चर्चा की, जिससे हनीपोट्स और अन्य निवारक उपायों का विकास हुआ, और निष्कर्ष निकाला कि साइबर अपराध को विशिष्ट तकनीकों के माध्यम से कम किया जा सकता है। उन्होंने देखा कि वैश्वीकरण और डिजिटलीकरण ने इंटरनेट ऑफ़ थिंग्स के माध्यम से व्यक्तियों और सेवाओं सहित समाज के सभी पहलुओं को आपस में जोड़ दिया है। ऑनलाइन बैंकिंग, जिसमें मार्केटिंग और वित्तीय लेनदेन शामिल थे, एक मानक अभ्यास बन गया था, जबकि क्लाउड कंप्यूटिंग का व्यवसाय में व्यापक रूप से उपयोग किया गया था, हालांकि यह डेटा स्वामित्व और जवाबदेही से संबंधित जोखिमों के प्रति संवेदनशील रहा। अंत में, उन्होंने भारत में साइबर सुरक्षा की चिंताजनक स्थिति पर टिप्पणी की तथा देश की साइबर सुरक्षा रणनीतियों में भविष्य के विकास का अनुमान लगाया।

शम्सुद्दीन एट अल. (2018) ने मलेशिया के बैंकिंग संस्थानों के भीतर साइबर सुरक्षा को संबोधित करने में आंतरिक लेखा परीक्षा प्रथाओं की प्रभावकारिता की जांच की। उनके अध्ययन का उद्देश्य साइबर सुरक्षा के प्रबंधन में आंतरिक लेखा परीक्षा की दक्षता को प्रभावित करने वाले तीन प्रमुख कारकों की जांच करना था: साइबर सुरक्षा के बारे में आंतरिक लेखा परीक्षकों की समझ, साइबर सुरक्षा पर संगठनात्मक नीतियाँ और साइबर सुरक्षा से संबंधित संगठनात्मक जोखिम प्रबंधन। डेटा एकत्र करने के लिए, उन्होंने चयनित वित्तीय

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

संस्थानों के आंतरिक लेखा परीक्षकों को वितरित प्रश्नावली का उपयोग करके एक सर्वेक्षण किया, जिसमें सात वाणिज्यिक बैंकों के 120 प्रतिभागियों से प्राप्त उत्तर शामिल थे। उनके निष्कर्षों ने तीन पहचाने गए कारकों में से प्रत्येक और साइबर सुरक्षा के प्रबंधन में आंतरिक लेखा परीक्षा की प्रभावशीलता के बीच एक मजबूत संबंध का संकेत दिया। उन्होंने सुझाव दिया कि परिणाम साइबर सुरक्षा प्रबंधन को बढ़ाने के लिए नीतियों और प्रक्रियाओं को तैयार करने में प्रासंगिक अधिकारियों और संगठनों की सहायता कर सकते हैं। इसके अतिरिक्त, उन्होंने इस बात पर जोर दिया कि उनका शोध मलेशिया में साइबर सुरक्षा पर मौजूदा साहित्य का विस्तार करने में योगदान देगा, जो सीमित बना हुआ है।

महले एट अल. (2018) ने कहा कि दुनिया भर में व्यवसायों और सरकारों ने क्लाउड कंप्यूटिंग आर्किटेक्चर और इंफ्रास्ट्रक्चर को तेजी से पहचाना और अपनाया है। उन्होंने देखा कि क्लाउड कंप्यूटिंग ने भौतिक और तकनीकी दोनों तरह के इंफ्रास्ट्रक्चर के प्रबंधन से जुड़ी लागतों को कम करने में योगदान दिया है, साथ ही वैश्विक और स्थानीय कर्मचारियों को सूचना प्रणालियों तक आसान पहुँच प्रदान की है। चूंकि क्लाउड कंप्यूटिंग ने उपयोगकर्ताओं को किसी भी स्थान से डेटा और एप्लिकेशन प्राप्त करने की अनुमति दी है, इसलिए व्यवसाय लगातार उभरती चुनौतियों के साथ तालमेल बनाए रखने के लिए अपनी गोपनीयता और सुरक्षा रूपरेखाओं का पुनर्मूल्यांकन कर रहे थे। उन्होंने नोट किया कि बैंकिंग और वित्तीय सेवाएँ प्रतिस्पर्धात्मक बढ़त बनाए रखने के लिए आंतरिक रूप से उत्पन्न डेटा और एप्लिकेशन पर निर्भर हैं, क्योंकि ये व्यावसायिक संचालन के लिए आवश्यक बौद्धिक संपदा (आईपी) का गठन करते हैं। हालाँकि, उन्होंने इस बात पर प्रकाश डाला कि ऐसे डेटा और एप्लिकेशन की दूरस्थ पहुँच से समय के साथ डेटा लीक और बौद्धिक संपदा के संभावित क्षरण का जोखिम पैदा होता है। क्लाउड कंप्यूटिंग को व्यापक रूप से अपनाने के कारण, उन्होंने इस बात पर जोर दिया कि बैंकिंग और वित्तीय सेवा क्षेत्र डेटा गोपनीयता और सिस्टम सुरक्षा सुनिश्चित करने के उद्देश्य से सख्त विनियामक और अनुपालन रूपरेखाओं के अधीन बना हुआ है। उन्होंने निष्कर्ष निकाला कि उपयोगकर्ता गोपनीयता संरक्षण और क्लाउड अवसंरचना सुरक्षा के बारे में चिंताएं वैश्विक स्तर पर बनी हुई हैं और इसका उद्देश्य बैंकिंग और वित्तीय सेवा उद्योग में डेटा गोपनीयता की सुरक्षा और सिस्टम सुरक्षा बनाए रखने से संबंधित क्लाउड कंप्यूटिंग के विभिन्न पहलुओं को प्रस्तुत करना था।

अल-अलावी और अल-बसम (2019) ने अकाउंटिंग उद्योग में साइबर सुरक्षा जागरूकता को प्रभावित करने वाले कारकों की पहचान करने का लक्ष्य रखा। उन्होंने देखा कि मौजूदा साहित्य में कई कमियाँ उजागर हुई हैं, जिन पर वरिष्ठ प्रबंधन और साइबर सुरक्षा विशेषज्ञों दोनों को दृढ़ विश्वास और निश्चितता के आधार पर

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

अर्थव्यवस्था में एक सुरक्षित डिजिटल संस्थान स्थापित करने के लिए ध्यान देने की आवश्यकता है। इन कमियों को चार प्रमुख कारकों के लिए जिम्मेदार ठहराया गया: शीर्ष प्रबंधन की प्रतिबद्धता और समर्थन, बजट, साइबर सुरक्षा विनियमों का अनुपालन और साइबर सुरक्षा संस्कृति। प्रश्नावली-आधारित विश्लेषण का उपयोग करके एक मात्रात्मक दृष्टिकोण अपनाया गया। अध्ययन ने स्व-प्रशासित प्रश्नावली के माध्यम से छह बहरीनी इस्लामी खुदरा बैंकों और पाँच बहरीनी पारंपरिक वाणिज्यिक खुदरा बैंकों के 109 आईटी कर्मचारियों का सर्वेक्षण किया। डेटा का मूल्यांकन करने के लिए प्रतिशत और संकेतकों की औसत-आधारित रैंकिंग सहित वर्णनात्मक विश्लेषण का उपयोग किया गया था। परिणामों ने संकेत दिया कि सुरक्षा अनुपालन का उच्चतम औसत स्कोर 4.28 था, जबकि साइबर सुरक्षा संस्कृति का सबसे कम 4.24 था, जो पुष्टि करता है कि सभी पहचाने गए कारक साइबर सुरक्षा जागरूकता के लिए प्रासंगिक थे। उत्तरदाताओं ने बैंकिंग क्षेत्र में इन कारकों की आवश्यकता पर सर्वसम्मति से सहमति व्यक्त की। हालांकि, अध्ययन ने तत्वों के प्रस्तावित संयोजन पर मौजूदा शोध की कमी में एक सीमा को स्वीकार किया। शोधकर्ताओं ने जोर दिया कि नीति निर्माताओं और साइबर सुरक्षा विशेषज्ञों को साइबर सुरक्षा जागरूकता बढ़ाने, साइबर खतरों को कम करने और साइबर अपराध को रोकने के लिए दिशानिर्देश तैयार करने में अध्ययन के व्यावहारिक निहितार्थों पर विचार करना चाहिए। उन्होंने जोर देकर कहा कि उनके निष्कर्षों ने साहित्य में एक अंतर को भरने में योगदान दिया, जिससे सुरक्षित डिजिटल संस्थानों के विकास में सहायता मिली। इसके अतिरिक्त, उन्होंने नोट किया कि साइबर सुरक्षा तंत्र ने कॉर्पोरेट प्रतिष्ठा, बौद्धिक संपदा और वित्तीय डेटा को अनधिकृत पहुँच से बचाने में महत्वपूर्ण भूमिका निभाई। उन्होंने यह भी बताया कि स्मार्टफोन, पर्सनल कंप्यूटर और इंटरनेट-आधारित सिस्टम जैसे इलेक्ट्रॉनिक उपकरणों का उपयोग करने वाले व्यक्ति साइबर जोखिमों के प्रति संवेदनशील बने हुए हैं। हालांकि, उन्होंने दोहराया कि बैंकिंग क्षेत्र में साइबर सुरक्षा जागरूकता से संबंधित कारकों के सुझाए गए संयोजन पर सीमित प्रकाशित शोध मौजूद हैं।

अधोलिया और अधोलिया (2019) ने कहा कि साइबर अपराध के खतरों और चुनौतियों ने राष्ट्रीय सुरक्षा, व्यक्तिगत डेटा गोपनीयता, वित्तीय लेनदेन सुरक्षा और इंटरनेट ब्राउज़िंग सुरक्षा सहित विभिन्न क्षेत्रों में महत्वपूर्ण जोखिम पैदा किए हैं। उन्होंने इस बात पर जोर दिया कि व्यक्तियों को अपनी साइबर सुरक्षा प्रथाओं के बारे में जागरूक होने और अपने उपकरणों और ऑनलाइन गतिविधियों की सुरक्षा सुनिश्चित करने के लिए अपने ज्ञान को बढ़ाने की आवश्यकता है। उनके अध्ययन का उद्देश्य उदयपुर, राजस्थान में आम ई-बैंकिंग सेवाओं के उपयोगकर्ताओं के बीच साइबर सुरक्षा प्रथाओं और सिफारिशों के बारे में जागरूकता के स्तर का आकलन करना था। वित्तीय और गैर- वित्तीय वेब-आधारित गतिविधियों से जुड़ी सुरक्षा चिंताओं और खतरों का विश्लेषण करने के लिए एक अच्छी तरह से संरचित प्रश्नावली समीक्षा पद्धति का उपयोग किया गया था। प्रतिभागियों में ऐसे

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

व्यक्ति शामिल थे जिन्होंने उन्नत या इलेक्ट्रॉनिक बैंकिंग सेवाओं का उपयोग किया था। एकत्रित प्रतिक्रियाओं का सांख्यिकीय रूप से F-परीक्षण और प्रतिगमन विश्लेषण का उपयोग करके विश्लेषण किया गया ताकि साइबर हमलों और खतरों के बारे में जागरूकता के महत्व की जांच की जा सके, साथ ही साइबर सुरक्षा ज्ञान पर बैंकों और सामाजिक-आर्थिक प्रोफाइल के प्रभाव का भी पता लगाया जा सके। उनके निष्कर्षों ने संकेत दिया कि सामाजिक-आर्थिक कारकों ने साइबर सुरक्षा खतरों, हमलों और सर्वोत्तम प्रथाओं के बारे में उपभोक्ताओं की समझ को निर्धारित करने में महत्वपूर्ण भूमिका निभाई। इसके अतिरिक्त, उन्होंने पाया कि उदयपुर क्षेत्र में बैंक ग्राहकों में साइबर जोखिम, सुरक्षा चुनौतियों और आवश्यक सुरक्षात्मक उपायों के बारे में गहरी जागरूकता है।

वांग एट अल. (2020) ने बताया कि उनके अध्ययन ने नाइजीरियाई इंटरनेट बैंकिंग क्षेत्र में सबसे महत्वपूर्ण साइबर सुरक्षा उल्लंघनों की जांच की, साथ ही इसकी साइबर सुरक्षा क्षमता और प्रथाओं की भी जांच की। उन्होंने कहा कि यह शोध नाइजीरिया में बैंकिंग और बैंकिंग सुरक्षा सेवाओं में काम करने वाले सौ अनुभवी पेशेवरों से जुड़े एक ऑनलाइन सर्वेक्षण पर आधारित था। उनके निष्कर्षों से संकेत मिलता है कि नाइजीरियाई साइबर अपराध कम तकनीक वाले साइबर-सक्षम अपराधों से विकसित होकर अधिक परिष्कृत उल्लंघनों में बदल गया है, जिसमें सबसे आम खतरे वायरस, कीड़े या ट्रोजन संक्रमण; इलेक्ट्रॉनिक स्पैम मेलिंग; और हैकिंग हैं। उन्होंने देखा कि बैंकिंग कर्मियों को साइबर सुरक्षा नीतियों और प्रक्रियाओं के संबंध में पर्याप्त प्रबंधन सहायता और प्रशिक्षण मिला था। हालांकि, उन्होंने नोट किया कि सुरक्षा उल्लंघनों का पता लगाने और उन्हें कम करने के लिए नवीन तकनीक की अनुपस्थिति, अपर्याप्त नियामक अनुपालन के साथ, सर्वेक्षण किए गए बैंकों में देखी गई कम साइबर सुरक्षा क्षमता में योगदान देने वाले प्रमुख कारक थे।

परवेज एट अल. (2021) ने कहा कि पिछले कई वर्षों में, इंटरनेट दुनिया भर में दैनिक जीवन का एक अनिवार्य हिस्सा बन गया है। हालांकि, उन्होंने नोट किया कि इंटरनेट उपयोगकर्ताओं की बढ़ती संख्या के साथ-साथ साइबर अपराध गतिविधि भी बढ़ी है। इसे संबोधित करने के लिए, साइबरस्पेस में तेजी से बदलाव के साथ तालमेल रखने के लिए साइबर सुरक्षा में तकनीकी प्रगति की गई थी। उन्होंने बताया कि साइबर सुरक्षा का मतलब राष्ट्रों या संगठनों द्वारा डिजिटल स्पेस में अपनी संपत्तियों और सूचनाओं की सुरक्षा के लिए अपनाए गए सुरक्षात्मक उपायों से है। इक्कीसवीं सदी की शुरुआत में, आम जनता ने साइबर सुरक्षा को एक गंभीर मुद्दा नहीं माना था, लेकिन तब से यह न केवल व्यक्तियों के लिए बल्कि संगठनों और सरकारों के लिए भी चिंता का विषय बन गया है। उन्होंने इस बात पर प्रकाश डाला कि जैसे-जैसे डिजिटलीकरण आगे बढ़ा है, साइबरनेटिक्स ने इस परिवर्तन को सुविधाजनक बनाने के लिए क्लाउड कंप्यूटिंग, स्मार्टफोन और इंटरनेट ऑफ थिंग्स जैसी विभिन्न

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

तकनीकों को नियोजित किया है। लगातार साइबर हमलों ने गोपनीयता, सुरक्षा और वित्तीय नुकसान के बारे में चिंताएँ बढ़ा दी हैं। साइबर सुरक्षा, जैसा कि उन्होंने बताया, नेटवर्क, कंप्यूटर, प्रोग्राम और डेटा को अनधिकृत पहुँच, हमलों या क्षति से बचाने के उद्देश्य से तकनीकों, विधियों और प्रथाओं का एक समूह शामिल है। उनके अध्ययन में विभिन्न प्रकार की साइबर सुरक्षा, इसकी आवश्यकता, रूपरेखा, उपकरण और संबंधित चुनौतियों का गहन विश्लेषण करने की कोशिश की गई। उन्होंने इस बात पर जोर दिया कि साइबर सुरक्षा का प्राथमिक लक्ष्य संगठन के नेटवर्क से जुड़ी कंप्यूटर संपत्तियों के डेटा और अखंडता की सुरक्षा करना है, जिससे साइबर हमले के पूरे जीवनचक्र में सभी खतरे वाले अभिनेताओं से सुरक्षा सुनिश्चित हो सके।

अलज़ौबी एट अल. (2022) ने कहा कि पारंपरिक बैंकिंग के विपरीत, डिजिटल बैंकिंग की विशेषता पेन और पेपर के उपयोग की अनुपस्थिति है। उन्होंने इस बात पर प्रकाश डाला कि डिजिटल बैंकिंग से जुड़ी प्रमुख चुनौतियों में से एक विभिन्न सुरक्षा चिंताओं की उपस्थिति थी। उनके अनुसार, ये खतरे हैकर्स और धोखेबाजों की अवैध गतिविधियों से उत्पन्न हुए हैं, जो लोगों को उनके पैसे चुराने के इरादे से निशाना बनाते हैं। ऐसे जोखिमों का मुकाबला करने के लिए, उन्होंने एक प्रभावी सुरक्षा प्रणाली की आवश्यकता पर जोर दिया, जिसमें कई सत्यापन चरण, प्रमाणीकरण प्रक्रियाएँ और डेटा एन्क्रिप्शन एकीकृत हों। उन्होंने स्वीकार किया कि इस विषय पर पहले से ही अन्य विद्वानों द्वारा व्यापक शोध किया जा चुका है। विभिन्न स्रोतों से निष्कर्षों का विश्लेषण करने के बाद, उनके अध्ययन ने निष्कर्ष निकाला कि साइबर सुरक्षा खतरे डिजिटल बैंकिंग में एक महत्वपूर्ण चुनौती पेश करते हैं। उन्होंने आगे देखा कि अधिकांश व्यक्ति या तो इन सुरक्षा जोखिमों से अनजान थे या उन्हें एक बड़ी चिंता के रूप में नहीं देखते थे। अध्ययन ने द्वितीयक सूचना स्रोतों पर निर्भर करते हुए एक सैद्धांतिक विश्लेषण पद्धति का उपयोग किया। इसके अतिरिक्त, उन्होंने इस विषय पर कुछ सिद्धांत विकसित किए, जिन्हें उन्होंने पिछले शोध से कथनों और ग्राफ़िकल चार्ट का उपयोग करके प्रमाणित किया। उन्होंने शोध विषय को दिलचस्प पाया और सुझाव दिया कि यह भविष्य में आगे के अध्ययनों के लिए आधार का काम कर सकता है।

अल-अलावी एट अल. (2023) ने कहा कि साइबर हमलों की बढ़ती जटिलता के कारण, विशेष रूप से वित्तीय क्षेत्र में, साइबर सुरक्षा व्यवसाय मालिकों और ग्राहकों दोनों की सुरक्षा के लिए एक महत्वपूर्ण क्षेत्र बन गया है। उन्होंने डिजिटल बैंकिंग उद्योग के भीतर साइबर सुरक्षा में काम करने वाली महिलाओं की भूमिका का पता लगाया, उनके योगदान को प्रभावित करने वाले विभिन्न कारकों का विश्लेषण किया। इन कारकों में उनके सामने आने वाली चुनौतियाँ और बाधाएँ, फिनटेक पारिस्थितिकी तंत्र और डिजिटल परिवर्तन में उनकी भागीदारी, साइबर सुरक्षा प्रबंधन रणनीतियों का उनका अनुप्रयोग, साथ ही उनकी भागीदारी के सामाजिक और आर्थिक प्रभाव शामिल थे। अध्ययन में बैंकिंग के लिए साइबर सुरक्षा में महिलाओं के कौशल और योग्यता की भी जाँच की गई। उन्होंने देखा कि

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

पिछले अधिकांश अध्ययनों ने इस क्षेत्र में महिलाओं के कम प्रतिनिधित्व पर जोर दिया था और नवाचार और सुधार की आवश्यकता पर प्रकाश डाला था। निष्कर्षों की विश्वसनीयता सुनिश्चित करने के लिए गुणात्मक और मात्रात्मक तरीकों का संयोजन नियोजित किया गया था। उनके परिणामों ने प्रदर्शित किया कि बहरीन में महिलाओं में साइबर सुरक्षा में सफल होने और मौजूदा चुनौतियों को दूर करने की क्षमता थी। इसके अतिरिक्त, महिलाओं ने अपने करियर को आगे बढ़ाने और डिजिटल बैंकिंग में साइबर सुरक्षा बढ़ाने में रुचि व्यक्त की। हालांकि, उन्होंने कहा कि पहले के शोध में मुख्य रूप से बैंकिंग में महिलाओं की विशिष्ट भूमिकाओं और महत्व को संबोधित करने के बजाय साइबर सुरक्षा में प्रवेश करने पर ध्यान केंद्रित किया गया था, जो साइबर सुरक्षा उपायों की आवश्यकता वाला एक महत्वपूर्ण उद्योग बना हुआ है। अध्ययन ने सिफारिश की कि बहरीन सरकार और संगठन प्रोत्साहन और प्रोत्साहन के माध्यम से साइबर सुरक्षा में महिलाओं की प्रगति का समर्थन कर सकते हैं, जो अंततः आर्थिक विकास में योगदान देगा। इसके अलावा, उन्होंने महिलाओं के लिए एक व्यवहार्य कैरियर पथ के रूप में साइबर सुरक्षा को स्थापित करने के लिए पेशेवर प्रमाणन, प्रशिक्षण सत्र और ज्ञान वृद्धि के अवसरों को बढ़ाने का सुझाव दिया।

इकबाल एट अल. (2024) ने सुरक्षा जोखिम ढांचे की ट्रेसबिलिटी, भेद्यता और गुणवत्ता, साथ ही एक वित्तीय प्रणाली के भीतर सुरक्षा उपायों की तैनाती और निगरानी की जांच करने के लिए एक अध्ययन किया। पाकिस्तानी बैंकिंग क्षेत्र के संदर्भ में, उनका उद्देश्य बैंकिंग संस्थानों द्वारा दी जाने वाली डिजिटल बैंकिंग सेवाओं के प्रदर्शन पर इन कारकों के प्रभाव का आकलन करना था। उन्होंने प्राथमिक डेटा का उपयोग किया और एक मात्रात्मक शोध पद्धति को अपनाया, अपने दृष्टिकोण के रूप में व्याख्यात्मक शोध का चयन किया। अध्ययन में मोबाइल बैंकिंग ग्राहकों पर ध्यान केंद्रित किया गया, जिनके पास इलेक्ट्रॉनिक बैंकिंग में कम से कम एक वर्ष का अनुभव और मैट्रिकुलेशन या उससे अधिक का साक्षरता स्तर था। सुविधा नमूनाकरण का उपयोग किया गया, जिसके परिणामस्वरूप 138 प्रतिभागियों का नमूना आकार था। डेटा को प्रश्नावली के माध्यम से एकत्र किया गया और पीएलएस स्मार्ट सॉफ़्टवेयर के साथ संरचनात्मक समीकरण मॉडलिंग का उपयोग करके विश्लेषण किया गया । उनके निष्कर्षों ने संकेत दिया कि सुरक्षा उपायों के कार्यान्वयन का डिजिटल बैंकिंग सेवाओं के प्रदर्शन पर नगण्य प्रभाव पड़ा (पी-वैल्यू = 0.228, 0.05 से अधिक, जिससे परिकल्पना को खारिज कर दिया गया)। हालांकि, उन्होंने पाया कि सुरक्षा नियंत्रण (पी-वैल्यू = 0.002, <0.05, एच2 का समर्थन करता है), ट्रेसिबिलिटी (पी-वैल्यू = 0.019, <0.05, एच4 का समर्थन करता है) और भेद्यता (पी-वैल्यू = 0.011, <0.05, एच5 का समर्थन करता है) की निगरानी का डिजिटल बैंकिंग प्रदर्शन पर महत्वपूर्ण प्रभाव पड़ा। सभी स्वीकृत परिकल्पनाओं में सकारात्मक गुणांक थे, जो डिजिटल बैंकिंग सेवाओं के प्रदर्शन के मूल्यांकन पर लाभकारी प्रभाव का संकेत देते हैं।

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

III. समीक्षाएँ और निष्कर्ष

लेखक (वर्ष)	संदर्भ/देश	फोकस/उद्देश्य	मुख्य निष्कर्ष
सर्विडियो और टेलर (2015)	संयुक्त राज्य अमेरिका (सामुदायिक बैंक)	सामुदायिक बैंकों के लिए साइबर सुरक्षा की तैयारी और रणनीति का आकलन करना	हमलों की आवृत्ति/परिष्कार में वृद्धि; छोटे बैंकों के पास संसाधनों की कमी; रणनीतिक ढांचे की आवश्यकता
प्रदीप (2015)	भारत	बैंकिंग पर आईटी प्रभाव और भारत में साइबर सुरक्षा की आवश्यकता का परीक्षण करें	साइबर अपराध अप्रत्याशित और बढ़ रहा है; डेटा संरक्षण के लिए नियामकीय आवश्यकता पर प्रकाश डाला गया
मल्होत्रा (2015)	संयुक्त राज्य अमेरिका (वीओआईपी नेटवर्क)	बैंकिंग में वीओआईपी के लिए एकीकृत साइबर जोखिम प्रबंधन ढांचा विकसित करना	खंडित मानकों की पहचान की गई; एकीकृत जोखिम प्रबंधन ढांचे का प्रस्ताव किया गया
मबेली और ड्वोलट्स्की (2016)	दक्षिण अफ्रीका	विश्लेषण करें और सुरक्षा संरचना का प्रस्ताव करें	बार-बार होने वाले साइबर हमले; अनुशंसित सीमा और अनुप्रयोग सुरक्षा वास्तुकला
कुशवाहा एट अल. (2016)	भारत	ऑनलाइन बैंकिंग में सूचना सुरक्षा, कानून, नैतिक मुद्दों की समीक्षा करें	गोपनीयता, अखंडता, उपलब्धता महत्वपूर्ण; सक्रिय सुरक्षा और विनियमन प्रभावी
गुप्ता एट अल. (2016)	वैश्विक	साइबर सुरक्षा हमलों और प्रतिवादों का सर्वेक्षण	साइबर खतरे विकसित हो रहे हैं; पहुंच नियंत्रण, एन्क्रिप्शन, घुसपैठ का पता लगाने की आवश्यकता है
अल्घाज़ो एट अल. (2017)	सऊदी अरब, पाकिस्तान, भारत	उपयोगकर्ता और बैंक के दृष्टिकोण से इंटरनेट बैंकिंग साइबर सुरक्षा का विश्लेषण करें	बैंक सुरक्षा अपेक्षाओं और उपभोक्ता व्यवहार के बीच अंतर; बैंक जिम्मेदारी बढ़ाने की आवश्यकता
अम्बोरे एट अल. (2017)	वैश्विक (एमएफएस)	मोबाइल वित्तीय सेवाओं के लिए सुदृढ़ साइबर सुरक्षा ढांचा विकसित करना	मोबाइल की कमज़ोरियाँ अपनाने में बाधा डालती हैं; प्रस्तावित लचीलापन ढांचा
हुसैन एट अल. (2017)	पाकिस्तान	ई-बैंकिंग कार्यान्वयन चुनौतियों और सुरक्षा प्रभाव की जांच करें	खराब इंटरनेट पहुंच और साइबर सुरक्षा के कारण ई-बैंकिंग में ग्राहकों का भरोसा कम हो रहा है

IJAMSR

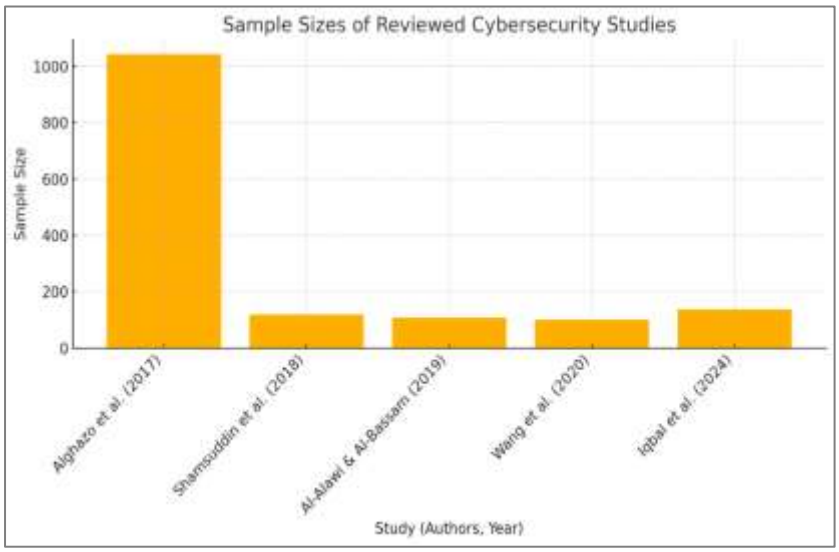
International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

दीप और शर्मा (2018)	भारत	मैलवेयर केस स्टडी का उपयोग करके भारत में साइबर खतरों का विश्लेषण करें	फ़िशिंग/मैलवेयर का प्रचलन; हनीपोट्स और निवारक तकनीक खतरों को कम करती है
शम्सुद्दीन एट अल. (2018)	मलेशिया	साइबर सुरक्षा के प्रबंधन में आंतरिक लेखापरीक्षा प्रभावशीलता का मूल्यांकन करें।	लेखा परीक्षक का ज्ञान, नीतियां और जोखिम प्रबंधन साइबर सुरक्षा प्रभावशीलता को दृढ़ता से प्रभावित करते हैं
महले एट अल. (2018)	वैश्विक (क्लाउड बैंकिंग)	बैंकिंग में क्लाउड कंप्यूटिंग डेटा गोपनीयता और सुरक्षा की जांच करें।	क्लाउड अपनाने से डेटा गोपनीयता जोखिम बढ़ता है; विनियामक अनुपालन महत्वपूर्ण है
अल-अलावी और अल-बस्सम (2019)	बहरीन	बैंकिंग में साइबर सुरक्षा जागरूकता को प्रभावित करने वाले कारकों की पहचान करें।	सुरक्षा अनुपालन को उच्च दर्जा दिया गया; संस्कृति सबसे कमजोर; जागरूकता के लिए सभी कारक प्रासंगिक
अधोलिया और अधोलिया (2019)	भारत (उदयपुर)	उपयोगकर्ताओं के बीच ई-बैंकिंग सुरक्षा जागरूकता का आकलन करें।	सामाजिक-आर्थिक कारक सुरक्षा जागरूकता को प्रभावित करते हैं; उपयोगकर्ता मजबूत जोखिम जागरूकता प्रदर्शित करते हैं
वांग एट अल. (2020)	नाइजीरिया	नाइजीरियाई इंटरनेट बैंकिंग में साइबर सुरक्षा उल्लंघनों और प्रथाओं का अध्ययन करें	परिष्कृत हमलों की ओर रुख; प्रशिक्षण पर्याप्त लेकिन तकनीक और अनुपालन का अभाव
पेरवेज़ एट अल. (2021)	वैश्विक	साइबर सुरक्षा के प्रकारों, रूपरेखाओं और चुनौतियों की व्यवस्थित समीक्षा।	साइबर सुरक्षा ढांचे और चुनौतियों का व्यापक अवलोकन
अलज़ौबी एट अल. (2022)	उभरती हुई अर्थव्यवस्था	डिजिटल बैंकिंग सुरक्षा खतरों और जागरूकता के स्तर की जांच करें	डिजिटल बैंकिंग में प्रमुख सुरक्षा खामियां; जोखिमों के बारे में उपयोगकर्ताओं की कम जागरूकता
अल-अलावी एट अल. (2023)	बहरीन	डिजिटल बैंकिंग के लिए साइबर सुरक्षा में महिलाओं की भूमिका और चुनौतियों का अन्वेषण करें।	साइबर सुरक्षा में सक्षम महिलाएं; करियर विकास के लिए समर्थन और प्रशिक्षण की आवश्यकता है
इकबाल एट अल. (2024)	पाकिस्तान	डिजिटल बैंकिंग प्रदर्शन पर सुरक्षा उपायों के प्रभाव का आकलन करें।	निगरानी, पता लगाने की क्षमता, भेद्यता प्रबंधन डिजिटल बैंकिंग प्रदर्शन पर सकारात्मक प्रभाव डालते हैं; बुनियादी उपाय कम प्रभावशाली होते हैं

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

IV. समीक्षाओं का नमूना आकार



चित्र 1: बैंकिंग में साइबर सुरक्षा पर पाँच अनुभवजन्य अध्ययन

बैंकिंग में साइबर सुरक्षा पर पाँच अनुभवजन्य अध्ययनों में नमूना आकार। अल्गाज़ो एट अल. (2017) 1,044 प्रतिभागियों के काफी बड़े नमूने के साथ सामने आया है, जो बैंकिंग ग्राहकों और वेबसाइटों से व्यापक सर्वेक्षण डेटा को दर्शाता है। इसके विपरीत, शम्सुद्दीन एट अल. (2018), अल -अलावी और अलबसम (2019), वांग एट अल. (2020), और इकबाल एट अल. (2024) प्रत्येक ने 100 से 140 उत्तरदाताओं के बीच एकत्र किया, जो छोटे, अधिक केंद्रित नमूनों (जैसे, आंतरिक लेखा परीक्षक या मोबाइल बैंकिंग उपयोगकर्ता) को दर्शाता है। यह असमानता बताती है कि अल्गाज़ो एट अल. के निष्कर्ष अधिक सामान्यीकरण प्रदान कर सकते हैं, जबकि अन्य अध्ययन बैंकिंग साइबर सुरक्षा के भीतर विशिष्ट हितधारक समूहों में अधिक लक्षित अंतर्दृष्टि प्रदान करते हैं।

V. निष्कर्ष

भारत के बैंकिंग क्षेत्र के तेजी से डिजिटल परिवर्तन ने पहुंच और परिचालन दक्षता में उल्लेखनीय सुधार किया है, लेकिन साथ ही साथ परिष्कृत साइबर खतरों के प्रति इसके जोखिम को भी बढ़ाया है। समीक्षा किए गए अध्ययनों में, आम चुनौतियाँ उभर कर सामने आती हैं: एक उभरता हुआ खतरा परिदृश्य जो स्थिर सुरक्षा ढाँचों से आगे निकल जाता है; विशेष रूप से छोटे बैंकों के बीच संसाधन की कमी जो उन्नत रक्षा तंत्रों की तैनाती में बाधा डालती है; और मानवीय कारक, जिसमें कर्मचारियों और ग्राहकों के बीच सीमित साइबर सुरक्षा जागरूकता शामिल है। भारतीय रिज़र्व बैंक और संबंधित कानून द्वारा विनियामक प्रयास एक आधारभूत अनुपालन आधार रेखा प्रदान करते हैं, फिर भी साक्ष्य बताते हैं कि अकेले अनुपालन लचीलापन सुनिश्चित करने

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

के लिए अपर्याप्त है। बैंकिंग में प्रभावी साइबर सुरक्षा एक समग्र दृष्टिकोण की मांग करती है जो सक्रिय खतरे की खुफिया जानकारी, निरंतर निगरानी और अनुकूली जोखिम प्रबंधन को मजबूत तकनीकी नियंत्रण जैसे कि मल्टी -फैक्टर ऑथेंटिकेशन, एन्क्रिप्शन और घुसपैठ का पता लगाने वाली प्रणालियों के साथ एकीकृत करता है। इसके अलावा, लक्षित प्रशिक्षण कार्यक्रमों और उपभोक्ता शिक्षा के माध्यम से साइबर सुरक्षा जागरूकता की संस्कृति को बढ़ावा देना सामाजिक इंजीनियरिंग जोखिमों को कम करने के लिए आवश्यक है। भविष्य के शोध को उभरती हुई सुरक्षा प्रौद्योगिकियों की वास्तविक -दुनिया की प्रभावकारिता का मूल्यांकन करने, तीसरे पक्ष और आपूर्ति श्रृंखला कमजोरियों का आकलन करने और संस्थागत साइबर लचीलापन मापने के लिए मीट्रिक विकसित करने पर ध्यान केंद्रित करना चाहिए। नीति, व्यवहार और उपयोगकर्ता व्यवहार के बीच मौजूदा अंतराल को पाटने के माध्यम से, भारतीय बैंक विश्वास को मजबूत कर सकते हैं, महत्वपूर्ण वित्तीय परिसंपत्तियों की सुरक्षा कर सकते हैं और सुरक्षित वातावरण में डिजिटल नवाचार की गति को बनाए रख सकते हैं।

संदर्भ

1. सर्विडियो, जेएस, और टेलर, आरडी (2015) । सुरक्षित और स्वस्थ: सामुदायिक बैंकों के लिए साइबर सुरक्षा। *जर्नल ऑफ टैक्सेशन एंड रेगुलेशन ऑफ फाइनेंशियल इंस्टीट्यूशंस, 28* (4) ।
2. प्रदीप, एम.डी. (2015) । बैंकिंग में सूचना प्रौद्योगिकी का प्रभाव-भारत में साइबर कानून और साइबर सुरक्षा। *इंटरनेशनल जर्नल ऑफ मैनेजमेंट, आईटी और इंजीनियरिंग, 5* (7), 2249-0558।
3. मल्होत्रा, वाई. (2015, अक्टूबर) । साइबर सुरक्षा पाठ्यक्रम और मानक विकास के लिए ब्रिजिंग नेटवर्क, सिस्टम और नियंत्रण रूपरेखा। *2015 एनवाई साइबर सुरक्षा और इंजीनियरिंग प्रौद्योगिकी एसोसिएशन सम्मेलन, अक्टूबर* (वॉल्यूम 22) में।
4. मेबेली, टीएम, और ड्वोलट्स्की , बी. (2016, जून)। साइबर सुरक्षा, दक्षिण अफ्रीका में साइबर बैंकिंग के लिए खतरा: नेटवर्क और एप्लिकेशन सुरक्षा के लिए एक दृष्टिकोण। *2016 में IEEE साइबर सुरक्षा और क्लाउड कंप्यूटिंग पर तीसरा अंतर्राष्ट्रीय सम्मेलन (CSCloud)* (पृष्ठ 1-6)। IEEE।
5. कुशवाह, पी.के., बिभु, वी., लोहानी, बी.पी., और सिंह, डी. (2016, फरवरी) । ऑनलाइन वित्तीय प्रणाली के साथ सूचना सुरक्षा, कानून और नैतिक मुद्दों पर समीक्षा। *2016 में साइबर सुरक्षा में नवाचार और चुनौतियों पर अंतर्राष्ट्रीय सम्मेलन (आईसीआईसीसीएस- आईएनबीयूएसएच)* (पृष्ठ 49-53) । आईईईई।

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

6. गुप्ता, एस., वशिष्ठ, एस., और सिंह, डी. (2016, फरवरी) । साइबर सुरक्षा हमलों और जवाबी उपायों पर एक कैनवस। *2016 में साइबर सुरक्षा में नवाचार और चुनौतियों पर अंतर्राष्ट्रीय सम्मेलन (ICICCS-INBUSH)* (पृष्ठ 31-35) । IEEE।
7. अल्गाज़ो, जे.एम., काज़मी, जेड., और लतीफ़, जी. (2017, नवंबर) । उभरते देशों में इंटरनेट बैंकिंग का साइबर सुरक्षा विश्लेषण: उपयोगकर्ता और बैंक के दृष्टिकोण। *2017 में इंजीनियरिंग प्रौद्योगिकी और अनुप्रयुक्त विज्ञान (ICETAS) पर 4th IEEE अंतर्राष्ट्रीय सम्मेलन* (पृष्ठ 1-6) । IEEE।
8. एम्बोरे, एस., रिचर्डसन, सी., डोगन, एच., एपेह, ई., और ओसेलटन, डी. (2017) । मोबाइल वित्तीय सेवाओं (एमएफएस) के लिए एक लचीला साइबर सुरक्षा ढांचा। *जर्नल ऑफ साइबर सिक्योरिटी टेक्नोलॉजी, 1* (3-4), 202-224।
9. हुसैन, जेड., दास, डी., भुट्टो, जेडए, हम्माद-उ-सलाम, एम., तालपुर, एफ., और राय, जी. (2017) । पाकिस्तान में ई-बैंकिंग चुनौतियां: एक अनुभवजन्य अध्ययन। *जर्नल ऑफ कंप्यूटर एंड कम्युनिकेशंस, 5* (2), 1-6।
10. दीप, वी., और शर्मा, पी. (2018, दिसंबर) । मज़ारबोट केस स्टडी का उपयोग करके भारत में साइबर सुरक्षा खतरों का विश्लेषण और प्रभाव । *2018 इंटरनेशनल कॉन्फ्रेंस ऑन कम्प्यूटेशनल टेक्निक्स, इलेक्ट्रॉनिक्स एंड मैकेनिकल सिस्टम्स (सीटीईएमएस) में* (पृष्ठ 499-503) । IEEE।
11. शम्सुद्दीन, ए., एडम, एम.ए., अदनान, एस.ए., मडज़लान, एस.एन.आई., और यासीन, वाई.एम. (2018) । मलेशिया के बैंकिंग संस्थानों में साइबर सुरक्षा के प्रबंधन में आंतरिक लेखापरीक्षा कार्यों की प्रभावशीलता। *इंटरनेशनल जर्नल ऑफ इंडस्ट्रियल मैनेजमेंट, 4*, 1-5।
12. महले, ए., योंग, जे., ताओ, एक्स., और शेन, जे. (2018, मई) । क्लाउड कंप्यूटिंग इंफ्रास्ट्रक्चर पर आधारित बैंकिंग और वित्तीय सेवा उद्योग के लिए डेटा गोपनीयता और सिस्टम सुरक्षा। *2018 IEEE 22वें इंटरनेशनल कॉन्फ्रेंस ऑन कंप्यूटर सपोर्टेड कोऑपरेटिव वर्क इन डिज़ाइन ((CSCWD))* (पृष्ठ 407-413) में। IEEE.
13. अल-अलावी, ए.आई., और अल-बस्सम, एस.ए. (2019) । बैंकिंग क्षेत्र में साइबर सुरक्षा जागरूकता के कारकों का आकलन। *अरब गल्फ जर्नल ऑफ साइंटिफिक रिसर्च, 37* (4), 17-32।
14. अधोलिया, ए., और अधोलिया, एस. (2019) । उदयपुर, राजस्थान के ई-बैंकिंग सेवा उपयोगकर्ताओं के बीच साइबर सुरक्षा प्रथाओं और युक्तियों के बारे में जागरूकता पर एक अध्ययन / *मल्टीडिसिप्लिनरी स्टडीज में अंतर्राष्ट्रीय जर्नल ऑफ साइंस रिसर्च, वॉल्यूम* 5 *(8)* ।

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

15. वांग, वी., ननाजी, एच., और जंग, जे. (2020) । नाइजीरिया में इंटरनेट बैंकिंग: साइबर सुरक्षा उल्लंघन, अभ्यास और क्षमता। *इंटरनेशनल जर्नल ऑफ लॉ, क्राइम एंड जस्टिस*, *62*, 100415।
16. परवेज, वाई., अब्बास, एसक्यू, दीक्षित, जेपी, अख्तर, एन., और जायसवाल, ए.के. (2021) । साइबर सुरक्षा पर एक व्यवस्थित साहित्य समीक्षा। *इंटरनेशनल जर्नल ऑफ साइंटिफिक रिसर्च एंड मैनेजमेंट*, *9* (12), 669-710।
17. अलज़ौबी, एचएम, ग़ज़ल, टीएम, हसन, एमके, अलकेटबी, ए., कामरान, आर., अल- डमौर, एनए, और इस्लाम, एस. (2022, मई) । डिजिटल बैंकिंग पर साइबर सुरक्षा खतरे। *2022 में साइबर सुरक्षा में एआई पर पहला अंतर्राष्ट्रीय सम्मेलन (ICAIC)* (पृष्ठ 1-4) । IEEE।
18. अल-अलावी, ए.आई., अल-खजा, एन.ए., और मेहरोत्रा, ए.ए. (2023) । साइबर सुरक्षा में महिलाएँ: बहरीन में डिजिटल बैंकिंग क्षेत्र का एक अध्ययन। *जर्नल ऑफ़ इंटरनेशनल विमेंस स्टडीज़*, *25* (1), 21।
19. इकबाल, एफ., नवाज, एस.ए., शाह, आर.ए., गुज्जर, ए.एम., एजाज, ए., दिलबर, जेड., और असलम, टी. (2024) । पाकिस्तान के डिजिटल बैंकिंग क्षेत्र में साइबर सुरक्षा उपायों का प्रभाव। *जर्नल ऑफ कंप्यूटिंग एंड बायोमेडिकल इंफॉर्मेटिक्स*।