

भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा खतरे: चुनौतियों, प्रभावों और सुरक्षा उपायों का विश्लेषण

पीएच.डी. (डॉक्टर ऑफ फिलॉसफी) उपाधि प्रदान किए जाने हेतु प्रस्तुत

डॉक्टर ऑफ फिलॉसफी (Ph.D.)

वाणिज्य विषय में

वाणिज्य संकाय के अंतर्गत

प्रस्तुतकर्ता

श्री राकेश कुमार राय

(नामांकन क्रमांक: 220101198)

शोध निर्देशन में

डॉ. शुभाशीष बासु

वाणिज्य विभाग

वाणिज्य संकाय

पी. के. विश्वविद्यालय

शिवपुरी (म० प्र०)



2026

पी. के. विश्वविद्यालय

शिवपुरी, म० प्र०, भारत – 473665

शोधार्थी का घोषणा पत्र

मैं यह घोषणा करता हूँ कि “**भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा खतरे: चुनौतियों, प्रभावों और सुरक्षा उपायों का विश्लेषण**” विषय पर प्रस्तुत यह शोध प्रबंध मेरा स्वयं का मौलिक कार्य है, जिसे मैंने डॉ शुभाशीष बासु के मार्गदर्शन में पी.के. विश्वविद्यालय (म.प्र.), भारत में, शोध उपाधि समिति द्वारा अनुमोदित विषय के अंतर्गत पूर्ण किया है।

मैं आगे यह भी घोषणा करता हूँ कि मेरे सर्वोत्तम ज्ञान के अनुसार इस शोध प्रबंध का कोई भी भाग किसी अन्य विश्वविद्यालय में किसी डिग्री/उपाधि की प्राप्ति हेतु प्रस्तुत नहीं किया गया है, और जहाँ भी अन्य स्रोतों का उपयोग किया गया है, वहाँ उचित संदर्भ दिया गया है।

शोधार्थी के हस्ताक्षर

दिनांक:

स्थान:



P.K. UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No 17 of 2015

पर्यवेक्षक का प्रमाण-पत्र

यह प्रमाणित किया जाता है कि “भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा खतरे: चुनौतियों, प्रभावों और सुरक्षा उपायों का विश्लेषण” विषय पर प्रस्तुत यह शोध कार्य राकेश कुमार राय द्वारा मेरे मार्गदर्शन एवं पर्यवेक्षण में संकाय वाणिज्य, पी.के. विश्वविद्यालय (म.प्र.), भारत से डॉक्टर ऑफ फिलॉसफी (Ph.D.) की उपाधि की प्राप्ति हेतु किया गया है।

मैं यह भी प्रमाणित करता हूँ कि शोधार्थी ने मेरे साथ 240 दिनों से अधिक की उपस्थिति दर्ज की है। मेरे सर्वोत्तम ज्ञान एवं विश्वास के अनुसार यह शोध प्रबंध:

- I. – शोधार्थी का स्वयं का मौलिक कार्य है।
- II. – विधिवत पूर्ण किया गया है।
- III. – विश्वविद्यालय के पी.एच.डी. उपाधि से संबंधित अध्यादेश की आवश्यकताओं को पूर्ण करता है।

पर्यवेक्षक के हस्ताक्षर

दिनांक:



P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No 17 of 2015

कॉपीराइट हस्तांतरण प्रमाण-पत्र

शोध प्रबंध का शीर्षक: “भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा खतरे: चुनौतियों, प्रभावों और सुरक्षा उपायों का विश्लेषण”

शोधार्थी का नाम: राकेश कुमार राय

कॉपीराइट हस्तांतरण

अधोहस्ताक्षरी द्वारा यह घोषित किया जाता है कि उपर्युक्त पी.एच.डी. उपाधि हेतु प्रस्तुत शोध प्रबंध के समस्त कॉपीराइट, जो इस शोध कार्य से संबंधित हैं, पी.के. विश्वविद्यालय, शिवपुरी को हस्तांतरित किए जाते हैं।

दिनांक:

(राकेश कुमार राय)

आभार

सर्वप्रथम मैं परमपिता परमात्मा को सादर नमन करता हूँ, जिनकी असीम कृपा एवं आशीर्वाद के बिना यह शोध-प्रबंध संभव नहीं था मैं अपने शोध कार्य की सफल पूर्णता के अवसर पर **पी.के. विश्वविद्यालय, शिवपुरी (मध्य प्रदेश)** के प्रति अपनी हार्दिक कृतज्ञता व्यक्त करता हूँ, जिसने मुझे इस शोध कार्य को सम्पन्न करने हेतु उपयुक्त शैक्षणिक वातावरण एवं संसाधन उपलब्ध कराए।

मैं विश्वविद्यालय के **माननीय कुलाधिपति श्री जगदीश प्रसाद शर्मा जी** के प्रति विशेष आभार व्यक्त करता हूँ, जिनके दूरदर्शी नेतृत्व एवं मार्गदर्शन ने एक उत्कृष्ट शैक्षणिक परिवेश का निर्माण किया। साथ ही, माननीय **कार्यकारी निदेशक डॉ. जे.के. मिश्रा जी** का मैं हृदय से धन्यवाद करता हूँ, जिनके प्रेरणादायक मार्गदर्शन एवं सतत सहयोग ने इस शोध कार्य को सफलतापूर्वक पूर्ण करने में महत्वपूर्ण भूमिका निभाई।

मैं **माननीय कुलपति डॉ. मुकेश चंसोरिया जी** का भी हार्दिक आभार व्यक्त करता हूँ, जिनके कुशल नेतृत्व एवं शैक्षणिक दृष्टिकोण ने शोध एवं नवाचार को प्रोत्साहित किया। इसके अतिरिक्त, **कुलसचिव डॉ. जितेन्द्र कुमार मलिक जी** का मैं सादर धन्यवाद करता हूँ, जिनके प्रशासनिक सहयोग एवं समन्वय से यह कार्य सुचारु रूप से सम्पन्न हो सका।

मैं **अकादमिक अधिष्ठाता डॉ. ऐमन फातमा जी** के प्रति अपनी विशेष कृतज्ञता प्रकट करता हूँ, जिनके मार्गदर्शन, प्रेरणा एवं सहयोग ने मेरे शोध कार्य को नई दिशा प्रदान की। साथ ही, वाणिज्य **संकायाध्यक्ष डॉ. ऐमन फातमा जी** का हार्दिक आभार व्यक्त करता हूँ, जिनके विद्वत्तापूर्ण मार्गदर्शन एवं सहयोग से मेरा शोध कार्य समृद्ध हुआ।

मैं अपने शोध मार्गदर्शक **डॉ. शुभाशीष बासु** के प्रति अपनी गहन कृतज्ञता व्यक्त करता हूँ, जिनके कुशल निर्देशन, अमूल्य मार्गदर्शन, निरंतर प्रेरणा एवं सतत सहयोग के बिना यह शोध कार्य पूर्ण होना संभव नहीं था। उनके विद्वत्तापूर्ण सुझावों एवं मार्गदर्शन ने मेरे शोध को सही दिशा प्रदान की।

अंततः, मैं शोध प्रकोष्ठ के **डॉ. मनीष कुमार जी** का भी सादर धन्यवाद करता हूँ, जिनके बहुमूल्य सुझावों एवं सहयोग ने इस शोध कार्य को सफलतापूर्वक पूर्ण करने में महत्वपूर्ण योगदान दिया।

अंत में, मैं अपने प्रिय पिता श्री बृज बिहारी राय एवं माता श्रीमति ललिता देवी, भाई ब्रजेश कुमार राय तथा मेरी धर्म पत्नी कुमारी आराधना का विशेष रूप से अभारी हूँ जिनके स्नेह, त्याग, आशीर्वाद एवं निरंतर प्रोत्साहन के बिना यह शोध कार्य संभव नहीं हो पाता। उनके नैतिक समर्थन एवं मार्गदर्शन ने मुझे हर कठिनाई में आगे बढ़ने की प्रेरणा दी।

मैं अपने **मित्रों, सहपाठियों एवं सभी रिश्तेदारों** का भी हृदय से धन्यवाद करता हूँ, जिन्होंने प्रत्यक्ष एवं अप्रत्यक्ष रूप से मेरे शोध कार्य में सहयोग प्रदान किया तथा कठिन समय में मेरा उत्साहवर्धन किया।

साथ ही, मैं अपने **प्रियजनों** के प्रति विशेष आभार व्यक्त करता हूँ, जिनके स्नेह, धैर्य एवं समझ ने मुझे इस शोध कार्य को सफलतापूर्वक पूर्ण करने की शक्ति प्रदान की।

मैं यह शोध-प्रबंध पूर्ण ईमानदारी एवं निष्ठा के साथ प्रस्तुत कर रहा हूँ। तथापि, यदि इसमें कहीं कोई त्रुटि या कमी रह गई हो, तो उसे मानवीय भूल मानते हुए क्षमा करने की कृपा करें।

दिनांक : _____

शोधार्थी

स्थान : _____

अनुक्रमाणिका

अध्याय 1 परिचय.....	1
1.1 अध्ययन की पृष्ठभूमि	1
1.2 साइबर सुरक्षा	8
1.2.1 बैंकिंग में साइबर सुरक्षा उपायों का अवलोकन	8
1.2.2 भारतीय बैंकिंग क्षेत्र और साइबर सुरक्षा	9
1.2.3 साइबर सुरक्षा चिंताओं के लिए बैंकिंग क्षेत्रों में एआई का कार्यान्वयन	10
1.2.4 साइबर सुरक्षा शब्दावली.....	11
1.3 साइबर अपराध	13
1.3.1 साइबर अपराध की विशेषताएं.....	16
1.3.2 वर्तमान और भविष्य में प्रौद्योगिकी का उपयोग.....	17
1.3.3 बैंकिंग उद्योग में साइबर अपराध	17
1.3.4 बैंकिंग क्षेत्र से जुड़े साइबर अपराध के प्रकार	18
1.3.5 बैंकों पर साइबर अपराध का प्रभाव	21
1.4 भारतीय बैंकिंग प्रणाली	23
1.4.1 बैंकिंग का अर्थ.....	23
1.4.2 वित्तीय लेनदेन का अर्थ	23
1.4.3 भारत में बैंकों का वर्गीकरण.....	24
1.4.4 भारत में बैंकिंग प्रणाली की संरचना	25
1.4.5 सार्वजनिक क्षेत्र के बैंक का अर्थ.....	27
1.4.6 निजी क्षेत्र के बैंक का अर्थ	28
1.4.7 विदेशी क्षेत्र बैंक का अर्थ	28
1.4.8 वित्तीय लेनदेन का प्रकार	29
1.5 साइबर सुरक्षा जोखिम और अनिश्चितता का नैतिक घटक	31
1.6 साइबर अपराध की दुनिया में प्रमुख रुझान और नवाचार	31
1.7 उद्देश्य	34
अध्याय 2 साहित्य की समीक्षा	35
अध्याय 3 अनुसंधान क्रियाविधि	73
3.1 अनुसंधान डिजाइन.....	73
3.2 डेटा संग्रह प्रक्रियाएं.....	73

3.3 डेटा संग्रहण के लिए उपकरण.....	74
3.4 नमूना डिजाइन.....	74
3.5 नमूनाकरण तकनीक / प्रक्रिया	75
3.6 नमूने का आकार	75
3.7 नमूनाकरण / जांच तकनीक	75
3.8 अध्ययन के लिए प्रयुक्त नमूना डिजाइन	75
3.9 डेटा विश्लेषण और परिकल्पना परीक्षण पूरा करना	76
3.10 सांख्यिकीय निष्कर्षों के लिए उपकरण कास्ट-ऑफ.....	76
अध्याय 4 डेटा विश्लेषण	77
4.1 ऑनलाइन खतरों से जुड़े जोखिम के बारे में उत्तरदाताओं की धारणा:.....	84
4.2 सभी लिंगों में साइबर सुरक्षा नियमों के बारे में जागरूकता:	90
4.3. सभी आयु वर्गों में साइबर सुरक्षा नियमों के बारे में जागरूकता:	91
4.4. शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता:.....	92
4.5. विभिन्न लिंगों के बीच एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन: ..	93
4.6. विभिन्न लिंगों के बीच नकद जमा के वित्तीय लेनदेन:	94
4.7. विभिन्न लिंगों के बीच नकद निकासी के वित्तीय लेनदेन	95
4.8 विभिन्न लिंगों के बीच एक खाते से दूसरे खाते में धन हस्तांतरण का वित्तीय लेनदेन:.....	96
4.9. विभिन्न लिंगों के बीच धन प्रेषण के वित्तीय लेनदेन:	98
4.10. विभिन्न लिंगों के बीच विदेशी मुद्रा का वित्तीय लेनदेन:	99
4.11. विभिन्न लिंगों के बीच प्रतिभूतियों का वित्तीय लेनदेन:	100
4.12. विभिन्न माध्यमों से एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन: .	101
4.13. विभिन्न आयु वर्गों में नकद जमा के वित्तीय लेनदेन:	103
4.14. विभिन्न आयु वर्गों में नकद निकासी के वित्तीय लेनदेन:.....	104
4.15. एक खाते से दूसरे खाते में विभिन्न अवधियों में धन हस्तांतरण के वित्तीय लेनदेन:.....	105
4.16. विभिन्न आयु वर्गों में धन प्रेषण के वित्तीय लेनदेन:	107
4.17. विभिन्न आयु वर्गों में विदेशी मुद्रा के वित्तीय लेनदेन:	108
4.18. विभिन्न आयु वर्गों की प्रतिभूतियों का वित्तीय लेनदेन:	109
4.19. शिक्षा क्षेत्र में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन.....	110
4.20. शिक्षा जगत में नकद जमा के वित्तीय लेनदेन:.....	112
4.21. शिक्षा जगत में नकद निकासी के वित्तीय लेनदेन:	114
4.22. शिक्षा जगत में एक खाते से दूसरे खाते में धन हस्तांतरण का वित्तीय लेनदेन:	116
4.23. शिक्षा के क्षेत्र में धन प्रेषण का वित्तीय लेनदेन:.....	118
4.24. शिक्षा के क्षेत्र में विदेशी मुद्रा का वित्तीय लेनदेन:.....	119

4.25. शिक्षा जगत में प्रतिभूतियों का वित्तीय लेनदेन:	121
4.26. विभिन्न लिंगों के ग्राहकों के विवरण जैसे मोबाइल नंबर, पता आदि को अद्यतन करने के गैर-वित्तीय लेनदेन:	122
4.27. विभिन्न लिंगों के खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन:	124
4.28. विभिन्न लिंगों में शेष राशि की जांच के गैर-वित्तीय लेनदेन:	125
4.29. विभिन्न लिंगों के बीच खाता विवरण मुद्रित करने के गैर-वित्तीय लेनदेन:	126
4.30. विभिन्न लिंगों के बीच चेक बुक/पासबुक जारी करने के गैर-वित्तीय लेनदेन:	128
4.31. विभिन्न लिंगों के बीच केवाईसी अद्यतन के गैर-वित्तीय लेनदेन:	129
4.32. आयु के आधार पर ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को अद्यतन करने के गैर-वित्तीय लेनदेन:	130
4.33. विभिन्न आयु वर्ग में खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन:	132
4.34. विभिन्न आयु वर्गों में शेष राशि की जांच के गैर-वित्तीय लेनदेन:	133
4.35. विभिन्न आयु वर्गों में खाता विवरण मुद्रित करने के गैर-वित्तीय लेनदेन:	134
4.36. विभिन्न आयु वर्ग के चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन:	136
4.37. विभिन्न आयु वर्गों में केवाईसी अद्यतन के गैर-वित्तीय लेनदेन:	137
4.38. ऑनलाइन लेनदेन में विभिन्न लिंगों के बीच ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में आने वाली चुनौतियाँ:	138
4.39. ऑनलाइन लेनदेन में डेटा सुरक्षा के रूप में विभिन्न लिंगों के समक्ष आने वाली चुनौतियाँ:	140
4.40. अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में विभिन्न लिंगों के समक्ष आने वाली चुनौतियाँ:	141
4.41. ऑनलाइन लेनदेन में भुगतान गेटवे चुनने में लिंग के आधार पर आने वाली चुनौतियाँ:	142
4.42. विभिन्न लिंगों के बीच बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	143
4.43. सभी लिंगों के लोगों के सामने डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	144
4.44. ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	145
4.45. ऑनलाइन लेनदेन में डेटा सुरक्षा के रूप में विभिन्न युगों में आने वाली चुनौतियाँ:	146
4.46. विभिन्न आयु वर्गों में अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	148
4.47. ऑनलाइन लेनदेन में भुगतान गेटवे चुनने में आने वाली चुनौतियाँ:	149
4.48. विभिन्न आयु वर्गों में बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	151
4.49. डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में विभिन्न आयु वर्गों में आने वाली चुनौतियाँ:	152

4.50. शिक्षा जगत में ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ.....	154
4.51. शिक्षा जगत में डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	156
4.52 शिक्षा के क्षेत्र में अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	157
4.53. शिक्षा जगत में भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	159
4.54 शिक्षा जगत में बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	160
4.55 शिक्षा जगत में डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:	162
4.56. लिंग के आधार पर ऑनलाइन सुरक्षा का महत्व:	164
4.57. आयु के आधार पर ऑनलाइन सुरक्षा का महत्व:	165
4.58 शिक्षा में ऑनलाइन सुरक्षा का महत्व:	167
4.59. लिंग के आधार पर डेटा सुरक्षा पर हमला:	169
4.60. सभी आयु वर्गों में डेटा सुरक्षा पर हमला:	170
4.61. शिक्षा जगत में डेटा सुरक्षा पर हमला:	171
4.62. मैलवेयर/लिंग-भेदभावपूर्ण गतिविधियों के विरुद्ध डेटा सुरक्षा:	173
4.63. मैलवेयर/विभिन्न आयु वर्गों की गतिविधियों के विरुद्ध डेटा सुरक्षा:	174
4.64. शिक्षा जगत में मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा:	175
अध्याय 5 निष्कर्ष	178
संदर्भ	184

तालिका सूचि

तालिका 4.1 लिंग.....	77
तालिका 4.2 आयु.....	77
तालिका 4.3 शिक्षा.....	78
तालिका 4. 4 उपकरणों का नियमित उपयोग.....	78
तालिका 4. 5 आपका पीसी किस ऑपरेटिंग सिस्टम (ओएस) का उपयोग करता है?	78
तालिका 4. 6 आपका फ़ोन किस ऑपरेटिंग सिस्टम का उपयोग करता है?.....	79
तालिका 4. 7 आपका टैबलेट किस ऑपरेटिंग सिस्टम (OS) का उपयोग करता है?.....	79
तालिका 4. 8 क्या आप पारंपरिक तरीकों की तुलना में ऑनलाइन लेनदेन को प्राथमिकता देते हैं?	80
तालिका 4. 9 आप कितनी बार ऑनलाइन लेनदेन करते हैं?	80
तालिका 4. 10 आप आमतौर पर किस प्रकार के ऑनलाइन लेनदेन को पसंद करते हैं?	80
तालिका 4. 11 इनमें से आपने कौन से गैर-वित्तीय लेनदेन किए हैं?	81
तालिका 4. 12 ऑनलाइन लेनदेन में आपको किन चुनौतियों का सामना करना पड़ता है?	82
तालिका 4. 13 यह भावना कि ऑनलाइन सुरक्षा महत्वपूर्ण है.....	83
तालिका 4. 14 ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?	83
तालिका 4. 15 ऑनलाइन लेनदेन करते समय क्या सुरक्षित रूप से साझा किया जा सकता है?	83
तालिका 4. 16 आपको ऑनलाइन खतरों से खतरा होने की भावना.....	84
तालिका 4. 17 आप जिन लोगों के लिए ज़िम्मेदार हैं (यानी परिवार के सदस्य) को ऑनलाइन खतरों से कितना जोखिम महसूस करते हैं	85
तालिका 4. 18 उत्तरदाता निम्नलिखित के बारे में चिंतित हैं?	85
तालिका 4. 19 उत्तरदाता निम्नलिखित के बारे में चिंतित हैं	85
तालिका 4. 20 मेलवेयर (वायरस, दुर्भावनापूर्ण/अवांछित प्रोग्राम, एडवेयर, आदि) पिछले बारह महीनों में उत्तरदाता के डिवाइस पर स्वयं इंस्टॉल होना	86
तालिका 4. 21 पिछले बारह महीनों में आपके कंप्यूटर में मौजूद वायरस को हटाने के लिए की गई कार्रवाई	86
तालिका 4. 22 डिवाइस को खतरों से बचाने के लिए की गई कार्रवाई	87
तालिका 4. 23 इनमें से आप कौन सी (यदि कोई हो) कार्रवाई करते हैं?	87
तालिका 4. 24 अपने डिवाइस की सुरक्षा के लिए कोई कार्रवाई न करना.....	88
तालिका 4. 25 यह सुनिश्चित करने के लिए उठाए गए कदम कि उत्तरदाताओं की ऑनलाइन उपस्थिति निजी बनी रहे अर्थात खाते सुरक्षित रहें।	89
तालिका 4. 26 गतिविधि / वे कार्रवाइें जो उत्तरदाता यह सुनिश्चित करने के लिए करते हैं कि उनकी ऑनलाइन उपस्थिति निजी रहे और खाता सुरक्षित रहे.....	89
तालिका 4. 27 साइबर सुरक्षा नियमों के बारे में लिंग के आधार पर जागरूकता	90
तालिका 4. 28 कार्रवाई-स्कायर परीक्षण	90
तालिका 4. 29 आयु वर्ग के अनुसार साइबर सुरक्षा नियमों के बारे में जागरूकता.....	91
तालिका 4. 30 कार्रवाई-स्कायर परीक्षण	91
तालिका 4. 31 शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता	92
तालिका 4. 32 कार्रवाई-स्कायर परीक्षण	93

तालिका 4. 33 विभिन्न लिंगों में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन	93
तालिका 4. 34 कार्ड-स्वायर परीक्षण	94
तालिका 4. 35 विभिन्न लिंगों में नकद जमा के वित्तीय लेनदेन	94
तालिका 4. 36 कार्ड-स्वायर परीक्षण	95
तालिका 4. 37 विभिन्न लिंगों में नकद निकासी के वित्तीय लेनदेन	95
तालिका 4. 38 कार्ड-स्वायर परीक्षण	96
तालिका 4. 39 विभिन्न लिंगों के बीच एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन	97
तालिका 4. 40 कार्ड-स्वायर परीक्षण	97
तालिका 4. 41 विभिन्न लिंगों में धन प्रेषण के वित्तीय लेनदेन	98
तालिका 4. 42 कार्ड-स्वायर परीक्षण	98
तालिका 4. 43 विभिन्न लिंगों में विदेशी मुद्रा के वित्तीय लेनदेन	99
तालिका 4.44 कार्ड-स्वायर परीक्षण	99
तालिका 4. 45 विभिन्न लिंगों में प्रतिभूतियों के वित्तीय लेनदेन	100
तालिका 4. 46 कार्ड-स्वायर परीक्षण	101
तालिका 4. 47 विभिन्न आयु वर्गों में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन	101
तालिका 4. 48 कार्ड-स्वायर परीक्षण	102
तालिका 4. 49 विभिन्न आयु वर्गों में नकद जमा के वित्तीय लेन-देन	103
तालिका 4. 50 कार्ड-स्वायर परीक्षण	104
तालिका 4. 51 आयु के अनुसार नकद निकासी के वित्तीय लेनदेन	104
तालिका 4. 52 कार्ड-स्वायर परीक्षण	105
तालिका 4. 53 विभिन्न आयु वर्गों में एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन	105
तालिका 4. 54 कार्ड-स्वायर परीक्षण	106
तालिका 4. 55 आयु के आधार पर धन प्रेषण के वित्तीय लेनदेन	107
तालिका 4. 56 कार्ड-स्वायर परीक्षण	107
तालिका 4. 57 आयु के आधार पर विदेशी मुद्रा के वित्तीय लेनदेन	108
तालिका 4. 58 कार्ड-स्वायर परीक्षण	109
तालिका 4. 59 विभिन्न आयु वर्गों में प्रतिभूतियों के वित्तीय लेनदेन	109
तालिका 4. 60 कार्ड-स्वायर परीक्षण	110
तालिका 4. 61 शिक्षा जगत में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन	111
तालिका 4. 62 कार्ड-स्वायर परीक्षण	112
तालिका 4. 63 शिक्षा जगत में नकद जमा के वित्तीय लेनदेन	112
तालिका 4. 64 कार्ड-स्वायर परीक्षण	114
तालिका 4. 65 शिक्षा जगत में नकद निकासी के वित्तीय लेनदेन	114
तालिका 4. 66 कार्ड-स्वायर परीक्षण	115
तालिका 4. 67 शिक्षा जगत में एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन	116
तालिका 4. 68 कार्ड-स्वायर परीक्षण	117
तालिका 4. 69 शिक्षा क्षेत्र में धन प्रेषण के वित्तीय लेनदेन	118
तालिका 4. 70 स्वायर परीक्षण के ग्रेड शून्य	119
तालिका 4. 71 शिक्षा जगत में विदेशी मुद्रा के वित्तीय लेनदेन	119

तालिका 4. 72 स्क्रायर परीक्षण का डोमिनो प्रभाव	120
तालिका 4.73 शिक्षा जगत में प्रतिभूतियों के वित्तीय लेनदेन.....	121
तालिका 4. 74 कार्ड-स्क्रायर परीक्षण	122
तालिका 4. 75 लिंग के आधार पर ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को अद्यतन करने के गैर-वित्तीय लेनदेन	123
तालिका 4. 76 कार्ड-स्क्रायर परीक्षण	123
तालिका 4. 77 लिंग के आधार पर खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन ...	124
तालिका 4. 78 कार्ड-स्क्रायर परीक्षण	124
तालिका 4. 79 लिंग के आधार पर शेष राशि की जांच के गैर-वित्तीय लेनदेन	125
तालिका 4. 80 कार्ड-स्क्रायर परीक्षण	126
तालिका 4. 81 लिंग के आधार पर खाता विवरण मुद्रित करने के गैर-वित्तीय लेन-देन.....	126
तालिका 4. 82 कार्ड-स्क्रायर परीक्षण	127
तालिका 4. 83 विभिन्न लिंगों के बीच चेक बुक/पासबुक जारी करने के गैर-वित्तीय लेनदेन.....	128
तालिका 4.84 कार्ड-स्क्रायर परीक्षण	128
तालिका 4. 85 लिंग के आधार पर केवाईसी अपडेट.....	129
तालिका 4. 86 कार्ड-स्क्रायर परीक्षण	130
तालिका 4. 87 लिंग के आधार पर ग्राहक विवरण.....	130
तालिका 4. 88 कार्ड-स्क्रायर परीक्षण	131
तालिका 4. 89 आयु के आधार पर खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन	132
तालिका 4. 90 कार्ड-स्क्रायर परीक्षण	133
तालिका 4. 91 आयु के अनुसार बैलेंस इंकायरी के गैर-वित्तीय.....	133
तालिका 4. 92 कार्ड-स्क्रायर परीक्षण	134
तालिका 4. 93 आयु के आधार पर खाता विवरण मुद्रित करने के गैर-वित्तीय लेन-देन	134
तालिका 4. 94 कार्ड-स्क्रायर परीक्षण	135
तालिका 4. 95 आयु के अनुसार चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेन-देन	136
तालिका 4. 96 कार्ड-स्क्रायर परीक्षण	137
तालिका 4. 97 आयु के अनुसार केवाईसी अपडेट के गैर-वित्तीय लेन-देन.....	137
तालिका 4. 98 कार्ड-स्क्रायर परीक्षण	138
तालिका 4. 99 लिंग के आधार पर ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन	138
तालिका 4. 100 कार्ड-स्क्रायर परीक्षण	139
तालिका 4. 101 लिंग के आधार पर डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति...	140
तालिका 4.102 कार्ड-स्क्रायर परीक्षण	140
तालिका 4. 103 लिंग के आधार पर ऑनलाइन लेनदेन में भुगतान गेटवे चुनने में आने वाली चुनौति ..	142
तालिका 4. 104 कार्ड-स्क्रायर परीक्षण.....	143
तालिका 4. 105 लिंग के आधार पर बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति.....	144
तालिका 4. 106 लिंग के आधार पर डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति.....	144
तालिका 4.107 ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति	145
तालिका 4. 108 कार्ड-स्क्रायर परीक्षण	146
तालिका 4. 109 विभिन्न आयु समूहों के लोगों द्वारा ऑनलाइन लेनदेन में डेटा सुरक्षा के रूप में आने वाली चुनौति.....	147

तालिका 4. 110	काई-स्कायर परीक्षण	147
तालिका 4. 111	विभिन्न आयु समूहों के लोगों द्वारा अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति	148
तालिका 4. 112	काई-स्कायर परीक्षण	149
तालिका 4. 113	ऑनलाइन लेनदेन में विभिन्न आयु समूहों के लिए भुगतान गेटवे चुनने में आने वाली चुनौति	149
तालिका 4. 114	काई-स्कायर परीक्षण	150
तालिका 4. 115	विभिन्न आयु समूहों के लोगों द्वारा बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति	151
तालिका 4. 116	काई-स्कायर परीक्षण	152
तालिका 4. 117	विभिन्न आयु समूहों में डिजिटल भुगतान विफलता रूप में ऑनलाइन लेनदेन में आने वाली चुनौति	152
तालिका 4. 118	काई-स्कायर परीक्षण	153
तालिका 4.119	शिक्षा के क्षेत्र में ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियों	154
तालिका 4. 120	काई-स्कायर परीक्षण	155
तालिका 4. 121	शिक्षा के क्षेत्र में डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति	156
तालिका 4. 122	काई-स्कायर परीक्षण	157
तालिका 4. 123	शिक्षा के क्षेत्र में अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति	157
तालिका 4. 124	काई-स्कायर परीक्षण	158
तालिका 4. 125	शिक्षा के क्षेत्र में भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति	159
तालिका 4. 126	काई-स्कायर परीक्षण	160
तालिका 4. 127	शिक्षा के क्षेत्र में बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति	161
तालिका 4. 128	काई-स्कायर परीक्षण	161
तालिका 4. 129	शिक्षा के क्षेत्र में डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति	162
तालिका 4. 130	काई-स्कायर परीक्षण	163
तालिका 4.131	लिंग के आधार पर ऑनलाइन सुरक्षा के महत्व	164
तालिका 4. 132	काई-स्कायर परीक्षण	165
तालिका 4. 133	विभिन्न आयु समूहों में ऑनलाइन सुरक्षा के महत्व	165
तालिका 4. 134	काई-स्कायर परीक्षण	166
तालिका 4. 135	शिक्षा के क्षेत्र में ऑनलाइन सुरक्षा के महत्व	167
तालिका 4.136	काई-स्कायर परीक्षण	168
तालिका 4. 137	डेटा सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) से जुड़े जोखिम कारक	169
तालिका 4. 138	संगति के माप	169
तालिका 4. 139	उत्तरदाताओं के लिए जिम्मेदार लोगों (उदाहरण के लिए, परिवार के सदस्यों) के लिए डेटा सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) में शामिल जोखिम कारक	170
तालिका 4. 140	संगति के माप	171
तालिका 4. 141	सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) से जुड़े जोखिम कारक	171
तालिका 4.142	संगति के माप	172

तालिका 4.143	मैलवेयर/लिंग-भेदभावपूर्ण गतिविधियों के विरुद्ध डेटा सुरक्षा.....	173
तालिका 4. 144	विभिन्न आयु वर्ग के लोगों के बीच मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा.....	174
तालिका 4. 145	शिक्षा जगत में मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा से संबंधित	175
तालिका 4. 146	संगति के माप.....	177

सार

साइबर-हमले लगातार विकसित हो रहे हैं और लगातार बढ़ रहे हैं तथा व्यापक हो रहे हैं। हमलावर अपनी रणनीति और तकनीकों में सुरक्षा टीमों की तुलना में तेज़ी से सुधार कर रहे हैं तथा उनके तरीके हर साल अधिक परिष्कृत होते जा रहे हैं। साइबर अपराधी तेज़ी से कॉर्पोरेट के रूप में कार्य कर रहे हैं, नए उत्पाद विकास दल और कुछ संगठन उनकी सेवाएँ दे रहे हैं या उन्हें अन्य आपराधिक गिरोहों के साथ एकीकृत कर रहे हैं। साइबर अपराध अन्य अपराधों की तुलना में अधिक लाभदायक है, इसलिए बैंकों को इसके विरुद्ध सुरक्षा बनाने में बहुत अधिक संसाधनों का निवेश करना जारी रखना चाहिए। यदि कॉर्पोरेट ग्राहक जानते हैं कि बैंक धोखाधड़ी और साइबर हमलों को रोकने के लिए प्रतिबद्ध है, तो बैंक में विश्वास बढ़ेगा तथा अच्छे संबंध स्थापित होंगे। साइबर अपराध से निपटने के लिए बैंकों को सिस्टम और लोगों में भारी निवेश करना चाहिए। चूंकि साइबर हमले लगातार बदल रहे हैं, इसलिए वित्तीय संस्थानों को साइबर अपराधों के विरुद्ध सुरक्षा की स्थायी रूप से निगरानी करने की आवश्यकता है, यह सुनिश्चित करते हुए कि साइबर हमलों से निपटने के उपाय तेज़ी से परिष्कृत होते जा रहे हैं। इसलिए, यह शोध समीक्षाओं, लेखों, साक्षात्कारों और केस स्टडी के माध्यम से वर्तमान साइबर सुरक्षा योजनाओं और अवधारणाओं का अध्ययन करने के लिए किया गया है। इसका उद्देश्य उपयोगकर्ताओं के बीच साइबर सुरक्षा और इसके नियमों के बारे में जागरूकता पैदा करना है। इसने यह मूल्यांकन करने का प्रयास किया है कि कितने लोग ऑनलाइन लेनदेन करते समय वास्तव में साइबर सुरक्षा नियमों का उपयोग कर रहे हैं। इसमें उपयोगकर्ताओं के बीच वित्तीय और गैर-वित्तीय लेनदेन के उपयोग और साइबर हमलों को नियंत्रित करने के लिए भारत सरकार द्वारा की गई पहल जैसे पहलुओं को भी शामिल करने का प्रयास किया गया।

संक्षिप्ताक्षर

संक्षिप्ताक्षर	पूर्ण रूप
AI	कृत्रिम बुद्धिमत्ता
ML	मशीन अधिगम
DL	गहन अधिगम
ANN	कृत्रिम तंत्रिका नेटवर्क
NLP	प्राकृतिक भाषा प्रसंस्करण
RBI	भारतीय रिज़र्व बैंक
NPCI	भारतीय राष्ट्रीय भुगतान निगम
UPI	एकीकृत भुगतान इंटरफ़ेस
IMPS	त्वरित भुगतान सेवा
NEFT	राष्ट्रीय इलेक्ट्रॉनिक निधि अंतरण
RTGS	वास्तविक समय सकल निपटान
ATM	स्वचालित टेलर मशीन
OTP	एक बार प्रयुक्त होने वाला कूटशब्द
PIN	व्यक्तिगत पहचान संख्या
KYC	अपने ग्राहक को जानिए
MFA	बहु-कारक प्रमाणीकरण
VPN	आभासी निजी नेटवर्क

IDS	घुसपैठ पहचान प्रणाली
IPS	घुसपैठ रोकथाम प्रणाली
SIEM	सुरक्षा सूचना एवं घटना प्रबंधन
CERT-In	भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल
NCIIPC	राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र
CISO	मुख्य सूचना सुरक्षा अधिकारी
DDoS	वितरित सेवा-अस्वीकरण हमला
DoS	सेवा-अस्वीकरण हमला
SQL	संरचित प्रश्न भाषा
SQLI	एसक्यूएल इंजेक्शन हमला
XSS	क्रॉस-साइट स्क्रिप्टिंग
MITM	मध्यस्थ हमला
IoT	वस्तुओं का इंटरनेट
OS	प्रचालन तंत्र
URL	एकसमान संसाधन स्थान सूचक
IP	इंटरनेट प्रोटोकॉल
TCP/IP	संचरण नियंत्रण प्रोटोकॉल / इंटरनेट प्रोटोकॉल

SSL	सुरक्षित सॉकेट स्तर
TLS	परिवहन स्तर सुरक्षा
AES	उन्नत कूटलेखन मानक
PKI	सार्वजनिक कुंजी अवसंरचना
IT	सूचना प्रौद्योगिकी
ICT	सूचना एवं संचार प्रौद्योगिकी
GDP	सकल घरेलू उत्पाद
WHO	विश्व स्वास्थ्य संगठन
ISO	अंतरराष्ट्रीय मानकीकरण संगठन
NIST	राष्ट्रीय मानक एवं प्रौद्योगिकी संस्थान

अध्याय 1 परिचय

इस अध्याय में अध्ययन की पृष्ठभूमि, उद्देश्य तथा शोध की आवश्यकता को स्पष्ट किया गया है। इसमें वैश्विक और भारतीय बैंकिंग प्रणाली में तेजी से बढ़ते डिजिटलीकरण के साथ उत्पन्न साइबर सुरक्षा खतरों का विस्तृत वर्णन किया गया है। साथ ही, साइबर अपराधों के प्रकार, उनके प्रभाव, बैंकिंग संरचना तथा तकनीकी विकास के कारण उत्पन्न जोखिमों को समझाया गया है। यह अध्याय शोध के लिए आधार तैयार करता है और यह दर्शाता है कि क्यों साइबर सुरक्षा आज के बैंकिंग क्षेत्र में एक महत्वपूर्ण मुद्दा बन चुका है।

1.1 अध्ययन की पृष्ठभूमि

वैश्विक वित्तीय परिदृश्य में चुनौतियों की एक निरंतर विकसित श्रृंखला सामने आ रही है, जिसमें परिचालन संबंधी कमियाँ, बाजार में अस्थिरता, भू-राजनीतिक अनिश्चितताएँ, साइबर सुरक्षा खतरे और विनियामक अनुपालन और ऋण स्तरों पर आशंकाएँ शामिल हैं। इन जोखिमों में वित्तीय संकटों को ट्रिगर करने, बाजार में व्यवधान पैदा करने और वैश्विक आर्थिक विकास को प्रभावित करने की अलग-अलग डिग्री की क्षमता होती है। वित्तीय संस्थानों, नियामकों और बाजार के खिलाड़ियों को इस बदलते माहौल में सतर्क और अनुकूलनशील रहना चाहिए। इन खतरों को संबोधित करने और कम करने के लिए, सक्षम जोखिम प्रबंधन, नियामक निरीक्षण, तकनीकी नवाचार और अंतर्राष्ट्रीय सहयोग महत्वपूर्ण घटक हैं।

वर्तमान में, साइबर सुरक्षा सभी संगठनों के लिए एक बढ़ती चुनौती है। पिछले वर्ष में, यह स्पष्ट हो गया है कि बैंकिंग क्षेत्र में इसके बुनियादी ढांचे और साइबर सुरक्षा उपायों में कई कमियाँ थीं।

डिजिटल परिवर्तन ने बैंकिंग उद्योग को मौलिक रूप से बदल दिया है, जिसके परिणामस्वरूप दक्षता में वृद्धि हुई है, पहुँच में विस्तार हुआ है और ग्राहकों के लिए बेहतर अनुभव हुआ है। फिर भी, इस तेज़ डिजिटलीकरण ने साइबर खतरों को भी बढ़ा दिया है, जिससे वित्तीय संगठनों के लिए साइबर सुरक्षा एक सर्वोपरि मुद्दा बन गई है। वर्तमान में, बैंकों को मैलवेयर हमलों, फ़िशिंग, पहचान की चोरी, रैनसमवेयर, अवैध डेटा उल्लंघनों और साइबर अपराध के तेजी से उन्नत प्रकारों सहित कई खतरों का सामना करना पड़ता है। ये कमज़ोरियाँ संस्थानों की वित्तीय व्यवहार्यता को खतरे में डालती हैं, उपभोक्ता विश्वास को कम करती हैं और राष्ट्रीय आर्थिक सुरक्षा के लिए व्यापक प्रभाव डालती हैं। एन्क्रिप्शन, मल्टी-फ़ैक्टर प्रमाणीकरण और रीयल-टाइम खतरे का पता

लगाने जैसे परिष्कृत सुरक्षा उपायों को अपनाने के बावजूद, बैंक अपने द्वारा संभाली जाने वाली संवेदनशील जानकारी के पर्याप्त मूल्य के कारण प्राथमिक लक्ष्य बने हुए हैं। कमज़ोर साइबर सुरक्षा अवसंरचना, अंदरूनी खतरे और अपर्याप्त उपयोगकर्ता ज्ञान इन कठिनाइयों को बढ़ाते हैं, जबकि हैकर्स की बदलती रणनीतियाँ मौजूदा सुरक्षा उपायों की प्रभावशीलता को कम करती हैं।

इन पारंपरिक जोखिमों के अलावा, ऑनलाइन बैंकिंग से जुड़े कई उभरते खतरे तत्काल ध्यान देने की मांग करते हैं। उदाहरण के लिए, मोबाइल बैंकिंग एप्लिकेशन का व्यापक रूप से अपनाया जाना, उपयोगकर्ताओं को कम से कम सुरक्षा उपायों के साथ काम करने पर बढ़ी हुई कमज़ोरियों के प्रति उजागर करता है, जिससे अनधिकृत पहुँच और धोखाधड़ी का जोखिम काफी बढ़ जाता है। इसके अलावा, जैसे-जैसे बैंक अपने आंतरिक बचाव को मजबूत करते हैं, साइबर अपराधी तीसरे पक्ष के नेटवर्क और साझा बैंकिंग सिस्टम को तेज़ी से निशाना बना रहे हैं, जिनमें अक्सर मजबूत सुरक्षा उपायों की कमी होती है, जिससे हमलों के लिए आसान प्रवेश बिंदु बन जाते हैं। तेज़ी से बढ़ता क्रिप्टोकॉरेसी बाज़ार इन चुनौतियों को और भी जटिल बनाता है; इस क्षेत्र में नवजात विनियामक ढाँचा और तकनीकी नवाचार की तेज़ गति साइबर हमलों के लिए अवसर पैदा करती है जो सुरक्षा खामियों का फ़ायदा उठाते हैं। ये बहुआयामी जोखिम अभिनव साइबर सुरक्षा रणनीतियों की तत्काल आवश्यकता को उजागर करते हैं जो गतिशील खतरे के परिदृश्य के अनुकूल हो सकते हैं और डिजिटल बैंकिंग पारिस्थितिकी तंत्र की सुरक्षा कर सकते हैं।

जबकि व्यापक शोध ने बैंकिंग क्षेत्र के डिजिटल परिवर्तन का दस्तावेजीकरण किया है और व्यक्तिगत साइबर सुरक्षा खतरों की पहचान की है - जैसे कि मैलवेयर, फ़िशिंग और रैनसमवेयर हमले - एकीकृत अध्ययनों में एक उल्लेखनीय अंतर बना हुआ है जो वर्तमान प्रतिवादों के साथ मिलकर इन जोखिमों का समग्र रूप से मूल्यांकन करता है। कई मौजूदा अध्ययन अलग-अलग पहलुओं पर ध्यान केंद्रित करते हैं, जैसे कि मोबाइल बैंकिंग अनुप्रयोगों में कमज़ोरियाँ या तीसरे पक्ष के नेटवर्क में कमज़ोरियाँ, लेकिन वे अक्सर इन खतरों के बीच परस्पर निर्भरता और समग्र बैंकिंग सुरक्षा पर संचयी प्रभाव को अनदेखा करते हैं। इसके अतिरिक्त, उभरते जोखिम, जैसे कि तेज़ी से विकसित हो रहे क्रिप्टोकॉरेसी परिदृश्य और AI-संचालित साइबर हमलों से संबंधित, कम खोजे गए हैं, विशेष रूप से भारत जैसी विकासशील अर्थव्यवस्थाओं के संदर्भ में, जहाँ नियामक ढाँचे और संसाधन की कमी अनूठी चुनौतियाँ पेश करती हैं।

इसके अलावा, हालांकि उन्नत सुरक्षा प्रोटोकॉल (जैसे, एन्क्रिप्शन, मल्टी-फैक्टर ऑथेंटिकेशन, रियल-टाइम खतरे का पता लगाना) को व्यापक रूप से लागू किया गया है, लेकिन परिष्कृत और गतिशील साइबर अपराधी रणनीति के खिलाफ इन उपायों की प्रभावशीलता को अपर्याप्त रूप से संबोधित किया गया है। व्यापक शोध की आवश्यकता है जो न केवल बैंकिंग क्षेत्र में साइबर सुरक्षा प्रथाओं की वर्तमान स्थिति का गंभीर रूप से आकलन करे बल्कि उभरते खतरों का मुकाबला करने के लिए अभिनव, अनुकूली रणनीतियों की भी खोज करे। इस तरह के शोध तकनीकी, संगठनात्मक और नियामक दृष्टिकोणों को एकीकृत करके अंतर को पाटेंगे, अंततः एक अधिक मजबूत और लकाईले डिजिटल बैंकिंग बुनियादी ढांचे में योगदान देंगे।

प्रौद्योगिकी हमारे जीवन के विभिन्न क्षेत्रों में महत्वपूर्ण भूमिका निभाती है, खासकर बैंकिंग क्षेत्र में। प्रौद्योगिकी ने बैंकिंग क्षेत्र और वित्तीय सेवा संस्थानों को प्रभावी ढंग से बढ़ाया है। प्रौद्योगिकी में आश्चर्यजनक विकास ने बैंकिंग क्षेत्र के काम करने के तरीके में एक मौलिक मोड़ लाया, जिसने बैंकिंग संस्थानों को ग्राहकों को प्रदान की जाने वाली सेवाओं के स्तर को बढ़ाने और सुधारने की दिशा में कई अवसर प्रदान किए। आजकल, प्रौद्योगिकी ने बैंकों और वित्तीय सेवा संस्थानों को इलेक्ट्रॉनिक लेनदेन के माध्यम से बैंकिंग और वित्तीय सेवाएं प्रदान करने में योगदान दिया है, जिससे समय, प्रयास और धन की बचत होती है।

बैंकिंग क्षेत्र में प्रौद्योगिकी द्वारा पैदा किए गए अवसरों और संभावनाओं के बावजूद, यह बैंकिंग क्षेत्र और वित्तीय सेवा संस्थानों के लिए एक विशेष चुनौती भी प्रस्तुत करती है। हम सभी जानते हैं कि प्रौद्योगिकी के दुर्भावनापूर्ण उपयोग से बैंकों और वित्तीय सेवा संस्थानों के बुनियादी ढांचे में व्यवधान, सुरक्षा का उल्लंघन, ग्राहक विश्वास, वित्तीय स्थिरता को खतरे में डालना और अन्य साइबर अपराध होते हैं। सूचना सुरक्षा उल्लंघन कभी भी अचानक हो सकता है क्योंकि सब कुछ इंटरनेट के साथ एकीकृत है और साइबर अपराधी जो बैंकों और वित्तीय सेवा संस्थानों की इंटरनेट कार्डों में हेरफेर कर रहे हैं, वे बैंकों के ग्राहक डेटा को हैक करने और वित्तीय संस्थानों के ग्राहकों के पैसे को डिजिटल रूप से चुराने में सक्षम हैं।

बैंकिंग क्षेत्र में प्रौद्योगिकी के महत्वपूर्ण विकास के साथ, प्रौद्योगिकी से जुड़े जोखिम भी बढ़ गए हैं। इसलिए, बैंकिंग क्षेत्र के संबंध में हर दिन कई प्रकार और रूप में साइबर सुरक्षा हमले/खतरे सामने आते हैं। साइबर सुरक्षा हमले पूरे वित्तीय तंत्र के लिए खतरा पैदा करते हैं, इस तथ्य की पुष्टि अंतर्राष्ट्रीय, क्षेत्रीय और स्थानीय स्तर पर इस संबंध में जारी रिपोर्टों से होती है। इस संदर्भ में,

विश्व बैंक की रिपोर्ट बैंकिंग क्षेत्र और वित्तीय सेवा संस्थानों में साइबर सुरक्षा हमलों की एकाग्रता का संकेत देती है, जिसमें 2016 में साइबर सुरक्षा हमलों में 65% की उल्लेखनीय वृद्धि देखी गई, जो पिछले वर्ष की तुलना में 29% की वृद्धि को दर्शाता है। इसके अलावा, वैश्विक बैंक की रिपोर्ट बताती है कि मैलवेयर का उपयोग करके वित्तीय क्षेत्र के खिलाफ चोरी पिछले वर्ष की तुलना में 2015 में प्रति वर्ष 80% बढ़ी है, जबकि इन हमलों में 2015 में रिपोर्ट की गई घटनाओं का 38% हिस्सा था, जो 2014 में 23% था।

2013 के अंत में साइबर अपराधियों के एक बहुराष्ट्रीय गिरोह का उदय (नजफ़ एट अल., 2021) जिसने दुनिया भर में बैंकिंग संस्थाओं के खिलाफ़ 100 से ज़्यादा परिष्कृत साइबर सुरक्षा हमलों की एक श्रृंखला को अंजाम दिया। ये हमले साइबर अपराधियों द्वारा "कार बैंक" हमलों का उपयोग करके बैंक कर्मचारियों को धोखाधड़ी वाले प्रतिक्रिया ईमेल भेजकर किए जाते हैं ताकि बैंक सिस्टम को कस्टमाइज़ किए गए मैलवेयर से संक्रमित किया जा सके जिसमें बैंक कर्मचारियों की गतिविधियों को कैप्चर करने के लिए वीडियो फ़ाइलें होती हैं। साइबर अपराध वित्तीय संस्थानों के सामने आने वाली मुख्य चुनौतियों में से एक है क्योंकि इससे पैसे की चोरी, संवेदनशील डेटा का रिसाव और महत्वपूर्ण वित्तीय नुकसान होता है। वित्तीय संस्थानों के सामने आने वाले साइबर अपराध पर चर्चा करने के लिए ग्रुप आईबी विशेषज्ञों के आकलन के आधार पर, वित्तीय संस्थानों के सामने आने वाले लगभग 99% साइबर अपराध पैसे की चोरी हैं, जिसने 2017 में कई कंपनियों को बर्बाद कर दिया, जैसे कि MDLZ और DLA Piper, पहचान की चोरी के अलावा, और इक्विफ़ैक्स उन पीड़ितों में से एक था जहाँ साइबर अपराधी संवेदनशील व्यक्तिगत जानकारी का उपयोग करते हैं और इसका उपयोग पहचान की चोरी के लिए करते हैं। 2018 में, विश्व आर्थिक मंच ने धोखाधड़ी और वित्तीय अपराधों पर ध्यान दिया, जिनकी राशि इस वर्ष एक ट्रिलियन डॉलर थी, जिसने निजी कंपनियों को 2017 में धन शोधन अपराधों से निपटने पर लगभग 8.2 बिलियन डॉलर खर्च करने के लिए प्रेरित किया।

धोखाधड़ी के अपराधों के परिणामस्वरूप बैंकों और वित्तीय संस्थानों को लगभग 3 डॉलर का नुकसान हुआ, जो धोखाधड़ी करने वाले संगठन के हर डॉलर के लिए है। वित्तीय संस्थान (FI) किसी भी अन्य उद्योग की तुलना में तीन गुना अधिक साइबर हमलों का लक्ष्य हैं। मोबाइल बैंकिंग और एटीएम वित्तीय संस्थानों को साइबर हमलों के प्रति अधिक संवेदनशील बनाते हैं। दुर्भाग्यपूर्ण साइबर हमलावरों के बीच वित्तीय संस्थानों पर हमला करने के लिए आंतरिक प्रेरणाएँ बहुत भिन्न होती हैं। साइबर अपराधी तेजी से बैंक नेटवर्क पर सीधे हमला कर रहे हैं। प्रत्येक

हमले के परिणामस्वरूप प्रत्येक बैंक को \$2.5 मिलियन से \$10 मिलियन तक का वित्तीय नुकसान हुआ है।

वित्तीय संस्थानों को साइबर खतरे की खुफिया जानकारी के संग्रह, विश्लेषण और साझाकरण में निरंतर निवेश को प्राथमिकता देनी चाहिए। अपने स्वयं के नेटवर्क की सुरक्षा के लिए उपाय करके और दूसरों के साथ ज्ञान साझा करके, वे व्यापक पैमाने पर साइबर हमलों के खतरे को कम करने में मदद कर सकते हैं। इसके लिए संस्थागत स्तर पर साइबर हमलों के बढ़ते जोखिम को दूर करने के लिए समय, धन और संसाधनों की निरंतर प्रतिबद्धता की आवश्यकता होती है। वेरिजोन 2017 डेटा ब्रीच इन्वेस्टिगेशन रिपोर्ट के अनुसार, सर्वेक्षण की गई आधी से अधिक फर्म शीर्ष पाँच साइबर खतरों से प्रभावित थीं: सेवा से इनकार (DoS), फ़िशिंग, मैलवेयर, स्पीयर फ़िशिंग और रैनसमवेयर। रिपोर्ट में यह भी पाया गया कि सभी सुरक्षा घटनाओं में से 88 प्रतिशत से अधिक तीन मुख्य हमले पैटर्न से उपजी हैं: DoS, वेब एप्लिकेशन हमले और क्रेडिट कार्ड स्किमिंग। भारत में, फ़िशिंग, पहचान की चोरी और मैलवेयर बैंकिंग क्षेत्र में सबसे प्रचलित अपराध हैं, जो अक्सर छोटी-छोटी गलतियों और साइबर सुरक्षा नीतियों के बारे में जागरूकता की कमी से बढ़ जाते हैं। सार्वजनिक क्षेत्र के बैंकों को सुरक्षा बढ़ाने, सार्वजनिक-निजी भागीदारी का लाभ उठाने और डेटा सुरक्षा के लिए धन बढ़ाने के लिए अधिक संसाधन आवंटित करने चाहिए। 2020 तक, वैश्विक ऑनलाइन बैंकिंग उपयोगकर्ता आधार 2 बिलियन तक पहुँचने का अनुमान है, जो 2017 में 1 बिलियन से दोगुना है - 2018 में निर्धारित समय से दो साल पहले हासिल किया गया एक मील का पथर। 2015 और 2017 के बीच, वित्तीय संस्थानों को लक्षित करने वाले साइबर-मध्यस्थ सुरक्षा उल्लंघनों में 30% से अधिक की वृद्धि हुई। नाइजीरिया में, इंटरनेट बैंकिंग की बढ़ती लोकप्रियता ने वित्तीय संस्थानों को कंप्यूटर तकनीक पर तेजी से निर्भर बना दिया है।

साइबर सुरक्षा का उल्लंघन इस उद्योग के लिए सबसे गंभीर खतरों में से एक बन गया है। साइबर अपराध और सुरक्षा सर्वेक्षण रिपोर्ट के अनुसार, मैलवेयर, फ़िशिंग, कंप्यूटर चोरी और बॉट हमले साइबर हमलों के लिए प्रचलित रणनीति हैं। तंजानिया ने कई साइबर अपराध घटनाओं के परिणामस्वरूप \$6 मिलियन का नुकसान उठाया है, जिससे देश को CCU और CERT बनाने के लिए मजबूर होना पड़ा है। आभासी दुनिया में गोपनीयता की रक्षा के लिए, नए सुरक्षा उपायों की आवश्यकता है। वांग एट अल., (2020) चार घटकों के माध्यम से साइबरनेटिक रक्षात्मक चक्र को प्राप्त करने के लिए साइबर-हमला प्रबंधन समाधान प्रदान करता है। साइबर हमले और जोखिम चिंता का एक प्रमुख स्रोत बन गए हैं। महत्वपूर्ण खोज यह थी कि चाहे कोई भी मजबूत

हमला हो, इराकी निजी बैंक एक निश्चित स्तर की सुरक्षा बनाए रखते हैं। इराक की अपर्याप्त सुरक्षा के कारण, कुछ उत्तरदाता अभी भी इंटरनेट बैंकिंग सेवाओं का उपयोग करने में संकोच कर रहे हैं। आतंकवाद के प्रभाव औद्योगिक और विकासशील देशों में भिन्न प्रतीत होते हैं, जो उस देश की विशेषताओं पर निर्भर करता है जहाँ घटना हुई थी। अधिक आरंभिक आर्थिक वृद्धि दर वाले देशों की तुलना में, कम आर्थिक वृद्धि दर वाले देशों को आतंकवाद के प्रति अधिक संवेदनशील माना जाता है। लोकतंत्र की कमी और अरब वसंत के बाद का माहौल MENA क्षेत्र में घरेलू और अंतरराष्ट्रीय आतंकवाद के प्रमुख कारक हैं। MENA क्षेत्र में आतंकवादी हमले तब अधिक गंभीर आर्थिक प्रभाव डालते हैं जब वे महत्वपूर्ण आर्थिक क्षेत्रों को निशाना बनाते हैं। जब हम 2015 में यूके में ऑनलाइन बैंकिंग में खोए गए धन की मात्रा की तुलना 2014 में खोए गए धन से करते हैं, तो खोए गए धन की मात्रा में महत्वपूर्ण अंतर होता है।

बैंकिंग सिस्टम में कई सुरक्षा मुद्दे हैं, जिससे बहुत सारा पैसा खो जाता है। 2019 में रिमोट बैंकिंग धोखाधड़ी वित्तीय धोखाधड़ी का सबसे आम प्रकार था; हालाँकि अन्य प्रकार के वित्तीय अपराध में कार्ड भुगतान धोखाधड़ी शामिल है। वर्ष 2019 में, यूनाइटेड किंगडम में अपराधियों ने लगभग 1.28 बिलियन पाउंड चुराए। क्रेडिट कार्ड धोखाधड़ी खाते।

सभी वित्तीय धोखाधड़ी के लगभग आधे के लिए। बैंकिंग प्रोटोकॉल के माध्यम से, बैंक शाखा कर्मियों ने 2020 की पहली छमाही में 19 मिलियन पाउंड की धोखाधड़ी को रोकने के लिए पुलिस के साथ सहयोग किया। बैंकिंग प्रोटोकॉल एक यूके-व्यापी कार्यक्रम है जो बैंक शाखा के कर्मचारियों को अपने स्थानीय पुलिस एजेंसी को सूचित करने की अनुमति देता है यदि उन्हें लगता है कि किसी ग्राहक को धोखा दिया जा रहा है। फिर पुलिस कथित धोखाधड़ी की जांच करने के लिए शाखा में जाएगी और परिसर में अभी भी मौजूद किसी भी संदिग्ध को पकड़ लेगी। जनवरी और जून 2020 के बीच, इस पहल ने धोखाधड़ी में 19.3 मिलियन पाउंड बचाए और 100 से अधिक गिरफ्तारियां हुईं। सबसे हालिया आंकड़ों के अनुसार, इस पहल ने पीड़ितों को धोखाधड़ी में 116 मिलियन पाउंड बचाए हैं। फ्रिशिंग में सबसे हालिया विकास एक ट्रोजन हॉर्स मैलवेयर का रोजगार है अक्टूबर और दिसंबर 2015 के महीनों के दौरान, एक दुष्ट एंटी-स्पैम टूल ने स्वीडन के सबसे बड़े बैंक से 250 से अधिक ग्राहकों की पहचान और 1.5 मिलियन डॉलर चुरा लिए।

"कार्डर" के कारण रूसी फर्मों को \$20,000,000,000 का वित्तीय नुकसान हुआ। कार्डर जो प्लास्टिक कार्डों को गलत तरीके से बनाने में माहिर हैं, वे कार्डधारकों और कार्ड नंबरों के बारे में

जानकारी प्राप्त करने के लिए इंटरनेट का उपयोग करते हैं। सिटीबैंक के फ़िशिंग ग्राहकों को टेक्स्ट संदेश प्राप्त होते हैं। रूसी अधिसूचना में कहा गया है, "आपके व्यक्तिगत खाते में \$2'000 से अधिक विदेशी मुद्रा में वायर भुगतान प्राप्त हुआ है।" अपने खाते में सफलतापूर्वक धन प्राप्त करने के लिए आपको सिटीबैंक ऑनलाइन के समझौते के अनुसार अपने डेटा की पुष्टि करनी होगी। इस गतिविधि को सत्यापित करने के लिए, खाता प्रबंधन उपकरण लॉन्च करें और सुझाए गए निर्देशों का पालन करें। वायर ट्रांसफर की पुष्टि न होने पर उसे प्रेषक को वापस कर दिया जाएगा।" एक 20 वर्षीय स्कूल ड्रॉपआउट ने ऑनलाइन बैंकिंग सिस्टम में प्रवेश किया और 50 मिलियन वॉन (\$A66, 111) चुरा लिए, जिससे देशों में आमतौर पर उपयोग किए जाने वाले इंटरनेट बैंकिंग सिस्टम की सुरक्षा को लेकर चिंताएँ बढ़ गई हैं। जांचकर्ताओं के अनुसार, ली 22 ने एक सामुदायिक इंटरनेट साइट पर लगाए गए संदेश में हैकिंग सॉफ़्टवेयर जोड़ा। जब महिला ने उस पर क्लिक किया, तो उसने अनजाने में "कीस्ट्रोक" लॉगिंग टूल डाउनलोड कर लिया, जिससे ली को उसके खाते के पासवर्ड और सुरक्षा कोड तक पहुँच प्राप्त करने की अनुमति मिल गई। पुलिस के अनुसार, इंटरनेट उपयोगकर्ताओं को इंटरनेट से अजीब प्रोग्राम इंस्टॉल करने से बचना चाहिए और बैंक द्वारा प्रदान किए गए सुरक्षा सॉफ़्टवेयर का उपयोग करना चाहिए।

साइबर अपराधी हर साल बैंकिंग क्षेत्र को निशाना बनाते हैं, दुनिया भर से अरबों डॉलर चुराते हैं। साइबर अपराधियों के कारण वार्षिक आर्थिक नुकसान (एक्शन फ्रॉड, 2020) \$ 500 बिलियन को पार कर गया है। सितंबर 2015 में भारतीय हैकरों द्वारा किए गए साइबर हमले का लक्ष्य हबीब बैंक लिमिटेड था। 26 अक्टूबर, 2018 को बैंकों पर साइबर हमलों में, 22 पाकिस्तानी बैंकों के 19,000 डेबिट कार्ड के डेटा से समझौता किया गया था। 27 अक्टूबर, 2018 को, बैंक इस्लामी ने एक और साइबर हमले की घोषणा की, जिसमें बैंक को 2.6 मिलियन डॉलर का नुकसान हुआ। भारतीय रिजर्व बैंक ने बैंकों को साइबर सुरक्षा मार्गदर्शक सिद्धांत जारी किया। साइबर हमले की तैयारियों के लिए, 148 वित्तीय संस्थानों ने मॉक साइबर अभ्यास में भाग लिया 2010 से 2016 के बीच दुनिया भर में इंटरनेट का उपयोग तेज़ी से बढ़ रहा है; 1.5 अरब नए इंटरनेट उपयोगकर्ता जुड़े। पिछले पाँच वर्षों में, छह दक्षिण एशियाई देशों में बांग्लादेश भारत से आगे पाँचवें स्थान पर था। 2016 की तुलना में 2017 और 2018 में बांग्लादेश का स्कोर लगातार गिर रहा है। बैंकिंग सिस्टम में हो सकने वाली घुसपैठ को सेवा से वंचित करना सबसे प्रसिद्ध हमला है जो वित्तीय ढांचे (CDoS) में हो सकता है। डेटा का उल्लंघन, मैलवेयर जैसे संक्रमण, ट्रोजन हॉर्स, वर्म्स टीसीपी/आईपी हमला जो हमलावर को पीड़ित के सर्वर तक रूट पहुँच प्राप्त करने की अनुमति

देता है, इस मामले में वित्तीय ढांचा, लक्षित ढाँचों में अप्रत्यक्ष पहुँच अनुभाग के विकास की अनुमति देता है।

डेटा के अनुसार, बैंकों को सार्वजनिक नेटवर्क का उपयोग करके घुसपैठ के खिलाफ अधिक सुरक्षित होने की आवश्यकता है। साइबर सुरक्षा संबंधी चिंताएँ बैंकों, वित्तीय संस्थानों और ग्राहकों की परिसंपत्तियों, डेटा और सूचनाओं को जोखिम में डालती हैं, जिसके परिणामस्वरूप एक नया और विकसित डिजिटल वातावरण बनता है (ओलेक्सांद्र एट अल., 2024)। जैसे-जैसे वित्तीय उद्योग और संस्थानों के खिलाफ साइबर हमलों की संख्या बढ़ती है, इन हमलों पर शोध और विश्लेषण करना और उपाय तैयार करना पहले से कहीं अधिक महत्वपूर्ण हो जाता है। इसके अलावा, ऐसे मॉडल विकसित करना और प्रस्तावित करना महत्वपूर्ण है जो बैंकों और वित्तीय संस्थानों पर साइबर सुरक्षा खतरों के प्रभाव को कम करते हैं।

1.2 साइबर सुरक्षा

1.2.1 बैंकिंग में साइबर सुरक्षा उपायों का अवलोकन

साइबर हमलों के विभिन्न प्रकारों को कई श्रेणियों में वर्गीकृत करके विस्तृत रूप से समझाया गया है। विभिन्न प्रकार के साइबर हमलों में SQL इंजेक्शन, सोशल इंजीनियरिंग, साइबरस्टॉकिंग, डेनियल ऑफ सर्विस अटैक, डिस्ट्रिब्यूटेड डेनियल ऑफ सर्विस अटैक, क्रॉस-साइट स्क्रिप्टिंग, एटीएम क्लोनिंग, पाइरेसी, मैन इन द मिडल अटैक, बर्थडे अटैक, रैनसमवेयर अटैक, बॉटनेट अटैक, ब्रूट फोर्स अटैक शामिल हैं। आईटी एक्ट के अनुसार, 2014 से 2016 तक 29 भारतीय राज्यों में से 10 में साइबर अपराधों में वृद्धि हुई है।

डिजिटल बैंकिंग में प्रमुख साइबर सुरक्षा खतरों को कई कारकों द्वारा सुव्यवस्थित किया जा सकता है, जैसे, अनएन्क्रिप्टेड डेटा, मैलवेयर, थर्ड-पार्टी सेवाएँ, स्पाफिंग, फ़िशिंग, आदि। कोविड के बाद के वर्षों में, दुनिया भर में साइबर खतरे बढ़ गए हैं, जिसमें प्रमुख बैंकिंग सर्वर हैकर्स द्वारा अपहृत किए जा रहे हैं। प्रमाणीकरण, गोपनीयता और डेटा अखंडता सहित कथित सुरक्षा कारक, इंटरनेट बैंकिंग सेवाओं का उपयोग जारी रखने के लिए ग्राहकों की इच्छा को महत्वपूर्ण रूप से प्रभावित करते हैं। यह सूचना सुरक्षा के मुख्य स्तंभों- गोपनीयता, अखंडता और उपलब्धता के महत्व को उजागर करता है - जो साइबर सुरक्षा खतरों से जुड़ी व्यापक चिंताओं के साथ संरेखित है। पाकिस्तान के बैंकिंग क्षेत्र में साइबर अपराध के मामलों के विश्लेषण से पता चला है कि

साइबर अपराध सीधे संगठनात्मक प्रदर्शन को प्रभावित करते हैं, जैसा कि पाकिस्तानी बैंकिंग क्षेत्र के भीतर अनुसंधान द्वारा उजागर किया गया है। अध्ययन प्रदर्शन पर साइबर अपराध की घटनाओं के पर्याप्त नकारात्मक प्रभाव की पहचान करता है, जो साइबर सुरक्षा खतरों से जुड़े हानिकारक परिणामों की व्यापक कथा को पुष्ट करता है। हालाँकि, सूचना सुरक्षा जागरूकता एक महत्वपूर्ण शमन कारक के रूप में उभरती है, जो संगठनात्मक प्रदर्शन पर साइबर अपराधों के प्रतिकूल प्रभावों को कम करने में महत्वपूर्ण भूमिका निभाती है। अध्ययन में यह भी पाया गया कि साइबर अपराधों का संगठनात्मक प्रदर्शन पर प्रभाव सूचना सुरक्षा जागरूकता के स्तर के आधार पर भिन्न होता है। साइबर सुरक्षा जागरूकता बढ़ाना और वित्तीय संस्थानों के बीच सहयोग बढ़ाना डिजिटल बैंकिंग को अपनाने को बढ़ावा देने के लिए महत्वपूर्ण उपाय हैं, साथ ही डिजिटल युग में वित्तीय लेनदेन की सुरक्षा और अखंडता सुनिश्चित करना भी महत्वपूर्ण है।

1.2.2 भारतीय बैंकिंग क्षेत्र और साइबर सुरक्षा

भारतीय बैंकिंग क्षेत्र में साइबर हमलों और बचाव रणनीतियों का विस्तृत विश्लेषण प्रस्तुत किया। अध्ययन में बैंकों द्वारा सामना किए जाने वाले विभिन्न साइबर खतरों पर प्रकाश डाला गया है, जिसमें 60% अधिकारियों ने ऑनलाइन पहचान चोरी की घटनाओं की रिपोर्ट की है, और सेवा से वंचित (DoS) हमलों, फ़िशिंग, विशिंग और स्फूफ़िंग पर महत्वपूर्ण चिंता व्यक्त की है, बाद वाले की पुष्टि 76% उत्तरदाताओं ने की है। अन्य कमजोरियों में दुर्भावनापूर्ण कोड, SQL इंजेक्शन और ब्रूट-फोर्स हमले शामिल हैं, जिसमें पहचान धोखा 80% अधिकारियों द्वारा बताई गई एक प्रमुख रणनीति है। एन्क्रिप्शन, अद्वितीय लॉगिन, बायोमेट्रिक्स और नियमित एंटीवायरस अपडेट सहित मजबूत सुरक्षा उपायों को अपनाने के बावजूद, डेटा ग्रेन्युलैरिटी, उपयोगकर्ता पहुँच नीतियाँ और लॉगिंग गतिविधियों जैसे क्षेत्रों पर अधिक ध्यान देने की आवश्यकता है। अध्ययन सक्रिय उपायों के महत्व को रेखांकित करता है, जैसे घुसपैठ का पता लगाने वाले उपकरण, लगातार नीति समीक्षा और संदिग्ध गतिविधियों के लिए उपयोगकर्ता अलर्ट। इसके अलावा, हैकिंग, फ़िशिंग और पहचान की चोरी जैसे खतरों को कम करने के लिए साइबर सुरक्षा और सुरक्षित प्रथाओं के बारे में ग्राहकों को शिक्षित करने के लिए सरकारों और निजी संस्थाओं के साथ सहयोग करना आवश्यक है। मुंधे एट अल. (2024) द्वारा किए गए एक अन्य अध्ययन ने यह निष्कर्ष निकाला कि भारतीय बैंकिंग क्षेत्र का डिजिटल परिवर्तन महत्वपूर्ण साइबर सुरक्षा चुनौतियों के साथ-साथ महत्वपूर्ण अवसर भी लाता है। जैसे-जैसे बैंक तेजी से डिजिटल चैनल अपना रहे हैं, डेटा उल्लंघन और सिस्टम कमजोरियों सहित साइबर सुरक्षा जोखिम प्रमुख चिंता का विषय बन गए हैं।

डिजिटल संचालन की सुरक्षा के लिए AI, मशीन लर्निंग और ब्लॉकचेन जैसी उन्नत तकनीकों जैसे साइबर सुरक्षा उपायों में मजबूत निवेश आवश्यक है। विश्वास और परिचालन अखंडता बनाए रखने के लिए विकसित नियामक आवश्यकताओं का अनुपालन भी उतना ही महत्वपूर्ण है। फिनटेक फर्मों और प्रौद्योगिकी प्रदाताओं के साथ सहयोग सुरक्षा ढांचे और उभरते खतरों के लिए अनुकूलनशीलता को और बढ़ा सकता है। इसके अतिरिक्त, डिजिटल उपकरणों को प्रभावी ढंग से लागू करने और प्रबंधित करने के लिए कार्यबल का निरंतर कौशल विकास महत्वपूर्ण है, जिससे एक सुरक्षित और लकाईला बैंकिंग पारिस्थितिकी तंत्र सुनिश्चित होता है। UPI, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, मोबाइल वॉलेट और QR कोड जैसी विभिन्न डिजिटल तकनीकों को अपनाने के साथ भारत में डिजिटल बैंकिंग में उल्लेखनीय प्रगति हुई है। डिजिटल बैंकिंग की प्रगति ने बैंकिंग और वित्तीय क्षेत्र में सुविधा, वैयक्तिकरण, दक्षता, पारदर्शिता और नवाचार को बढ़ाया है। हालाँकि, डिजिटल बैंकिंग सुरक्षा, डेटा गोपनीयता और तेजी से विकसित हो रहे प्रौद्योगिकी रुझानों के साथ तालमेल बनाए रखने के लिए निरंतर अनुकूलन की आवश्यकता से संबंधित चुनौतियाँ भी प्रस्तुत करती है।

1.2.3 साइबर सुरक्षा चिंताओं के लिए बैंकिंग क्षेत्रों में एआई का कार्यान्वयन

AI में मशीन लर्निंग (ML) और डीप लर्निंग (DL) सहित विभिन्न तकनीकें शामिल हैं, जिनका उद्देश्य निर्णय लेने और भाषा प्रसंस्करण जैसी जटिल मानवीय क्षमताओं की नकल करना है। बैंकिंग में, AI-संचालित उपकरण मल्टीचैनल ग्राहक पहुँच को बढ़ाते हैं, वरीयताओं में अंतर्दृष्टि प्रदान करते हैं, और अनुकूलित सेवाएँ सक्षम करते हैं, जिससे बैंकों को फिनटेक फर्मों के साथ प्रतिस्पर्धा करने में मदद मिलती है। हालाँकि, पारंपरिक बैंकों में विरासत प्रणाली अक्सर नई तकनीकों के एकीकरण में बाधा डालती है, जिससे अतिरिक्त सुरक्षा जोखिम पैदा होते हैं। डेटा गोपनीयता एक महत्वपूर्ण चिंता का विषय है क्योंकि विनियामक ढाँचे विकसित होते हैं, तीसरे पक्ष के प्रदाताओं पर निर्भरता और चैटबॉट और प्राकृतिक भाषा प्रसंस्करण (NLP) जैसे उपकरणों के संभावित गोपनीयता उल्लंघन के बारे में अनिश्चितताएँ बढ़ती हैं। साइबर सुरक्षा रणनीतियों को उपयोगकर्ता व्यवहार पर विचार करना चाहिए, जैसा कि TAM, TRA और UTAUT जैसे मॉडलों द्वारा उल्लिखित है, जो कथित उपयोगिता, उपयोग में आसानी, सांस्कृतिक प्रभावों और प्रौद्योगिकी स्वीकृति में जोखिमों की भूमिका पर जोर देते हैं। AI-संचालित बैंकिंग प्रणालियों को सुरक्षित करने के लिए तकनीकी और व्यवहारिक दोनों दृष्टिकोणों से कमजोरियों को संबोधित करना आवश्यक है। AI बैंकों को अनियमितताओं का विश्लेषण करके और खतरे

की प्रतिक्रिया को बढ़ाकर साइबर अपराध को रोकने और पता लगाने के लिए कृत्रिम तंत्रिका नेटवर्क (ANN), फ़ज़ी लॉजिक और आनुवंशिक एल्गोरिदम जैसे उन्नत उपकरण प्रदान करता है। AI को तीन स्तरों पर लागू किया जाता है—सुरक्षा, पता लगाना और प्रतिक्रिया—लेकिन इसमें कमजोरियाँ भी हैं, जैसे कि प्रतिकूल मशीन लर्निंग (ML), जो खामियों का फायदा उठाने या झूठे आउटपुट उत्पन्न करने के लिए AI सिस्टम में हेरफेर करती है। AI संचालित साइबर अपराधों में अनुकूलित फ़िशिंग, प्रतिरूपण, सुरक्षा प्रणालियों में व्यवधान और बड़े पैमाने पर ब्लैकमेल शामिल हैं, जो बैंकों की अखंडता, दक्षता और प्रतिष्ठा के लिए महत्वपूर्ण खतरे पैदा करते हैं। नियामक अंतराल, विशेष रूप से विकासशील अर्थव्यवस्थाओं में, इन जोखिमों को बढ़ाते हैं, बढ़ते खतरों से निपटने और विश्वास बनाए रखने के लिए मजबूत AI शासन और साइबर सुरक्षा ढांचे की आवश्यकता पर बल देते हैं। फ़राजी एट अल. (2024) द्वारा एक व्यवस्थित समीक्षा कार्य ने विस्तार से समझाया है कि वित्तीय लेनदेन में साइबर सुरक्षा को बढ़ाने में AI का बड़ा महत्व कैसे है एमएल के विभिन्न दृष्टिकोण, अर्थात् सुदृढीकरण सीखना (आरएल), गहन सीखना (डीएल), बेहतर डेटा विश्लेषण और खतरे की भविष्यवाणी के लिए तंत्रिका नेटवर्क की कई स्तरित संरचनाएं स्थापित की जा सकती हैं।

1.2.4 साइबर सुरक्षा शब्दावली

अध्ययन विषय से जुड़े मुख्य विचारों को बेहतर ढंग से समझने के लिए आवश्यक शब्दावली की कुछ परिभाषाएँ निम्नलिखित हैं। साइबरस्पेस सूचना जगत के भीतर एक विश्वव्यापी क्षेत्र है, जिसकी विशेषता इलेक्ट्रॉनिक और विद्युत चुम्बकीय स्पेक्ट्रम है, जो अत्याधुनिक सूचना और संचार प्रौद्योगिकी का उपयोग करके जुड़े और आश्रित नेटवर्क के माध्यम से सूचना उत्पन्न, अद्यतन, संग्रहीत, वितरित और शोषण करता है।

- **कमजोरियाँ**

ये सिस्टम या उसके डिजाइन की कमजोरियाँ हैं जो हमलावर को दुर्भावनापूर्ण निर्देशों को निष्पादित करने, डेटा तक अनधिकृत पहुँच प्राप्त करने और विभिन्न सेवा अस्वीकार हमलों को अंजाम देने की अनुमति देती हैं

- **धमकियाँ**

ये उपाय सिस्टम में सुरक्षा खामियों से लाभ उठाने के लिए किए जाते हैं, जबकि इससे सिस्टम पर नकारात्मक प्रभाव पड़ता है

- **आक्रमण**

ये वे उपाय हैं जो किसी सिस्टम को नुकसान पहुँचाने या विभिन्न उपकरणों और तकनीकों के साथ कमज़ोरियों का फ़ायदा उठाकर उसके सामान्य कामकाज को बाधित करने के लिए किए जाते हैं। हमलावर अपने नापाक उद्देश्यों को पूरा करने के लिए ये हमले करते हैं, चाहे वे आत्म-संतुष्टि के लिए हों या वित्तीय लाभ के लिए। साहित्य में कई सुरक्षा खामियों का उल्लेख किया गया है। पाठकों को कुछ सबसे आम साइबर सुरक्षा कमज़ोरियों को समझने में मदद करने के लिए,

- **सेवा अस्वीकार (DoS)**

इस तरह का हमला इच्छित उपयोगकर्ताओं को मशीन या नेटवर्क संसाधन तक पहुँचने से रोकता है। कोई भी घटना जो नेटवर्क की अपने अनुमानित उद्देश्य को निष्पादित करने की क्षमता को कम या नष्ट कर देती है, इसका कारण बनती है। IoT संदर्भ में अधिकांश कंप्यूटर डिवाइस अपनी कम मेमोरी क्षमता और सीमित प्रसंस्करण संसाधनों के कारण संपत्ति के विनाश के हमलों के प्रति संवेदनशील हैं। DoS हमले के कारणों में से एक यह है कि विभिन्न व्यवसाय समान तकनीक का उपयोग करते हैं, जिसका संभावित हमलावर फायदा उठाते हैं।

- **मैलवेयर**

हमलावर इस हमले में सुरक्षा खामियों का फायदा उठाकर कंप्यूटर सिस्टम तक अनधिकृत पहुँच प्राप्त करने के लिए दुर्भावनापूर्ण सॉफ़्टवेयर प्रोग्रामर का उपयोग करता है। मैलवेयर के पीछे का उद्देश्य एक महत्वपूर्ण वित्तीय या राजनीतिक लाभ है जो हमलावर को अपने हानिकारक लक्ष्यों को प्राप्त करने के लिए यथासंभव अधिक से अधिक नेटवर्क उपकरणों में घुसपैठ करने के लिए प्रेरित करता है।

- **फ़िशिंग**

यह एक आपराधिक अपराध है जिसमें इंटरनेट उपयोगकर्ता से संवेदनशील जानकारी प्राप्त करने के लिए सोशल इंजीनियरिंग और प्रौद्योगिकी का उपयोग किया जाता है। फ़िशिंग रणनीतियाँ

ईमेल, इंस्टेंट चैट, पॉप-अप संदेश और वेब साइटों सहित विभिन्न संचार चैनलों का उपयोग करती हैं।

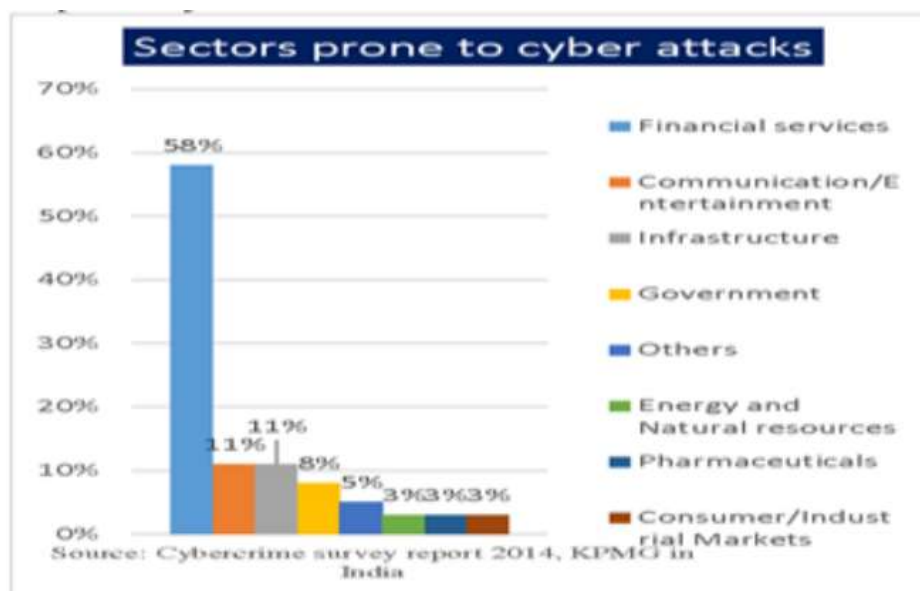
- **SQL इंजेक्शन हमला**

इस हमले में SQL केरी को हमलावर के लाभ के लिए अपडेट या हेरफेर करने के लिए एप्लिकेशन में एक इनपुट स्ट्रिंग इंजेक्ट की जाती है। यह हमला कई तरीकों से डेटाबेस को नुकसान पहुंचाता है, जिसमें अवैध डेटाबेस एक्सेस और संशोधन, साथ ही संवेदनशील डेटा का खुलासा शामिल है। यह हमला खतरनाक है क्योंकि इससे डेटा की हानि हो सकती है या अनधिकृत संगठनों द्वारा इसका उपयोग किया जा सकता है, जिससे कार्यक्षमता और गोपनीयता नष्ट हो सकती है। इसके अलावा, इस प्रकार के हमले के हिस्से के रूप में सिस्टम-स्तरीय निर्देश निष्पादित किए जाते हैं, जो अधिकृत उपयोगकर्ताओं को आवश्यक जानकारी तक पहुंचने से रोकते हैं। मैन-इन-द-मिडल हमले और सत्र अपहरण मैन-इन-द-मिडल (MITM), जिसे कभी-कभी साहित्य में MIM, MitM, MiM या MITMA के रूप में जाना जाता है, एक ऐसा हमला है जिसमें एक अनधिकृत तीसरा पक्ष कई अंत बिंदुओं के बीच संचार चैनल का नियंत्रण चुपके से प्राप्त कर लेता है। MITM हमलावर लक्षित पीड़ितों के संचार प्रवाह को बाधित, संशोधित या यहां तक कि प्रतिस्थापित भी कर सकता है।

1.3 साइबर अपराध

किसी देश की प्रगति और विस्तार को निर्धारित करने वाले मूलभूत तत्वों में से एक उसकी अर्थव्यवस्था है। बैंकिंग उद्योग को अर्थव्यवस्था की नींव माना जाता है। हम अपने दैनिक कार्यों को डिमांड ड्राफ्ट, चेक और नकदी का उपयोग करके पूरा करते हैं। दूसरी ओर, इस डिज़ाइन ने एक नए क्रेडिट/डेबिट कार्ड-स्वाइपिंग भुगतान पद्धति के लिए जगह बनाई है। वित्तीय चिंताओं पर अपनी 1991-1998 की रिपोर्ट में, नरसिम्हा समिति ने सिफारिश की कि बैंकिंग उद्योग की दक्षता में सुधार के लिए सूचना प्रौद्योगिकी (आईटी) का उपयोग किया जाना चाहिए।

इस अध्ययन का लक्ष्य बैंकिंग उद्योग के लिए साइबर खतरों से संबंधित चिंताओं को उजागर करने के लिए इस्तेमाल की जाने वाली अंतर्निहित रणनीतियों की जांच करना है। यह इस बात पर केंद्रित है कि वित्तीय संस्थान साइबर अपराध की घटनाओं से निपटने के लिए कितने तैयार हैं।



साइबर सुरक्षा एक जटिल, बहुआयामी और समझने में चुनौतीपूर्ण समस्या क्षेत्र है। जैसे-जैसे इलेक्ट्रॉनिक उपकरणों का उपयोग करने वाले लोगों की संख्या बढ़ती जा रही है, वैसे-वैसे खतरे का माहौल भी विकसित हो रहा है। कमजोरियों की पहचान करना और उनका समाधान करना पारंपरिक साइबर सुरक्षा पद्धतियों का मुख्य लक्ष्य है। यह मानसिकता आवश्यक है, लेकिन पर्याप्त नहीं है। संभावित और मौजूदा साइबर हमलों की विशेषताओं के बारे में अधिक जानकारी प्राप्त करना बुद्धिमानी से निवारक निर्णय लेने के लिए आवश्यक है जो उपलब्ध संसाधनों की संख्या को अनुकूलित करते हैं। इस परियोजना का लक्ष्य सामान्य संवेदनशीलता के विषयों की पहचान करना है जिन्हें अभी तक पहचाना नहीं गया है। हमारी जांच के परिणामों की रिपोर्ट की जाती है, और उनके निहितार्थों पर चर्चा की जाती है। फिर हम समापन करते हैं और अतिरिक्त शोध के लिए सिफारिशें प्रदान करते हैं। कई सुरक्षा-आधारित नवाचार विधियाँ प्रस्तावित की गई हैं, लेकिन उनमें से सभी का वास्तविक दुनिया की सेटिंग्स में अनुभवजन्य रूप से परीक्षण नहीं किया गया है। परिणामस्वरूप, हम उनकी प्रयोज्यता या वास्तविक उपयोग को पूरी तरह से नहीं समझ पाते हैं, विशेष रूप से वित्तीय समाधान बनाने के संदर्भ में। बैंकिंग की इस शैली के साथ मुख्य मुद्दों में से एक गोपनीयता के लिए मौजूद खतरों की विविधता है। बैंकिंग उद्योग लगातार तकनीकी रूप से बदल रहा है क्योंकि वित्तीय सेवाओं के सैद्धांतिक ढांचे में बदलाव हो रहा है। मौजूदा तरीकों के फायदे, क्षमता और नुकसान का पता लगाने के लिए, यह आलेख मान्यता प्राप्त मूल्यांकन मानकों के आधार पर सुरक्षित ऑनलाइन बैंकिंग बुनियादी ढांचे के निर्माण में उनकी प्रयोज्यता के संदर्भ में सुरक्षा समाधानों का विश्लेषण और जांच करता है।

इंटरनेट के माध्यम से संभावित हमलों से सूचना, नेटवर्किंग और कंप्यूटर के लिए सिस्टम और प्रोग्राम की सुरक्षा के लिए, कुछ प्रोटोकॉल, रणनीति और उपकरणों को "साइबर सुरक्षा" कहा जाता है। हमलावर अधिक परिष्कृत हमलों के लिए आर्टिफिशियल इंटेलिजेंस तकनीकों का उपयोग कर सकते हैं। डीपफेक वर्तमान में उपयोग में हैं, और रोबोट अभी भी बढ़ रहे हैं।

आजकल पेशेवरों को एक विशिष्ट स्थान से काम करने के लिए आने-जाने की आवश्यकता नहीं है, आभासी परिस्थितियों में काम करने के प्रचलन ने सुरक्षा पेशेवरों को दूरस्थ कार्य से जुड़े व्यावसायिक खतरों का मूल्यांकन करने और तीसरे पक्ष को इन कार्य स्थितियों में सेंध लगाने या लॉग इन करने से रोकने के लिए कदम उठाने के लिए मजबूर किया है। साइबर खतरों को रोकने के लिए व्यवसाय चाहे कितने भी परिष्कृत तकनीकी सुरक्षा उपाय लागू करें, "मानवीय तत्व" - यानी कार्मिक कौशल - अधिक ध्यान देने योग्य है क्योंकि यह इस श्रृंखला में सबसे कमजोर घटक है। सुरक्षा अनुपालन चिंताओं के बारे में सवाल लोगों और उनकी धारणाओं, समझ और सुरक्षा खतरों पर उनकी प्रतिक्रिया के बारे में निर्णयों से जुड़ा है, यानी, क्या वे अनुशंसित सुरक्षा प्रक्रियाओं का पालन करना चाहते हैं। हालाँकि शोधकर्ता और पेशेवर समान रूप से स्वीकार करते हैं कि लोग सुरक्षा प्राप्त करने में महत्वपूर्ण भूमिका निभाते हैं, उन्हें सुरक्षा नेटवर्क में सबसे कमजोर घटक के रूप में भी संदर्भित किया जाता है क्योंकि वे अक्सर सुरक्षा-अनुशंसित प्रक्रियाओं की अवहेलना करते हैं। नतीजतन, यह अप्रत्याशित नहीं है कि किसी व्यक्ति का सुरक्षा संबंधी आचरण संगठनों के लिए एक महत्वपूर्ण चिंता और अध्ययन का केंद्र बिंदु बन गया है। उद्योग के आंकड़े दर्शाते हैं कि सुरक्षा बढ़ाने के लिए नेतृत्व के बेहतर प्रयासों के बावजूद, उल्लंघनों का मुख्य कारण मानवीय व्यवहार है - चाहे वह जानबूझकर किया गया हो, लापरवाही से किया गया हो या अनजाने में किया गया हो।

साइबर सुरक्षा विशेषज्ञता, धारणा और आचरण पर ध्यान केंद्रित करते हुए, अध्ययन में पाया गया कि हालांकि इज़राइल, स्लोवेनिया, पोलैंड और तुर्की जैसे देशों में उपभोक्ता ऑनलाइन खतरों के बारे में पर्याप्त जागरूकता प्रदर्शित करते हैं, लेकिन वे अपर्याप्त सावधानी बरतते हैं। अधिक जागरूकता और साइबर शिक्षा के बीच एक क्रॉस-नेशनल और लिंग-तटस्थ संबंध है। हालांकि डेटा नहीं दिया गया है, समझ सुरक्षात्मक तरीकों के उपयोग को प्रभावित करती है। भौगोलिक असमानताओं के आधार पर अनुकूलित साइबर सुरक्षा रणनीतियों पर जोर देना महत्वपूर्ण है क्योंकि राष्ट्र-विशिष्ट चर धारणाओं, समझ और कार्यों को कैसे प्रभावित करते हैं।

1.3.1 साइबर अपराध की विशेषताएं

साइबर अपराधों की कुछ विशेषताएं इस प्रकार हैं:

1. **स्वभावतः मौन**: साइबर अपराध उनके घरों की गोपनीयता में किए जा सकते हैं। इसमें कोई प्रत्यक्षदर्शी नहीं होता और पीड़ित के साथ कोई शारीरिक संपर्क नहीं होता। ये अपराध माउस के एक क्लिक पर किए जाते हैं, पीड़ित को अपराध के बारे में कोई जानकारी नहीं होती और वे अक्षम हो जाते हैं। ज्यादातर मामलों में उन्हें एहसास ही नहीं होता कि वे वास्तव में साइबर अपराध के शिकार हैं।
2. **वैश्विक चरित्र**: साइबर अपराध की कोई सीमा नहीं होती और यह पारंपरिक क्षेत्रीय अधिकार क्षेत्र का पालन नहीं करता। नेटवर्क से संबंधित अपराध के मामले में पूरी दुनिया पीड़ित या अपराध स्थल हो सकती है। किसी देश की सुविधा में बैठकर पूरे देश की अर्थव्यवस्था को नष्ट किया जा सकता है।
3. **भौतिक साक्ष्य का अभाव**: साइबर अपराध के मामलों में, अपराध स्थल पर भौतिक साक्ष्य उपलब्ध नहीं होते हैं। एक जगह साफ-सुथरी और बिना किसी गड़बड़ी के दिख सकती है, लेकिन एक प्रशिक्षित आंख डिजिटल प्रारूप में मौजूद प्रचुर मात्रा में साक्ष्य देख सकती है। इस डिजिटल साक्ष्य का इस्तेमाल साइबर अपराधी को दोषी ठहराने के लिए किया जा सकता है।
4. **उच्च प्रभाव पैदा करता है**: साइबर अपराधों के मामलों में, ऐसी घटनाओं का प्रभाव गंभीर होता है। यह ऑपरेशन को बाधित कर सकता है और पीड़ितों के लिए बड़े पैमाने पर तबाही मचा सकता है। ऐसा ही एक क्षेत्र ई-कॉमर्स हो सकता है, जो पूरी तरह से इंटरनेट पर निर्भर है।
5. **उच्च क्षमता**: युवा सॉफ्टवेयर कंपनियों द्वारा अच्छी तनख्वाह वाली नौकरियों की ओर आकर्षित होते हैं। ऐसे कई प्रशिक्षण संस्थान हैं जो ऐसे पेशेवरों को तैयार करते हैं जो लाखों कमाने के सपने देखते हैं, लेकिन वे इस क्षेत्र में पारंगत नहीं होते। नौकरी के अवसरों की कमी के कारण ये पेशेवर खुद को आपराधिक गतिविधियों में शामिल कर सकते हैं, जिससे साइबर अपराधों का खतरा बढ़ सकता है।

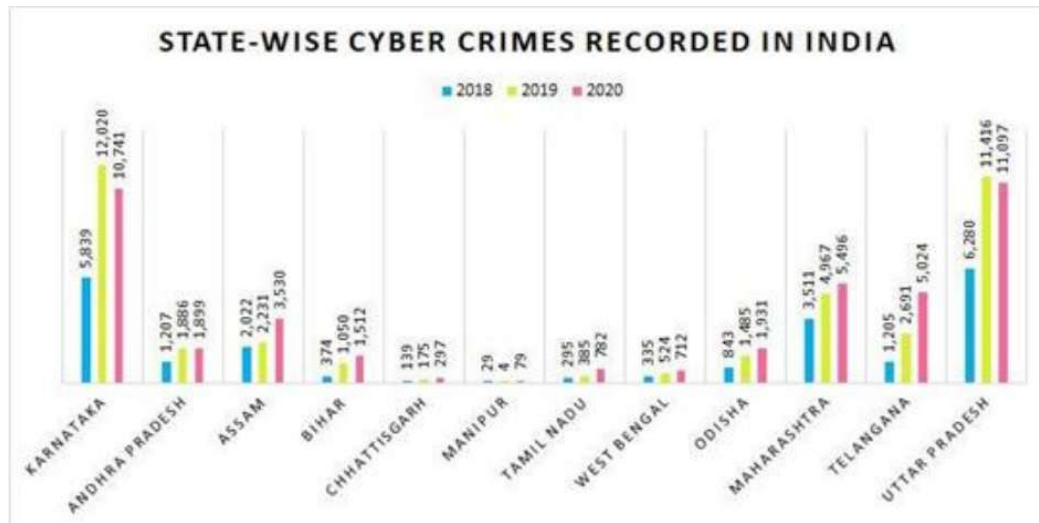
1.3.2 वर्तमान और भविष्य में प्रौद्योगिकी का उपयोग

डिजिटल सुरक्षा और अनुकूली धारणा की मूल अवधारणा "ढांचे" है। कोई भी गड़बड़ी जो डिजिटल प्रौद्योगिकियों की सामान्य रूप से काम करने की क्षमता को बाधित करती है, उसे साइबर-हमला कहा जाता है। जोखिम "कंप्यूटर सिस्टम, सिस्टम सुरक्षा विधियों, आंतरिक सुरक्षा उपायों या निष्पादन में कमज़ोरियाँ हैं जिनका किसी अवांछनीय स्रोत द्वारा लाभ उठाया जा सकता है" जो डिजिटल दुनिया में जानबूझकर गड़बड़ी को संभव बनाते हैं। तकनीकी वास्तुकला से मौजूदा कमज़ोरियों को पूरी तरह से मिटाना और नई कमज़ोरियों को उभरने से रोकना मुश्किल है।

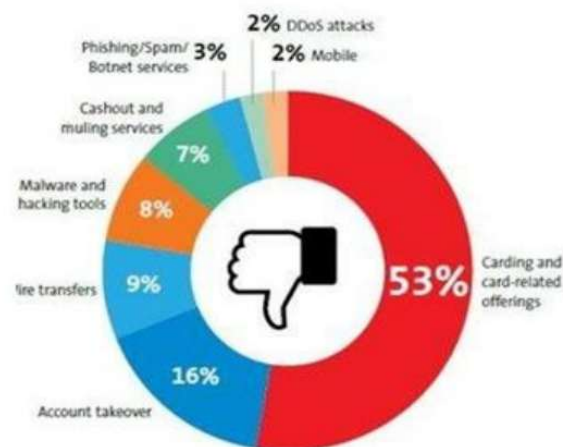
1.3.3 बैंकिंग उद्योग में साइबर अपराध

साइबर अपराध कोई भी अवैध गतिविधि है जो ऑनलाइन या कंप्यूटर के माध्यम से होती है। दूसरे शब्दों में कहें तो डिजिटल कदाचार को साइबर अपराध भी कहा जाता है, जब कोई अपराधी कंप्यूटर या किसी अन्य इलेक्ट्रॉनिक डिवाइस और इंटरनेट का उपयोग करके कई तरह के अपराध करता है, जिसमें अनधिकृत पहुँच के माध्यम से धन हस्तांतरण और निकासी शामिल है।

आज की वैश्वीकृत दुनिया में, बैंकिंग उद्योग अपने ग्राहकों को क्रेडिट कार्ड सेवाओं और इंटरनेट बैंकिंग सहित कई तरह की सेवाएँ प्रदान करता है। "डेबिट कार्ड से ऑनलाइन भुगतान करना" उपभोक्ताओं को सभी बैंक सेवाओं तक चौबीसों घंटे पहुँच मिलती है, और वे अपने फ़ोन और इंटरनेट का उपयोग करके दुनिया के किसी भी स्थान से सुविधाजनक रूप से व्यवसाय कर सकते हैं और अपने खातों का प्रबंधन कर सकते हैं।" हालाँकि ये सेवाएँ उपयोगकर्ताओं के लिए मददगार हैं, जैसा कि हम सभी जानते हैं, इनका एक नकारात्मक पहलू भी है जिसमें डकैती और हैकर शामिल हैं।



1.3.4 बैंकिंग क्षेत्र से जुड़े साइबर अपराध के प्रकार



- **हैकिंग**

हैकिंग एक प्रकार का साइबर अपराध है, जिसमें कोई व्यक्ति बैंकिंग वेबसाइट या ग्राहक खातों में सेंध लगाकर सुरक्षा उपायों को भंग करने का प्रयास करता है, या सिस्टम तक अनधिकृत पहुंच प्राप्त कर लेता है।

- **वायरस**

यह एक प्रकार का स्व-प्रतिकृति सॉफ्टवेयर है जो संक्रमित करने के लिए दस्तावेज़ों या निष्पादन योग्य कोड में अपनी प्रतियाँ सम्मिलित करता है। एक निष्पादन योग्य फ़ाइल जिसे किसी प्रोग्राम द्वारा संक्रमित किया गया है जो इसे अजीब तरह से व्यवहार करता है उसे वायरस कहा जाता है।

यह ऑपरेटिंग सिस्टम और प्रोग्राम फ़ाइलों सहित निष्पादन योग्य फ़ाइलों से खुद को जोड़कर फैलता है। निष्पादन योग्य फ़ाइल लोड करने की प्रक्रिया वायरस को खुद को दोहराने का कारण बन सकती है। दूसरी ओर, वर्म्स ऐसे प्रोग्राम होते हैं जो पीड़ित के कंप्यूटर से खुद को कॉपी करने और अन्य कंप्यूटरों को प्रतियां भेजने की क्षमता रखते हैं। वर्म्स बिना किसी फ़ाइल को बदले या हटाए उपयोगकर्ता के कंप्यूटर से खुद की प्रतियों को दूसरे कंप्यूटरों में कॉपी और ट्रांसफर करते हैं।

- **स्पाइवेयर**

ऑनलाइन बैंकिंग क्रेडेंशियल्स लेने और उन्हें धोखाधड़ी से इस्तेमाल करने का सबसे लोकप्रिय तरीका स्पाइवेयर है। स्पाइवेयर द्वारा कंप्यूटर और वेबसाइटों के बीच जानकारी एकत्र की जाती है या भेजी जाती है। अधिकतर, इसे झूठे "पॉप अप" विज्ञापनों द्वारा इंस्टॉल किया जाता है जो सॉफ़्टवेयर डाउनलोड करने का अनुरोध करते हैं। इस तरह के सॉफ़्टवेयर को उद्योग-मानक एंटीवायरस प्रोग्राम द्वारा खोजा और समाप्त किया जाता है, ज्यादातर कंप्यूटर को संक्रमित करने से पहले प्रोग्राम के डाउनलोड और इंस्टॉलेशन को रोककर।

- **फ़िशिंग**

फ़िशिंग एक प्रकार का घोटाला है जिसमें प्रतिष्ठित स्रोतों से आने वाले ईमेल का उपयोग ग्राहक आईडी, आईपिन, सीवीवी नंबर, डेबिट/क्रेडिट कार्ड नंबर और समाप्ति तिथि जैसी व्यक्तिगत जानकारी चुराने के लिए किया जाता है। ईमेल स्पूर्फिंग और इंस्टेंट मैसेजिंग फ़िशिंग में इस्तेमाल की जाने वाली दो विधियाँ हैं।

इस तरह की धोखाधड़ी में, जालसाज बैंक कर्मचारियों के रूप में खुद को पेश करते हैं और एक सीधा लिंक बनाते हैं जो इच्छित शिकार के ब्राउज़र को एक नकली वेबपेज पर ले जाता है जो वास्तविक बैंक वेबसाइट की नकल करता है। ग्राहक के खाते पर, प्राप्त गोपनीय जानकारी का उपयोग करके बाद में धोखाधड़ी वाले लेनदेन किए जाते हैं। इन दिनों, फ़िशर्स अपने अपराधों को अंजाम देने के लिए मोबाइल (वॉयस फ़िशिंग) और एसएमएस (स्मैशिंग) तकनीकों का भी उपयोग करते हैं।

- **फ़ार्मिंग**

इंटरनेट का इस्तेमाल औषधीय कार्यों के लिए किया जाता है। हैकर्स यूआरएल में हेरफेर करते हैं ताकि जब कोई उपभोक्ता बैंक की वेबसाइट पर जाए, तो उसे एक नकली वेबसाइट पर ले जाया जाए जो बैंक की मूल वेबसाइट की नकल करती है।

- **ATMSKIMMIN गैड बिक्री अपराध बिंदु**

मशीन कीपैड के ऊपर स्क्रीमिंग डिवाइस लगाना ताकि यह असली कीपैड जैसा लगे या कार्ड रीडर से जुड़ा कोई उपकरण लगाना ताकि यह मशीन का ही एक घटक लगे, एटीएम या पॉइंट-ऑफ-सेल (POS) सिस्टम में घुसने का एक तरीका है। इन डिवाइस पर सीधे क्रेडिट कार्ड की जानकारी चुराने वाले मैलवेयर भी इंस्टॉल किए जा सकते हैं। कार्ड नंबर और व्यक्तिगत पहचान संख्या (पिन) उन एटीएम से प्राप्त किए जा सकते हैं जिनमें स्किमर सफलतापूर्वक इंस्टॉल किए गए हैं। फिर इन विवरणों की नकल की जाती है और धोखाधड़ी वाले लेनदेन में उनका उपयोग किया जाता है।

- **DNSकैशपॉइज़निंग**

किसी संगठन के नेटवर्क में, DNS सर्वर का उपयोग कैश में पहले से प्राप्त क्रेरी परिणामों को संग्रहीत करके समाधान प्रतिक्रिया समय को तेज़ करने के लिए किया जाता है। DNS सॉफ़्टवेयर में भेद्यता का लाभ उठाकर, DNS सर्वर के विरुद्ध ज़हर भरे हमले किए जाते हैं। सर्वर उन सभी उपयोगकर्ताओं को गलत प्रविष्टियाँ प्रदान करेगा जो इसके स्थानीय कैश से समान अनुरोध करते हैं। बैंक क्लाइंट को आपराधिक-नियंत्रित सर्वर पर पुनर्निर्देशित किया जा सकता है, जहाँ मैलवेयर परोसा जा सकता है या उन्हें धोखाधड़ी वाली वेबसाइट के लिए अपनी लॉगिन जानकारी दर्ज करने के लिए धोखा दिया जा सकता है। IP स्पूफ़िंग एक ऐसी तकनीक है जिसका उपयोग क्लाइंट पर नियंत्रण पाने के लिए किया जाता है। इसमें बैंक की वेबसाइट के DNS रिकॉर्ड को एक DNS सर्वर से दूसरे DNS सर्वर में बदलना शामिल है, जिसमें उनके स्वामित्व वाले सर्वर का IP पता इस्तेमाल किया जाता है।

1.3.5 बैंकों पर साइबर अपराध का प्रभाव

दैनिक जीवन में मोबाइल नेटवर्क के प्रसार और सूचना एवं प्रौद्योगिकी (आईटी) की उन्नति ने वित्तीय सेवाओं को व्यापक दर्शकों के लिए अधिक सुलभ बना दिया है। लेकिन जहाँ तकनीकी प्रगति ने बैंकिंग सेवाओं को अधिक सुलभ और किफ़ायती बना दिया है, वहीं इसने साइबर हमलों का लक्ष्य बनने के जोखिम को भी बढ़ा दिया है।

साइबर अपराधियों द्वारा पैसे चुराने, कंपनियों की जासूसी करने और निजी कंपनी की जानकारी तक पहुँचने के लिए इस्तेमाल किए जाने वाले सरल तरीकों का बैंक के वित्त पर अप्रत्यक्ष प्रभाव पड़ता है। इन साइबर अपराधों का मुकाबला करने के लिए, बैंकिंग उद्योग को नियंत्रण प्रतिमान बनाने के लिए सरकारी अधिकारियों और निगरानी समूहों के साथ मिलकर काम करना चाहिए।

इस मामले में मुख्य रुचि का विषय बैंकिंग क्षेत्र में एक प्रभावी संकलन सेवा का अभाव है, जो साइबर अपराध के पैटर्न की पहचान करने तथा उनके आधार पर एक मॉडल तैयार करने में सक्षम हो।

A. भारत में साइबर हमले

1. पुणे में कॉसमॉस बैंक पर साइबर हमला

2018 में हैकर्स ने पुणे स्थित बैंक कॉसमॉस कोऑपरेटिव बैंक लिमिटेड से 94.42 करोड़ रुपये चुरा लिए। हैक से भारत का बैंकिंग उद्योग हिल गया। यह साइबर हमला कॉसमॉस बैंक पर किया गया था। हैकर्स ने बैंक के एटीएम सर्वर तक पहुँच प्राप्त की और वीज़ा और रुपी डेबिट कार्डधारकों से संबंधित व्यक्तिगत डेटा की एक बड़ी मात्रा चुरा ली। यह जानने के बाद कि पैसा नष्ट हो गया है, 28 देशों के साइबर समूहों ने तुरंत पैसे वापस ले लिए। निगरानी प्रक्रियाओं को मजबूत करके और अनुमति प्राप्त लोगों की सहायता करके इसे टाला जा सकता है

2. एटीएम सिस्टम क्षतिग्रस्त

2018 में केनरा बैंक के एटीएम सर्वर को हैक किया गया था। कई बैंक खातों से बीस लाख रुपये निकाल लिए गए थे। साइबर अपराधियों ने कथित तौर पर 300 से ज़्यादा लोगों के एटीएम क्रेडेंशियल्स तक पहुँच बनाई, जिससे कुल 50 लोग पीड़ित बन गए। हैकर्स ने डेबिट कार्डधारकों का डेटा इकट्ठा करने के लिए स्किमिंग डिवाइस नामक डिवाइस का इस्तेमाल किया। चुराए गए

डेटा का इस्तेमाल 10,000 से 40,000 रुपये के बीच के लेन-देन में किया गया। अगर डेटा के दुरुपयोग को रोकने के लिए एटीएम सुरक्षा उपायों को मजबूत किया जाए तो इसे टाला जा सकता है।

3. बैंक एनएसपी मामला

एक मामले में, एक बैंक प्रबंधन प्रशिक्षु की सगाई शादी के लिए तय हुई थी। दोनों ने ईमेल भेजने और प्राप्त करने के लिए कंपनी के कंप्यूटर का व्यापक उपयोग किया। कुछ समय बाद वे अलग हो गए, और लड़की ने लड़के के अंतरराष्ट्रीय ग्राहकों से संवाद करने के लिए "भारतीय बार एसोसिएशन" जैसे नकली ईमेल खाते बनाना शुरू कर दिया। उसने बैंक के कंप्यूटर पर ऐसा किया। लड़के की कंपनी ने बहुत सारा व्यवसाय खो दिया, इसलिए उसने बैंक के खिलाफ मुकदमा दायर किया। बैंक को अदालत ने उत्तरदायी पाया क्योंकि ईमेल बैंक के सिस्टम का उपयोग करके भेजे गए थे।

साइबर अपराध रोकने की तकनीक

1. प्रत्येक कर्मचारी के पास एक उपयोगकर्ता खाता होना चाहिए, और नीति के अनुसार हर तीन महीने में पासवर्ड अपडेट करना अनिवार्य होना चाहिए। यह जरूरी है कि कर्मचारी बिना अनुमति वाले सॉफ्टवेयर को डाउनलोड या इंस्टॉल न कर सकें।
2. हर कर्मचारी को अज्ञात प्रेषकों से ईमेल अटैचमेंट डाउनलोड करने या खोलने में शामिल जोखिमों के बारे में जागरूक किया जाना चाहिए। कर्मचारियों को संगठन के बारे में निजी जानकारी का खुलासा या आदान-प्रदान न करने के महत्व के बारे में सूचित करें।
3. बैंक के आईटी विभाग को यह सुनिश्चित करना होगा कि इंटरनेट से जुड़े प्रत्येक वर्कस्टेशन और डिवाइस में फायरवॉल चालू हो, क्योंकि वे अनधिकृत स्रोतों से किसी भी संचार को सिस्टम में आने से रोकते हैं।
4. नेटवर्क पर रैनसमवेयर या खतरनाक मैलवेयर की मौजूदगी का पता लगाने के लिए हर पीसी पर एंटी-स्पाइवेयर और एंटी-वायरस सॉफ्टवेयर इंस्टॉल किया जाना चाहिए। वायरलेस नेटवर्क और सभी पासवर्ड को सुरक्षित और संरक्षित रखने की आवश्यकता है।
5. मोबाइल उपकरणों का उपयोग करने वाले ग्राहकों की संख्या में वृद्धि के साथ, बैंकों को सत्यापन तकनीकों जैसे वेब-आधारित लेनदेन सत्यापन और गतिशील डिवाइस

प्रमाणीकरण को लागू करने की आवश्यकता है। 6. बैंकों को अपने ग्राहकों को उनके लेनदेन की वैधता की पुष्टि करने के लिए स्वचालित संदेश और सूचनाएं भेजने की आवश्यकता होती है।

1.4 भारतीय बैंकिंग प्रणाली

1.4.1 बैंकिंग का अर्थ

बैंकिंग दूसरों के लिए पैसे की सुरक्षा का व्यवसाय है। बैंक इस पैसे को उधार देते हैं, जिससे ब्याज मिलता है जो बैंक और उसके ग्राहकों के लिए मुनाफ़ा पैदा करता है।

बैंक एक वित्तीय संस्था है जिसे जमा स्वीकार करने और ऋण देने का लाइसेंस दिया गया है। लेकिन वे अन्य वित्तीय सेवाएँ भी प्रदान कर सकते हैं।

शब्द "बैंक" का तात्पर्य कई अलग-अलग प्रकार की वित्तीय संस्थाओं से हो सकता है - जिसमें बैंक और ट्रस्ट कंपनियाँ, बचत और ऋण संघ, क्रेडिट यूनियन या कोई अन्य प्रकार की संस्थाएँ शामिल हैं जो जमा स्वीकार करती हैं।

1.4.2 वित्तीय लेनदेन का अर्थ

वित्तीय लेनदेन एक समझौता या संचार है, जो खरीदार और विक्रेता के बीच भुगतान के लिए वस्तुओं, सेवाओं या परिसंपत्तियों का आदान-प्रदान करने के लिए होता है। किसी भी लेनदेन में दो या अधिक व्यवसायों या व्यक्तियों के वित्त की स्थिति में बदलाव शामिल होता है। एक वित्तीय लेनदेन में हमेशा एक या अधिक वित्तीय परिसंपत्तियाँ शामिल होती हैं, सबसे आम तौर पर पैसा या कोई अन्य मूल्यवान वस्तु जैसे सोना या चाँदी।

वित्तीय लेन-देन के कई प्रकार हैं। सबसे आम प्रकार, खरीद, तब होती है जब कोई वस्तु, सेवा या अन्य वस्तु पैसे के बदले उपभोक्ता को बेकाई जाती है। ज़्यादातर खरीद नकद भुगतान के साथ की जाती है, जिसमें भौतिक मुद्रा, डेबिट कार्ड या चेक शामिल हैं। भुगतान का दूसरा मुख्य रूप क्रेडिट है, जो बाद की तारीख में पुनर्भुगतान के बदले में धन तक तत्काल पहुँच प्रदान करता है।

1.4.3 भारत में बैंकों का वर्गीकरण

भारत में बैंकिंग प्रणाली का हिस्सा बनने वाले बैंकों को दो श्रेणियों में विभाजित किया जा सकता है - अनुसूचित बैंक और गैर-अनुसूचित बैंक।

❖ अनुसूचित बैंक

भारत में बैंकिंग प्रणाली के अंतर्गत अनुसूचित बैंकों से तात्पर्य उन वित्तीय संस्थाओं से है जो भारतीय रिज़र्व बैंक अधिनियम, 1934 की दूसरी अनुसूकाई में सूकाईबद्ध हैं। इस समावेशन का अर्थ है कि वे आरबीआई द्वारा निर्धारित विशिष्ट मानदंडों को पूरा करते हैं और इसके सख्त नियमों के अधीन हैं।

अनुसूकाई में सूकाईबद्ध होने के लिए बैंक को निम्नलिखित 2 शर्तें पूरी करनी होंगी:

1. इसकी चुकता पूंजी और आरक्षित निधि 5 लाख रुपये से कम नहीं होनी चाहिए, और
2. इससे आरबीआई को संतुष्टि मिलनी चाहिए कि उनके कामकाज का संचालन उनके जमाकर्ताओं के हितों के लिए हानिकारक तरीके से नहीं किया जा रहा है।

यदि कोई अनुसूचित बैंक इन शर्तों का उल्लंघन करता है तो उसे अनुसूकाई से हटा दिया जाता है।

अनुसूचित बैंक को निम्नलिखित लाभ मिलते हैं:

- आरबीआई से बैंक दर पर ऋण की सुविधा।
- क्लियरिंग हाउस की स्वचालित सदस्यता।
- भारतीय रिज़र्व बैंक से प्रथम श्रेणी विनिमय बिलों की पुनः छूट की सुविधा।

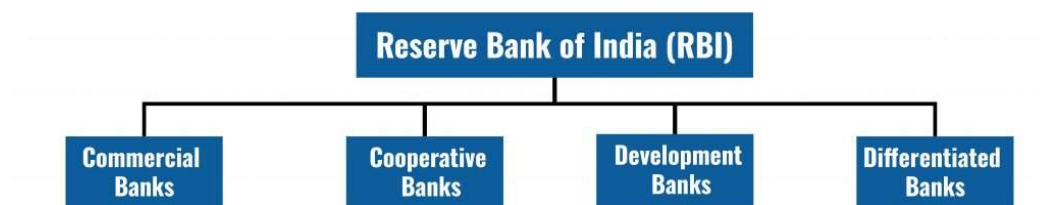
❖ गैर-अनुसूचित बैंक

भारत में बैंकिंग प्रणाली के अंतर्गत गैर-अनुसूचित बैंक उन वित्तीय संस्थाओं को कहा जाता है, जो भारतीय रिज़र्व बैंक अधिनियम, 1934 की दूसरी अनुसूकाई में शामिल किए जाने के मानदंडों को

पूरा नहीं करते हैं। अनुसूकाई से बाहर रखे जाने का अर्थ है कि वे अनुसूचित बैंकों की तुलना में अलग नियमों के तहत काम करते हैं।

1.4.4 भारत में बैंकिंग प्रणाली की संरचना

भारतीय रिज़र्व बैंक (RBI) भारत में बैंकिंग प्रणाली की संरचना के शीर्ष पर है और भारत के केंद्रीय बैंक के रूप में कार्य करता है। केंद्रीय बैंक के नीचे विभिन्न प्रकार के बैंक संचालित होते हैं, जिनकी चर्चा आगे के अनुभागों में की गई है।



भारतीय रिजर्व बैंक (आरबीआई)

- भारतीय रिजर्व बैंक (आरबीआई) भारत का केन्द्रीय बैंक है, अर्थात यह भारत की बैंकिंग प्रणाली का सर्वोच्च निकाय है।
- इसका स्वामित्व केंद्रीय वित्त मंत्रालय के पास है।
- यह एक नियामक निकाय के रूप में कार्य करता है, जो भारतीय बैंकिंग प्रणाली के विनियमन के साथ-साथ भारतीय अर्थव्यवस्था में मुद्रा आपूर्ति को नियंत्रित करने, जारी करने और बनाए रखने के लिए जिम्मेदार है।

भारतीय रिजर्व बैंक (आरबीआई) पर हमारे विस्तृत लेख में इसके उद्देश्यों, इतिहास, संरचना, कार्यों और अन्य संबंधित अवधारणाओं का अध्ययन किया जा सकता है।

वाणिज्यिक बैंक

- वाणिज्यिक बैंक भारत में बैंकिंग प्रणाली के अंतर्गत आने वाले उन बैंकों को कहते हैं जो वाणिज्यिक आधार पर चलते हैं। इसका मतलब है कि वे लाभ कमाने के लिए काम करते हैं और सेवाएँ प्रदान करते हैं।
- इन्हें बैंकिंग विनियमन अधिनियम, 1949 के तहत विनियमित किया जाता है।

उनकी संरचना, प्रकार, महत्व और अन्य संबंधित अवधारणाओं का अध्ययन भारत में वाणिज्यिक बैंकों पर हमारे विस्तृत लेख में किया जा सकता है।

सहकारी बैंक

- सहकारी बैंक भारत में बैंकिंग प्रणाली के अंतर्गत उन वित्तीय संस्थाओं को कहते हैं जो अपने सदस्यों के लिए सहयोग और पारस्परिक लाभ के सिद्धांतों पर काम करते हैं।
- वे उनके सदस्यों के हैं जो बैंक के मालिक और ग्राहक दोनों हैं।
 - इस प्रकार, यह कहा जा सकता है कि ग्राहक ही इन बैंकों के मालिक हैं।
- सहकारी बैंकों का नाम इसलिए रखा गया है क्योंकि इनका उद्देश्य हितधारकों का सहयोग प्राप्त करना है।

सहकारी बैंकों से संबंधित उनकी विशेषताएं, विनियमन, संरचना, महत्व और अन्य संबंधित अवधारणाओं का अध्ययन भारत में सहकारी बैंकों पर हमारे विस्तृत लेख में किया जा सकता है।

विकास बैंक

- विकास बैंकों को टर्म-लेंडिंग इंस्टीट्यूशंस (टीएलआई) या विकास वित्त संस्थान (डीएफआई) के रूप में भी जाना जाता है।
- वे भारत में बैंकिंग प्रणाली के अंतर्गत विशिष्ट वित्तीय संस्थान हैं जो भारतीय अर्थव्यवस्था के उन क्षेत्रों को दीर्घकालिक वित्त और सहायता प्रदान करते हैं जिनमें जोखिम अधिक है और जिन्हें वाणिज्यिक बैंकों से पर्याप्त ऋण नहीं मिल पाता है।

उनके प्रकार, भूमिका और अन्य संबंधित अवधारणाओं का अध्ययन भारत में विकास बैंकों पर हमारे विस्तृत लेख में किया जा सकता है।

विभेदित बैंक

- भारतीय बैंकिंग प्रणाली के अंतर्गत विभेदित बैंकों से तात्पर्य उन बैंकों से है जो ग्राहकों के एक विशिष्ट वर्ग को सेवाएं प्रदान करते हैं।
- विभेदित बैंकों की अवधारणा को भारतीय रिजर्व बैंक द्वारा 2013 में नचिकेत मोर समिति की सिफारिशों के आधार पर भारतीय बैंकिंग प्रणाली में पेश किया गया था, जिसका उद्देश्य किसी विशेष क्षेत्र के अनुरूप विशिष्ट सेवाएं या अनूठे उत्पाद प्रदान करना था।

उनके प्रकार, भूमिकाएं और अन्य संबंधित अवधारणाओं का अध्ययन भारत में विभेदित बैंकों पर हमारे विस्तृत लेख में किया जा सकता है।

1.4.5 सार्वजनिक क्षेत्र के बैंक का अर्थ

सार्वजनिक क्षेत्र के बैंक या राष्ट्रीयकृत बैंक वे हैं जिनमें सरकार ने सार्वजनिक हित के प्राथमिक उद्देश्य से अपनी अधिकांश हिस्सेदारी बरकरार रखी है।

आज़ादी के बाद भारत सरकार ने बैंकिंग कारोबार में उतरने के लिए 1955 में इंपीरियल बैंक ऑफ़ इंडिया का राष्ट्रीयकरण शुरू किया। भारतीय रिज़र्व बैंक ने 60% हिस्सा ले लिया और इसका नाम बदलकर स्टेट बैंक ऑफ़ इंडिया रख दिया।

1969 में भारत सरकार ने 14 और बैंकों का राष्ट्रीयकरण किया। 20वीं सदी के आखिरी दशक में सार्वजनिक क्षेत्र के बैंकों ने भारी वृद्धि हासिल की।

21वीं सदी की शुरुआत में कई राजनीतिक बदलावों ने सार्वजनिक क्षेत्र के बैंकों की वृद्धि को प्रभावित किया और इन बैंकों को भारी घाटा हुआ। 2002-03 में ये बैंक वृद्धि की राह पर लौट आए और ₹7780 करोड़ का लाभ कमाया।

भारत सरकार ने दस सार्वजनिक क्षेत्र के बैंकों को पुनर्गठित करने और कार्यक्षमता को अनुकूलित करने के लिए चार में विलय कर दिया, जिससे लाभ में उल्लेखनीय वृद्धि हुई। भारतीय स्टेट बैंक भारत और दुनिया भर में सबसे बड़े बैंकों में से एक है।

1.4.6 निजी क्षेत्र के बैंक का अर्थ

बैंक पैसे रखने के लिए सबसे सुरक्षित स्थानों में से एक हैं और इन्हें सबसे महत्वपूर्ण वित्तीय संस्थानों में से एक माना जाता है। बैंकों को जनता की वित्तीय ज़रूरतों को पूरा करने के लिए जाना जाता है। उन्हें बैंक में खाता खोलना होता है और वहीं से उनका वित्तीय रिकॉर्ड शुरू होता है। सभी बैंक एक ही सिद्धांत के तहत काम नहीं करते हैं। बैंकों के वर्गीकरण में दो श्रेणियां शामिल हैं, सार्वजनिक और वाणिज्यिक बैंक। समय के साथ, निजी क्षेत्र के बैंक भी पारदर्शिता और उत्कृष्टता के वर्षों के साथ विकसित हुए हैं। निजी और सार्वजनिक क्षेत्र के दोनों बैंक अपने ग्राहकों को उनके बैंकिंग अनुभव को सुखद और आरामदायक बनाने के लिए अधिक विकल्प प्रदान करते हैं। इस ब्लॉग में निजी क्षेत्र के बैंकों, उनके संचालन और उनके फायदे और नुकसान पर चर्चा की जाएगी।

निजी बैंक की इक्विटी का केंद्रीय हिस्सा या तो व्यक्तियों के समूह या निजी कंपनियों के पास होता है। हालाँकि, उन्हें स्वतंत्र वित्तीय रणनीतियों के अपने सेट के बावजूद केंद्रीय बैंक के दिशा-निर्देशों के नियमों और विनियमों का पालन करने की आवश्यकता होती है। इन बैंकों का कारोबार शेयर बाजार में होता है। अधिकांश निजी क्षेत्र के बैंक संचालन में उत्कृष्ट नवीन सेवा और दक्षता प्रदान करते हैं। हालाँकि, चूँकि वे लाभ-आधारित वित्तीय संस्थान हैं, इसलिए वे अतिरिक्त लागत पर कुशल सेवाएँ प्रदान करते हैं।

1990 के दशक में जब एलपीजी नीति की स्थापना हुई, तब वाणिज्यिक बैंक लोकप्रिय हो गए। इंडसैंड बैंक और एक्सिस बैंक देश के निजी क्षेत्र के सबसे पुराने बैंकों में से हैं। दोनों की स्थापना 1993 से 1994 के बीच भारत सरकार की अनुमति के बाद हुई थी।

1.4.7 विदेशी क्षेत्र बैंक का अर्थ

विदेशी बैंक वे बैंकिंग कंपनियाँ हैं जो मुख्यालय से अलग किसी दूसरे देश में शाखा खोलती हैं। इनका पंजीकृत कार्यालय एक देश में होता है। ये विदेशी बैंक दूसरे देशों में शाखा खोलते हैं। इसका उद्देश्य बहुराष्ट्रीय ग्राहकों को बेहतर सेवाएँ और सुविधा प्रदान करना है। विषय को बेहतर ढंग से समझने के लिए नीचे कुछ तथ्यों पर चर्चा की गई है।

- विदेशी बैंक अक्सर कॉर्पोरेट कंपनियों को सेवाएं देते हैं। इन कंपनियों की विभिन्न देशों में शाखाएं होती हैं।

- वे अपने देश के विशिष्ट बैंकों के साथ मिलकर काम करते हैं। ऐसे बैंक इन ग्राहकों की सेवा के लिए विदेशी बैंक भी खोलते हैं। इससे काम करने की प्रक्रिया आसान हो जाती है।
- विदेशी बैंक अक्सर कम कर वाले देशों का इस्तेमाल करते हैं। वे वहां शाखाएं खोलकर अधिक लाभ कमा सकते हैं।
- इसके अलावा, विदेशी बैंकों की पहचान और ग्राहक आधार बेहतर है। उनके पास विभिन्न देशों के ग्राहकों का पोर्टफोलियो है।
- इन विदेशी बैंकों को दोनों देशों के नियमों का पालन करना होता है। अपने गृह देश और शाखा देश के नियमों का पालन करना होता है। इसमें निगमन, ऋण देने, उधार लेने, संचालन आदि के लिए दिशा-निर्देश शामिल हैं।
- इसके अलावा, विदेशी बैंक अंतर्राष्ट्रीय व्यापार को भी आसान बनाते हैं। लोग ऐसे ही बैंक खातों के ज़रिए आसानी से काम कर सकते हैं।
- विदेशी बैंक भी सहयोग को बढ़ावा देते हैं। इससे अंतरराष्ट्रीय कंपनियों के लिए दरवाज़े खुलते हैं। वे भारतीय बैंकों के साथ प्रतिस्पर्धा करते हैं। इससे बाज़ार में स्वस्थ प्रतिस्पर्धा को बढ़ावा मिलता है।
- विदेशी बैंकों के पास भी ज़्यादा पूंजी होती है। ये बैंक किसी बड़े बैंक की सहायक कंपनी होते हैं। इसलिए, वे ज़्यादा उधार देने में सक्षम होते हैं।

भारत में विदेशी बैंकों की एक सूकाई है। इन शाखाओं को भारतीय नियमों का पालन करना होगा। साथ ही, उन्हें अपनी मुख्य कंपनी के दिशा-निर्देशों को पूरा करना होगा। इससे अक्सर विदेशी बैंकों के लिए नियम अधिक हो जाते हैं। लेकिन वे कम कर वाले देशों में लाभ कमाते हैं।

1.4.8 वित्तीय लेनदेन का प्रकार

❖ नकद लेनदेन

नकद लेनदेन वह लेनदेन है जिसमें पैसे का आदान-प्रदान किसी वस्तु, सेवा या अन्य वस्तु के लिए किया जाता है। नकद लेनदेन में भौतिक धन, जैसे सिक्के या नकदी, या डेबिट कार्ड से खरीदी

गई वस्तुएँ शामिल हो सकती हैं। ये क्रेडिट लेनदेन से भिन्न होते हैं क्योंकि पैसा तुरंत खरीदार से लिया जाता है और विक्रेता को दिया जाता है।

❖ क्रेडिट लेनदेन

क्रेडिट का उपयोग करने वाले लेन-देन में दी गई वस्तुओं या सेवाओं के लिए आस्थगित भुगतान शामिल होता है। जब क्रेडिट का उपयोग करके कुछ खरीदा जाता है, तो यह विक्रेता को एक परिसंपत्ति (बाद की तारीख में भुगतान) देता है और खरीदार को एक देयता (वह राशि जो बाद की तारीख में चुकाई जानी चाहिए) देता है। क्रेडिट कार्ड इसका एक उदाहरण है जब क्रेडिट का उपयोग किया जाता है, जहां कार्ड जारीकर्ता (आमतौर पर एक बैंक) ग्राहक को क्रेडिट की एक लाइन देता है जिसके साथ वे खरीदारी कर सकते हैं। ग्राहक द्वारा कार्ड के साथ अर्जित देयताओं का भुगतान आमतौर पर एक निर्धारित तिथि पर किया जाता है, और किसी भी अवैतनिक देयताओं पर जारीकर्ता के लिए ब्याज बनता है।

ऋण और बंधक ऋण के उदाहरण हैं। ऋणदाता उधारकर्ता को एकमुश्त राशि ("मूलधन") देने के लिए सहमत होता है, जो एक निश्चित अवधि (जिसे "अवधि" कहा जाता है) में उधार ली गई राशि का भुगतान करता है। ऋणदाता आमतौर पर उधार ली गई प्रारंभिक राशि के ऊपर एक अतिरिक्त प्रतिशत लेता है, जिसे "ब्याज दर" कहा जाता है। बंधक ऋण के समान होते हैं, लेकिन आमतौर पर बड़ी राशि और लंबी अवधि के लिए होते हैं, अक्सर अचल संपत्ति खरीदने के लिए। बंधक लगभग हमेशा संपार्श्विक द्वारा सुरक्षित होते हैं, सबसे आम तौर पर वे अचल संपत्ति होती हैं जिनका उपयोग उन्हें खरीदने के लिए किया जा रहा है। यदि उधारकर्ता बंधक पर आवश्यक भुगतान करने में विफल रहता है, तो ऋणदाता को फौजदारी के रूप में जानी जाने वाली प्रक्रिया में संपत्ति का दावा करने और बेचने का अधिकार है।

❖ आंतरिक और बाह्य लेनदेन

बाहरी लेन-देन कोई भी व्यावसायिक लेन-देन होता है जिसमें एक से अधिक पक्ष शामिल होते हैं। उदाहरण के लिए, किसी आपूर्तिकर्ता से इन्वेंट्री खरीदने वाली कंपनी को बाहरी माना जाएगा। सभी नकद और क्रेडिट लेन-देन बाहरी होते हैं, क्योंकि वे एक से अधिक व्यक्ति या समूह के वित्त को प्रभावित करते हैं। दूसरी ओर, आंतरिक लेन-देन केवल एक व्यवसाय को प्रभावित करते हैं।

किसी व्यवसाय में विभिन्न विभागों के बीच माल का स्थानांतरण एक आंतरिक लेन-देन है, क्योंकि यह कंपनी के समग्र वित्त को नहीं बदलता है।

1.5 साइबर सुरक्षा जोखिम और अनिश्चितता का नैतिक घटक

सभी नेताओं को निम्नलिखित प्रश्नों के उत्तर देने की दिशा में काम करना चाहिए: किसके लिए तकनीकी सुरक्षा उपयुक्त है? साइबर सुरक्षा की कौन सी डिग्री आवश्यक और वांछनीय है? दुख की बात है कि साइबर सुरक्षा एक "क्रूर मुद्दा" है, इसलिए इन चिंताओं को केवल तर्क से हल नहीं किया जा सकता है। बेतुके मुद्दों को संबोधित करना मुश्किल है क्योंकि इसका कोई एक, व्यावहारिक उत्तर नहीं है क्योंकि कई पक्षों के पास अलग-अलग उद्देश्य और दृष्टिकोण हैं। कमजोरी और अप्रत्याशितता पर ज़ोर देकर लोगों और सामूहिक नेटवर्क के साथ संबंध स्थापित करना संभव है, और ये आपातकालीन तैयारी, मानव लकाईलापन और तकनीकी सुरक्षा अध्ययनों में मौलिक विचार हैं।

व्यवसायों, सार्वजनिक स्थानों, इलेक्ट्रॉनिक सामान और निजी व्यवसायों के लिए सुरक्षा उपायों में बायोमेट्रिक सत्यापन में अधिक रुचि हो रही है। कंपनियाँ, व्यक्ति और व्यवसाय साइबरस्पेस को हमलावरों के साथ-साथ अन्य दुर्भावनापूर्ण अभिनेताओं से सुरक्षित रखने के लिए बायोमेट्रिक प्रमाणीकरण का उपयोग तेजी से कर रहे हैं।

1.6 साइबर अपराध की दुनिया में प्रमुख रुझान और नवाचार

उदाहरण के लिए, ब्लॉकचेन नवाचार बैंकिंग क्षेत्र को बदल रहे हैं, और कृत्रिम बुद्धिमत्ता और मशीन लर्निंग में हाल की प्रगति ने क्रांतिकारी वस्तुओं और प्रौद्योगिकियों के साथ-साथ कॉर्पोरेट अधिकारियों के लिए संगठनात्मक तकनीकों और प्रबंधन में आगे के योगदानकर्ताओं के रूप में प्रतिनिधित्व को प्रेरित करने की संभावनाओं से संबंधित व्यवसायों के लिए वातावरण को बदल दिया है (डेमिरकन एट अल., 2020; हस्सानी एट अल., 2018; हसानोवा एट अल., 2019)। क्लासिफायर की सटीकता में एक महत्वपूर्ण कारक फीचर फ़िल्टरिंग है, और XGBoost सुविधाओं की संख्या और प्रसंस्करण समय को कम करने के लिए एक उपयोगी तकनीक है (बरजावी एट अल., 2023)। मैलवेयर का पता लगाने के लिए एंड्रॉइड सुविधाओं के साथ, गतिशील मूल्यांकन एक विशेष रूप से अक्सर उपयोग की जाने वाली विधि है। अधिभोग में एल्गोरिदम के बीच, मशीन लर्निंग फ्रेमवर्क सबसे अधिक हिस्सा बनाता है। उपयोग किए जाने वाले अधिकांश

दक्षता उपाय सटीक हैं। न्यूरल नेटवर्क फ्रेमवर्क नॉन-न्यूरल नेटवर्क फ्रेमवर्क (पैन एट अल., 2020; हुसेन एट अल., 2023; चेरकी एट अल., 2023) से बेहतर काम करता है। हैकर्स द्वारा एल्गोरिदम को संशोधित करने के लिए मशीन लर्निंग (एमएल) पर आधारित प्रतिकूल तरीकों का उपयोग किया जा रहा है। इससे उन्हें सुरक्षा अनुप्रयोगों द्वारा पहचान से बचने और वित्तीय प्लेटफार्मों पर जटिल हमले शुरू करने में मदद मिलती है।

रैनसमवेयर हमले बैंकिंग संगठनों के लिए खतरनाक स्तर का खतरा पैदा करते हैं क्योंकि वे गोपनीय जानकारी को एन्क्रिप्ट करते हैं और इसे अनलॉक करने के लिए शुल्क की अपेक्षा करते हैं। इस तरह के हमले 2023 में वित्तीय उद्योग के लिए महत्वपूर्ण खतरा पैदा करते रहेंगे (ब्लेज़, 2023)। तकनीकी विकास के बावजूद आंतरिक जोखिम और जानकारी की चोरी जारी है। साइबर अपराधी निजी वित्तीय डेटा का अनधिकृत कब्ज़ा प्राप्त करने के लिए विशिष्ट हमले शुरू कर सकते हैं या कमज़ोर अंदरूनी लोगों का फ़ायदा उठा सकते हैं (AAG IT Support, nd; Porcedda, 2023; Georgiadou et al., 2022; Bamrara et al., 2013)। रैनसमवेयर के रूप में जाना जाने वाला खतरनाक मैलवेयर ट्रिगर होने के बाद लक्ष्य के डेटा को लॉक कर देता है और अक्सर साझा नेटवर्किंग स्टोरेज में फैल जाता है। जब तक हमलावरों को भुगतान नहीं मिल जाता और उन्हें सामग्री को अनलॉक करने वाला इलेक्ट्रॉनिक कोड नहीं मिल जाता, तब तक डेटा सुरक्षित रहता है। हैकर पुराने या ठीक नहीं किए गए सॉफ़्टवेयर की खामियों का फ़ायदा उठाते हैं। जब भी उन्हें कोई ऐसा सॉफ़्टवेयर वाला मशीन मिलता है जो किसी विशेष हमले के लिए कमज़ोर होता है, तो वे मशीन के अंदर सीधे रैनसमवेयर इंस्टॉल करने के लिए खामी का इस्तेमाल करते हैं। हैकर्स ऐसी मशीनों के लिए वेब पर खोज करते हैं।

एक बड़ी समस्या अज्ञात सेटों से मैलवेयर की पहचान है। भारी मात्रा में जानकारी के इंटरनेट से जुड़े साइबर सुरक्षा के क्षेत्र में सबसे बड़ी बाधा मैलवेयर खतरों और पायरेटेड सॉफ़्टवेयर की पहचान है। कुछ शोधपत्रों ने एक गहन शिक्षण-आधारित विधि प्रस्तावित की है जो मैलवेयर और पायरेटेड फ़ाइल पहचान को जोड़ती है (उल्लाह एट अल., 2019; पैन एट अल., 2020; इस्कैन एट अल., 2023)

फ़िशिंग सोशल इंजीनियरिंग के एक व्यवहार को संदर्भित करता है जो इच्छित शिकार को निजी डेटा का खुलासा करने के लिए मजबूर करने के लिए विभिन्न तकनीकों का उपयोग करता है, जिसमें उनका ईमेल पता, लॉगिन, लॉगिन क्रेडेंशियल और बैंकिंग विवरण शामिल हैं, लेकिन ये

शामिल नहीं हैं। फिर एक घुसपैठिया इस जानकारी का उपयोग अपने लक्ष्य के खिलाफ नकारात्मक तरीके से करता है (अलबदान, 2020; मोहम्मद एट अल., 2015; गोयनका एट अल., 2023; सफी और सिंह, 2023)।

आजकल, लोग अपना काफी समय ऑनलाइन स्पेस में बिताते हैं, जिसमें विभिन्न सार्वजनिक सेवाएँ, निजी प्लेटफ़ॉर्म और सोशल नेटवर्क शामिल हैं। ये स्थितियाँ महत्वपूर्ण हैं, इसलिए साइबर खतरों के खिलाफ़ मज़बूत सुरक्षा की आवश्यकता है - जो डेटा चोरी से लेकर सिस्टम में व्यवधान तक हो सकती है (गोयनका एट अल., 2023)। साइबरसिक्यूरिटी के रूप में जाना जाने वाला एक पूरा ढाँचा सूचना प्रौद्योगिकी प्लेटफ़ॉर्म के दुरुपयोग या अवैध उपयोग को रोकने के लिए प्रबंधक, प्रशासनिक और तकनीकी नियंत्रणों का उपयोग करता है। यह उपयोगकर्ताओं को संभावित खतरों और उल्लंघनों से बचाता है, इन प्लेटफ़ॉर्म के सुचारू संचालन की गारंटी देता है और उनकी निजी जानकारी की सुरक्षा को बनाए रखता है। हमलों, मैलवेयर और सूचना चोरी को रोकने के लिए, इस पेपर में साइबरसिक्यूरिटी विधियों की जाँच की गई है, जिसमें आर्टिफिशियल इंटेलिजेंस (AI) (खान एट अल., 2023) के कार्य पर विशेष जोर दिया गया है। इसके अलावा, यह साइबरसिक्यूरिटी में डीप लर्निंग और मशीन लर्निंग विधियों के अनुप्रयोगों और निहितार्थों पर जोर देते हुए प्रासंगिक शोध का एक संक्षिप्त सारांश प्रस्तुत करता है। परिणाम इस बात पर प्रकाश डालते हैं कि कंप्यूटर सिस्टम को मजबूत करने, दुर्भावनापूर्ण सॉफ़्टवेयर की क्रियाओं का अनुमान लगाने और समझने तथा अनजाने में शामिल होने और कंप्यूटर घुसपैठ को रोकने के लिए ये विधियाँ कितनी महत्वपूर्ण हैं (मिजविल एट अल., 2023)।

चिंताजनक आंकड़े दर्शाते हैं कि साइबर अपराध किस हद तक विश्व भर में एक खतरा बना हुआ है:

- इन हमलों की व्यापकता अनुमानित 53.35 मिलियन अमेरिकी व्यक्तियों में परिलक्षित होती है जो 2022 की शुरुआत में साइबर अपराधियों से प्रभावित थे (एएजी आईटी सपोर्ट, एनडी)।
- एफबीआई इंटरनेट अपराध डेटा के अनुसार, कम से कम 422 मिलियन लोग साइबर अपराध से प्रभावित हुए, जो इस मुद्दे की गंभीरता को उजागर करता है (पैलेटी, 2022)।
- पूर्वानुमानों के अनुसार, साइबर हमलों का आर्थिक प्रभाव 2023 तक 8 ट्रिलियन डॉलर और 2025 तक 10.5 ट्रिलियन डॉलर तक पहुंचने की उम्मीद है (ब्रूक्स, एनडी)।

- सिनोप्सिस के विश्लेषकों ने बताया कि 84% प्रोग्राम लाइब्रेरीज़ में कम से कम एक ओपन-सोर्स खतरा अवश्य होता है (ब्रूक्स, एन.डी.)।
- यह अनुमान लगाया गया है कि 2023 में साइबर अपराध का मूल्य करीब 224 बिलियन डॉलर होगा (क्रेन, 2023)।
- भारत में, धन की चोरी कई सामान्य साइबर अपराधों में से एक है, जिसमें इंटरनेट-आधारित बैंकिंग और यूपीआई जैसे प्लेटफॉर्म अक्सर शिकार होते हैं (हिंदुस्तान टाइम्स, 2023)।
- उद्योग में संभावित कमजोरियों को इस तथ्य से उजागर किया जाता है कि छोटे उद्यमों की साइबर सुरक्षा की प्राथमिकता घट रही है, जो 2022 में 80% से घटकर 2023 में 68% हो जाएगी (एएजी आईटी सपोर्ट, एनडी)।
- दुनिया भर में बैंकिंग क्षेत्र हैकिंग की घटनाओं से प्रभावित होता है, क्योंकि हैकर्स कमजोरियों का फायदा उठाकर अरबों संवेदनशील फाइलों को उजागर कर देते हैं (सिक््योरिटी इंटेलिजेंस, 2023)।
- बढ़ते खतरों के बावजूद, वित्तीय क्षेत्र के 51% संगठन बढ़ती चुनौती के जवाब में साइबर सुरक्षा खर्च बढ़ाने की योजना बना रहे हैं (स्टेटिस्टा, एनडी)।

1.7 उद्देश्य

1. भारतीय बैंकिंग प्रणाली में साइबर खतरों की पहचान और वर्गीकरण करना
2. बैंकिंग लेनदेन और ग्राहकों की वित्तीय सुरक्षा पर साइबर अपराधों के प्रभाव का मूल्यांकन करना
3. भारतीय बैंकों द्वारा अपनाई जा रही साइबर सुरक्षा नीतियों और उनके प्रभाव का अध्ययन करना
4. ग्राहकों और बैंक कर्मचारियों के बीच साइबर सुरक्षा जागरूकता के स्तर का विश्लेषण करना
5. भारतीय बैंकिंग प्रणाली की साइबर सुरक्षा को मजबूत करने के लिए नीतिगत ढांचा तैयार करना, सुधार और तकनीकी समाधान की सिफारिश करना

अध्याय 2 साहित्य की समीक्षा

इस अध्याय में विभिन्न शोधकर्ताओं, लेखकों और संस्थानों द्वारा किए गए पूर्व अध्ययनों का विश्लेषण प्रस्तुत किया गया है। इसमें साइबर सुरक्षा, साइबर अपराध, बैंकिंग प्रणाली में जोखिम, डिजिटल लेनदेन की सुरक्षा तथा तकनीकी नवाचारों से संबंधित शोधों की समीक्षा की गई है। यह अध्याय यह दर्शाता है कि अब तक इस क्षेत्र में क्या कार्य हुआ है और किन पहलुओं पर अभी भी शोध की आवश्यकता है।

अतुल (2013) संगठन संचार नेटवर्क के बिना सफल नहीं हो सकते जो दुनिया भर में सूचना के व्यापक स्रोतों को जोड़ते हैं, और सूचना प्रौद्योगिकी विशेषज्ञ समकालीन उच्च तकनीक उद्यमों की मांगों को पूरा करने के लिए उच्च प्रदर्शन वाले हार्डवेयर और सॉफ्टवेयर विकसित करने का प्रयास कर रहे हैं। साइबर अपराधियों की एक विविध सरणी से विशाल मात्रा में डेटा की सुरक्षा करने का संभावित खतरा समकालीन डिजिटल परिदृश्य में एक महत्वपूर्ण समस्या है। इस शोध का उद्देश्य भारत में चयनित बैंकों के खिलाफ साइबर अपराधियों द्वारा उपयोग की जाने वाली विविध साइबर-हमला तकनीकों को स्पष्ट करना है, जहां स्पीफिंग, ब्रूट फोर्स अटैक, बफर ओवरफ्लो और क्रॉस-साइट स्क्रिप्टिंग सार्वजनिक और निजी दोनों क्षेत्र के बैंकों के साथ सकारात्मक रूप से जुड़े हुए हैं। निष्कर्ष घुसपैठिए का पता लगाने और साइबर हमलों के बीच एक सकारात्मक सहसंबंध का संकेत देते हैं, जिसमें ऑनलाइन पहचान की चोरी, हैकिंग, दुर्भावनापूर्ण कोड, सेवा से इनकार (DOS) हमले और क्रेडिट कार्ड / ATM धोखाधड़ी शामिल हैं। इसके अतिरिक्त, ऑनलाइन पहचान की चोरी, DOS हमले और क्रेडिट कार्ड / ATM धोखाधड़ी सिस्टम मॉनिटरिंग के साथ सकारात्मक रूप से सहसंबद्ध हैं।

रज्जाक (2013) साइबर सभ्यता सूचना विनिमय और व्यावसायिक प्रयासों जैसे वाणिज्य, वित्तीय लेनदेन, खुदरा, सेवाओं और विज्ञापन के लिए एक महत्वपूर्ण मंच के रूप में उभरी है। ऑनलाइन उपयोग में तेजी से वृद्धि के साथ, साइबर अपराधी गतिविधियाँ भी काफी बढ़ रही हैं। मूल कारण यह है कि वर्ल्ड वाइड वेब के आगमन के साथ, उपयोगकर्ता की परवाह किए बिना, डेटा भंडारण और साझा करने के लिए वेब ऐप्स ने लोकप्रियता हासिल की। जैसे-जैसे समय बीतता गया, ऑनलाइन एप्लिकेशन अधिक जटिल होते गए, जिससे डिज़ाइन दोषों में तेज़ी से वृद्धि हुई जिसने इंटरनेट ब्राउज़िंग को पूरी तरह से खतरनाक बना दिया। 90 प्रतिशत से अधिक ऑनलाइन ऐप्स में डिज़ाइन या विकास संबंधी कमज़ोरियाँ थीं जिनका साइबर अपराधियों द्वारा आसानी से फ़ायदा

उठाया जा सकता है। ऑनलाइन एप्लिकेशन में ये कमज़ोरियाँ किसी भी उद्यम के व्यापार रहस्यों तक अनधिकृत पहुँच प्रदान कर सकती हैं। कभी-कभी, वेब एप्लिकेशन स्वयं कोई खतरा पैदा नहीं कर सकता है; फिर भी, इन ऐप्स में उपयोग की जाने वाली तकनीक अंतर्निहित कारण बन सकती है, जिससे प्रोग्राम अनधिकृत पहुँच के जोखिम में आ सकता है। वर्तमान में, सोशल नेटवर्क, इंटरनेट से जुड़े मोबाइल डिवाइस, व्यक्तिगत गोपनीयता और बैंकों जैसी संस्थाओं की ऑनलाइन कनेक्टिविटी साइबर अपराधियों के लिए सबसे आकर्षक लक्ष्य हैं। यह रिपोर्ट मौजूदा साइबर खतरों पर जोर देती है और औद्योगिक समाधानों के लिए इस्तेमाल की जाने वाली मौजूदा प्रणालियों और कार्यप्रणालियों की व्यापक समीक्षा प्रदान करती है। इस रिपोर्ट में कई महत्वपूर्ण औद्योगिक अनुप्रयोगों का भी मूल्यांकन किया गया है।

गाडे (2014) सूचना प्रौद्योगिकी के क्षेत्र में साइबर सुरक्षा आवश्यक है। समकालीन समाज में सूचना सुरक्षित करना सबसे महत्वपूर्ण मुद्दों में से एक बन गया है। जब भी हम साइबर सुरक्षा पर विचार करते हैं, तो सबसे पहला पहलू जो उभर कर आता है, वह है साइबर अपराधों का महत्वपूर्ण और बढ़ता प्रचलन। विभिन्न सरकारें और निगम इन साइबर अपराधों को रोकने के लिए कई रणनीतियाँ लागू कर रहे हैं। कई कदमों के बावजूद, साइबर सुरक्षा कई लोगों के लिए एक महत्वपूर्ण मुद्दा बनी हुई है। यह प्रस्तुति मुख्य रूप से उभरती हुई प्रौद्योगिकी के संबंध में साइबर सुरक्षा द्वारा सामना किए जाने वाले मुद्दों को संबोधित करती है। यह साइबर सुरक्षा प्रौद्योगिकी, नैतिकता और साइबर सुरक्षा के क्षेत्र को बदलने वाले रुझानों में नवीनतम विकास पर भी जोर देता है।

फिशर, ई.ए. (2015) सूचना और संचार प्रौद्योगिकी (ICT) क्षेत्र ने पिछले पचास वर्षों में उल्लेखनीय प्रगति की है। यह तकनीक सर्वव्यापी है और समकालीन संस्कृति के लगभग हर पहलू के लिए तेजी से आवश्यक होती जा रही है। ICT उपकरण और घटक अक्सर एक दूसरे से जुड़े होते हैं, और एक के बाधित होने से कई अन्य प्रभावित हो सकते हैं। हाल के वर्षों में, विशेषज्ञों और नीति निर्माताओं ने साइबर हमलों से ICT प्रणालियों की सुरक्षा के बारे में बढ़ती आशंकाओं को आवाज़ दी है, जो आने वाले वर्षों में आवृत्ति और गंभीरता दोनों में बढ़ने की आशंका है। ICT प्रणालियों और उनकी सामग्री की सुरक्षा को साइबर सुरक्षा कहा जाता है। साइबर सुरक्षा एक व्यापक और संभावित रूप से अस्पष्ट विषय है, जो महत्वपूर्ण होने के बावजूद कभी-कभी स्पष्ट परिभाषा से बच जाता है। इसे कभी-कभी गोपनीयता, सूचना विनिमय, खुफिया संग्रह और निगरानी सहित अन्य विचारों के साथ गलत तरीके से भ्रमित किया जाता है। साइबर सुरक्षा

गोपनीयता की सुरक्षा और गैरकानूनी निगरानी को विफल करने के लिए एक महत्वपूर्ण तंत्र के रूप में कार्य करती है, जबकि सूचना विनिमय और खुफिया संग्रह साइबर सुरक्षा को बढ़ाने के लिए मूल्यवान साधन हैं। सूचना प्रणालियों के लिए जोखिम प्रबंधन को अच्छी साइबर सुरक्षा के लिए आवश्यक माना जाता है। हर हमले से जुड़े खतरे तीन कारकों पर निर्भर करते हैं: खतरे (हमलावर की पहचान), कमज़ोरियाँ (इस्तेमाल की जाने वाली विधियाँ) और प्रभाव (हमले के परिणाम)। अधिकांश साइबर हमलों के बहुत कम परिणाम होते हैं; लेकिन, महत्वपूर्ण बुनियादी ढाँचे के कुछ तत्वों का सफल उल्लंघन - मुख्य रूप से निजी क्षेत्र के स्वामित्व में - राष्ट्रीय सुरक्षा, अर्थव्यवस्था और व्यक्तिगत निवासियों के कल्याण और सुरक्षा को गहराई से प्रभावित कर सकता है। ऐसे जोखिमों को कम करने के लिए अक्सर खतरे के स्रोतों को खत्म करना, कमज़ोरियों को दूर करना और परिणामों को कम करना शामिल होता है। साइबर सुरक्षा में सरकार की ज़िम्मेदारी में संघीय प्रणालियों की सुरक्षा और गैर-संघीय प्रणाली सुरक्षा का समर्थन शामिल है। मौजूदा कानून के अनुसार, सभी संघीय एजेंसियों के पास अपने संबंधित नेटवर्क से संबंधित साइबर सुरक्षा दायित्व हैं, और अन्य एजेंसियों के पास महत्वपूर्ण बुनियादी ढाँचे के संबंध में क्षेत्र-विशिष्ट कर्तव्य हैं। संघीय एजेंसियाँ औसतन अपने वार्षिक ICT व्यय का लगभग 10% साइबर सुरक्षा के लिए आवंटित करती हैं। 50 से अधिक अधिनियम साइबर सुरक्षा के विभिन्न पहलुओं से संबंधित हैं, और अतिरिक्त कानून कम से कम 111वीं कांग्रेस के बाद से चर्चा में हैं। फरवरी 2013 में जारी कार्यकारी आदेश 13636 और राष्ट्रपति नीति निर्देश 21, सार्वजनिक और निजी क्षेत्रों के बीच स्वैच्छिक सहयोग और मौजूदा विनियामक शक्तियों के उपयोग के माध्यम से महत्वपूर्ण बुनियादी ढाँचे की साइबर सुरक्षा से संबंधित हैं। दिसंबर 2014 में पारित चार अधिनियम संघीय सूचना और संचार प्रौद्योगिकी (ICT), होमलैंड सुरक्षा विभाग (DHS) में साइबर सुरक्षा कार्यबल और DHS सूचना-साझाकरण पहल की सुरक्षा से संबंधित हैं। अतिरिक्त कानून में व्यापक सूचना विनिमय, अनुसंधान और विकास, महत्वपूर्ण बुनियादी ढाँचे की सुरक्षा, डेटा उल्लंघनों के बारे में पीड़ितों को सूचित करना, तथा साइबर अपराध विनियमन, अन्य मामलों के अलावा। कार्यकारी शाखा की गतिविधियाँ तथा प्रस्तावित कानून मुख्य रूप से साइबर सुरक्षा में कई मान्यता प्राप्त तत्काल आवश्यकताओं को पूरा करने का लक्ष्य रखते हैं। फिर भी, ये मांगें डिजाइन, प्रोत्साहन, आम सहमति तथा पर्यावरण से संबंधित अधिक जटिल दीर्घकालिक कठिनाइयों के ढाँचे के भीतर उत्पन्न होती हैं। 114वीं कांग्रेस के दौरान विधायी उपाय तथा प्रशासनिक कार्रवाइयाँ ऐसी कठिनाइयों को काफी हद तक प्रभावित कर सकती हैं।

राव, हर्षिता. (2019). प्रौद्योगिकी में प्रगति के साथ, भारतीय बैंकिंग क्षेत्र ने उभरते रुझानों और महत्वपूर्ण परिचालन परिवर्तनों के साथ तालमेल बनाए रखा है। विकास की आवश्यकता ने इस इकाई को पर्याप्त अवसर प्रदान किए हैं, जिससे बैंक आईटी विद्रोह के सबसे बड़े लाभार्थियों में से कुछ बन गए हैं। NEFT (नेशनल इलेक्ट्रॉनिक फंड ट्रांसफर), RTGS (रियल-टाइम ग्राँस सेटलमेंट), ECS (इलेक्ट्रॉनिक क्लियरिंग सर्विस) और मोबाइल लेनदेन जैसे विकासों द्वारा सुगम ऑनलाइन लेनदेन में वृद्धि बैंकिंग और वित्तीय मामलों में गहराई से जुड़ी प्रौद्योगिकी को दर्शाती है। फिर भी, एक सिक्के के दो पहलुओं के लिए, अवसरों में जोखिम शामिल हैं, और सफलता के साथ संबंधित चुनौतियाँ हैं। नतीजतन, कंप्यूटर और इंटरनेट प्रौद्योगिकी की तीव्र प्रगति के साथ, 'साइबर अपराध' नामक वैश्विक अपराधों के नए रूप परिदृश्य में उभरे हैं। अनिश्चित अवधि में, डिजिटल आपराधिक गतिविधियों के प्रकार और उदाहरण अधिक परिष्कृत और जटिल हो गए हैं। पिछले दशक में बैंक और वित्तीय संस्थाएँ लगातार डिजिटल अपराधियों के प्राथमिक लक्ष्य रहे हैं। अधिकांश साइबर आपराधिक गतिविधियों के पीछे मौद्रिक लाभ प्राथमिक प्रेरणा बनी हुई है, और निकट भविष्य में इसमें बदलाव की बहुत कम संभावना है। यह अध्ययन वित्तीय संस्थानों से जुड़े विभिन्न प्रकार के साइबर अपराधों और उनके संबंधित प्रभावों के विशिष्ट पहलुओं पर केंद्रित है। इसके अलावा, यह इन कदाचारों को सुविधाजनक बनाने वाले खतरे के कारकों की पहचान करता है और साइबर हमलों से निपटने में सहायता करने के लिए रणनीति तैयार करता है, जिससे भविष्य में बेहतर सुरक्षा के लिए रोकथाम को बढ़ावा मिलता है।

हुमायूँ (2020) साइबर सुरक्षा के क्षेत्र में साइबर अनुप्रयोगों को बढ़ाने और इन अनुप्रयोगों द्वारा सामना किए जाने वाले महत्वपूर्ण सुरक्षा जोखिमों को कम करने के लिए अनुसंधान में उल्लेखनीय वृद्धि हुई है। इस शोध का उद्देश्य प्रचलित साइबर सुरक्षा कमजोरियों को उजागर करना और उनका आकलन करना है। इस उद्देश्य को प्राप्त करने के लिए गहन मानचित्रण अनुसंधान किया गया, जिसके परिणामस्वरूप 78 मुख्य अध्ययनों की पहचान और विश्लेषण हुआ। चुने गए शोध के व्यापक अध्ययन के बाद, हमने महत्वपूर्ण सुरक्षा खामियों और उनकी व्यापकता को पहचाना। प्रकाशन स्थल, प्रकाशन के देश और प्राथमिक लक्षित अवसंरचनाओं और अनुप्रयोगों को चित्रित करने के लिए डेटा को एकत्र और मूल्यांकन किया गया। निष्कर्ष बताते हैं कि अब तक चर्चा की गई सुरक्षा रणनीतियाँ केवल सामान्य सुरक्षा चिंताओं को संबोधित करती हैं, और इस शोध में प्रस्तावित समाधानों को और अधिक अनुभवजन्य सत्यापन और व्यावहारिक अनुप्रयोग की आवश्यकता है। इसके अलावा, हमारे निष्कर्ष बताते हैं कि इस अध्ययन में शामिल अधिकांश

शोध केवल सीमित संख्या में प्रचलित सुरक्षा कमजोरियों पर केंद्रित थे, जिनमें फ़िशिंग, सेवा से इनकार और मैलवेयर शामिल हैं। भविष्य के शोध में शोधकर्ताओं और चिकित्सकों को बेहतर जानकारी प्रदान करने के लिए महत्वपूर्ण साइबर सुरक्षा कमजोरियों, लक्षित अनुप्रयोगों, शमन रणनीतियों और अवसंरचनाओं की पहचान करनी चाहिए।

स्टैनिकज़र्ड (2021) वित्तीय उद्योग में ऐसे संगठन और संस्थान शामिल हैं जो वाणिज्यिक और खुदरा दोनों तरह के ग्राहकों को वित्तीय सेवाएँ प्रदान करते हैं। इसमें बैंकिंग, निवेश या बीमा फ़र्म और रियल एस्टेट उद्यमों सहित कई तरह के क्षेत्र शामिल हैं। वित्तीय संस्थान साइबर हमलों के प्रति संवेदनशील होते हैं। बैंक पूंजी के भंडार के रूप में काम करते हैं और साइबर अपराधियों के लिए इन संस्थानों पर हमला करना जबरन वसूली, चोरी और धोखाधड़ी के ज़रिए मुनाफ़ा कमाने के कई रास्ते खोल देता है। साथ ही, राष्ट्रीय सरकारें राजनीतिक और वैचारिक प्रभाव डालने के उद्देश्य से हैकर्स को वित्तीय सहायता प्रदान कर सकती हैं। ग्लोबल फ़ाइंडेक्स की रिपोर्ट है कि 2011 से 1.2 बिलियन से ज़्यादा लोगों ने बैंक खाते बनाए हैं। इस शोध का उद्देश्य वित्तीय अपराध को कम करने और सीआईए ट्रायड को पूरा करने में मौजूदा साइबर सुरक्षा उपायों की प्रभावकारिता का आकलन करना है, साथ ही संभावित संवर्द्धन के लिए सुरक्षा सुझाव तैयार करना है।

श्रीमती कल्पना नायर (2021) साइबर-सुरक्षा का मामला हमारे अस्तित्व के लिए उतना ही आवश्यक है जितना कि तकनीक। वास्तव में, वे अविभाज्य हैं: हमारी आर्थिक जीवन शक्ति, राष्ट्रीय सुरक्षा और हमारे समाज का मूल ढांचा अब उस तकनीक द्वारा परिभाषित किया जाता है जिस पर हम प्रतिदिन निर्भर करते हैं। साइबर सुरक्षा हमारी राष्ट्रीय सुरक्षा, राष्ट्रीय हितों और आर्थिक विकास से संबंधित है। उपसर्ग 'साइबर' कंप्यूटर और सूचना युग से जुड़े किसी व्यक्ति, वस्तु या अवधारणा को दर्शाता है। ग्रीक शब्द "स्टीयरमैन" और "गवर्नर" से व्युत्पन्न, इस वाक्यांश का पहली बार साइबरनेटिक्स के क्षेत्र में उपयोग किया गया था, एक शब्द जिसे नॉर्बर्ट वीनर ने पेश किया था। साइबरस्पेस इंटरनेट के आभासी क्षेत्र को संदर्भित करता है, और इस डोमेन को नियंत्रित करने वाले नियमों को साइबर कानून कहा जाता है। सभी नेटिज़ेंस, या इंटरनेट नागरिक, इन साइबर कानूनों के अधीन हैं, जिनके पास एक तरह का सार्वभौमिक अधिकार क्षेत्र है। साइबर अपराध को ऐसे अपराध के रूप में परिभाषित किया जाता है जिसमें कंप्यूटर अपराध के लक्ष्य के रूप में कार्य करता है (जैसे हैकिंग, फ़िशिंग और स्पैमिंग) या किसी अवैध कार्य (बाल पोर्नोग्राफी और घृणा अपराध सहित) को अंजाम देने के लिए एक साधन के रूप में उपयोग किया

जाता है। साइबर अपराध को कंप्यूटर अपराध के रूप में भी जाना जाता है। साइबर अपराधी व्यक्तिगत जानकारी, कॉर्पोरेट व्यापार रहस्य प्राप्त करने या नापाक उद्देश्यों के लिए इंटरनेट का शोषण करने के लिए कंप्यूटर तकनीक का उपयोग कर सकते हैं। यह शोध अध्ययन भारतीय बैंकों द्वारा सामना की जाने वाली साइबर सुरक्षा चुनौतियों की जांच करता है। यह साइबर अपराधों के बारे में जनता के ज्ञान का आकलन करने में भी सहायता करता है।

तारिक शाहब (2021) इस शोध अध्ययन का उद्देश्य भारतीय बैंकिंग उद्योग द्वारा सामना की जाने वाली साइबर सुरक्षा कठिनाइयों की जांच करना है। वित्तीय क्षेत्र में प्रौद्योगिकी अपनाने और डिजिटलीकरण के तेजी से प्रसार ने बैंकों को हैकर्स के लिए आकर्षक लक्ष्य बना दिया है। अध्ययन विकासशील साइबर खतरों, भारतीय बैंकिंग उद्योग में निहित कमजोरियों और उन रणनीतियों की जांच करता है जिनका उपयोग संस्थान अपने साइबर सुरक्षा ढांचे को बेहतर बनाने के लिए कर सकते हैं। यह अध्ययन भारतीय बैंकिंग उद्योग में साइबर सुरक्षा के बारे में प्रासंगिक साहित्य, प्रकाशनों और केस स्टडीज़ की व्यापक जांच पर आधारित है।

वह वार्ड (2021) कोविड-19 महामारी ने स्वास्थ्य सेवा सूचना प्रणाली की स्थायित्व का परीक्षण किया है, इसलिए स्वास्थ्य और कल्याण के विश्वव्यापी उद्देश्य को प्राप्त करने की हमारी क्षमता में बाधा उत्पन्न हुई है। महामारी के कारण अस्पतालों, दवा व्यवसायों, अमेरिकी स्वास्थ्य और मानव सेवा विभाग, विश्व स्वास्थ्य संगठन और इसके सहयोगियों सहित कई अन्य को निशाना बनाकर हाल ही में कई साइबर हमले हुए हैं। इस समीक्षा का उद्देश्य महत्वपूर्ण साइबर सुरक्षा चुनौतियों, स्वास्थ्य सेवा क्षेत्र द्वारा लागू किए गए समाधानों और हाल ही में साइबर हमलों में वृद्धि को कम करने के लिए आवश्यक सुधारों की पहचान करना था, जैसे कि फ़िशिंग अभियान और रैनसमवेयर हमले, जो कोविड-19 महामारी के कारण कार्य प्रथाओं में परिवर्तन से उत्पन्न होने वाली प्रौद्योगिकी और कर्मियों की कमजोरियों का फायदा उठाते हैं। खोज सूत्र “(कोविड या स्वास्थ्य सेवा) और साइबर सुरक्षा” का उपयोग करके दो मुख्य वैज्ञानिक डेटाबेस (PubMed और Scopus) को क्लेरी करके एक स्कोपिंग अध्ययन किया गया था। रिपोर्ट, समाचार और उद्योग श्वेत पत्र शामिल किए गए थे यदि वे सीधे पहले प्रकाशित कार्यों से संबंधित थे या लेखन के समय एकमात्र सुलभ स्रोत थे। समकालीन विषयों, कठिनाइयों और समाधानों पर ध्यान केंद्रित करने के लिए पिछले दशक (2011-2020) के दौरान प्रकाशित केवल अंग्रेजी भाषा के लेखों का चयन किया गया था। हमने साइबर सुरक्षा में नौ प्राथमिक कठिनाइयों, ग्यारह आवश्यक समाधानों की पहचान की, जिनका उपयोग स्वास्थ्य सेवा संगठनों ने इन चुनौतियों से निपटने के लिए किया, और स्वास्थ्य

क्षेत्र के भीतर साइबर सुरक्षा क्षमताओं में वृद्धि की आवश्यकता वाले चार महत्वपूर्ण क्षेत्रों की पहचान की। महामारी के दौरान साइबर हमलों की सबसे उल्लेखनीय और प्रमुख तकनीकें फ़िशिंग, रैनसमवेयर, वितरित इनकार-सेवा हमले और मैलवेयर थीं। इस स्कोपिंग मूल्यांकन ने साइबर सुरक्षा समस्याओं, प्रस्तावित उपायों और सुधार की आवश्यकता वाले क्षेत्रों के साथ-साथ COVID-19 महामारी के दौरान स्वास्थ्य क्षेत्र पर हमला करने वाली सबसे महत्वपूर्ण साइबर हमले की पद्धतियों को चित्रित किया। हमने COVID-19 महामारी और संभावित भविष्य की महामारियों या महामारियों के दौरान साइबर सुरक्षा चुनौतियों पर स्वास्थ्य सेवा उद्योग को बहुमूल्य जानकारी प्रदान की।

सुगन्या, सुश्री के. (2022). साइबर अपराध और डेटा सुरक्षा हमेशा एक दूसरे से जुड़े होते हैं। साइबर अपराधी अवैध संचालन के लिए वित्तीय और आर्थिक क्षेत्रों की जानकारी तक अनधिकृत पहुँच प्राप्त करने का लगातार प्रयास करते रहते हैं। ऑनलाइन बैंकिंग उपयोगकर्ता ऑनलाइन बैंकिंग सेवाओं का उपयोग करते समय अपने वित्तीय डेटा की सुरक्षा को लेकर लगातार चिंता व्यक्त करते हैं। यह निस्संदेह ऑनलाइन बैंकिंग सेवाओं के उपयोग और ग्राहक व्यवहार को प्रभावित कर रहा है। मौजूदा खतरों को कम करने के तरीके के बारे में ऑनलाइन बैंकिंग उपयोगकर्ताओं को शिक्षित करना आवश्यक है। भारत में, कुछ बैंक अक्सर बड़े साइबर हमलों का शिकार होते हैं, जो न केवल महत्वपूर्ण और संवेदनशील जानकारी से समझौता करते हैं, बल्कि बड़े वित्तीय नुकसान भी उठाते हैं। यह लेख ऑनलाइन बैंकिंग सेवाओं पर साइबर जोखिमों के प्रभाव की जाँच करता है। अध्ययन का निष्कर्ष है कि डिजिटल बैंकिंग और संवेदनशील वित्तीय जानकारी से जुड़े संभावित साइबर अपराधों के बारे में उपभोक्ता ज्ञान को बढ़ाने की आवश्यकता है। कार्ड और इंटरनेट लेनदेन के दौरान कमजोरियों को रोकने के लिए नवीनतम विकास के बारे में जानकारी होना।

शैरगोजरी (2022) साइबर सुरक्षा समकालीन सूचना, संचार और प्रौद्योगिकी-संचालित परिदृश्य में एक जटिल और लगातार बदलती सुरक्षा चिंता के रूप में विकसित हुई है। वैश्विक अर्थव्यवस्था और बुनियादी ढाँचा सूचना और संचार प्रौद्योगिकी (ICT) पर अधिक निर्भर होने के कारण साइबर हमले अधिक प्रचलित होने की आशंका है। कंप्यूटर और इंटरनेट पर बढ़ती निर्भरता ने दुनिया भर में साइबर हमलों में वृद्धि की है। इन हमलों के प्राथमिक लक्ष्य हमेशा व्यक्ति, संगठन और सरकारें रहे हैं। सूचना और संचार प्रौद्योगिकी (ICT) को कुछ राष्ट्रों द्वारा रणनीतिक युद्ध के लिए एक थिएटर और राष्ट्रीय सुरक्षा को बढ़ाने के लिए एक रणनीतिक संपत्ति के रूप में देखा जा रहा

है। यह महत्वपूर्ण है क्योंकि राष्ट्रीय सुरक्षा खतरे में है। यह लेख सुरक्षा मुद्दों पर वर्तमान प्रवचन में साइबर सुरक्षा की प्रासंगिकता की जांच करता है। लेखक इस विषय की समझ को बढ़ाने के लिए भारत के दृष्टिकोण से साइबर सुरक्षा का विश्लेषण करते हैं।

जेबारी (2022) इक्कीसवीं सदी में इंटरनेट सुरक्षा एक गंभीर समस्या है, खासकर जब अन्य ऑनलाइन मुद्दों के साथ इसका मूल्यांकन किया जाता है। तकनीकी उन्नति, संचार का विस्तार और साइबर-इंटरनेट के निर्माण ने सूचना और डेटा के प्रसारण के साथ-साथ ई-कॉमर्स में भी क्रांति ला दी है। नतीजतन, इलेक्ट्रॉनिक मौद्रिक खातों और डिजिटल वॉलेट को सुरक्षित करने के अलावा, ऑनलाइन सूचना और डेटा की सुरक्षा के तरीकों की पहचान करना अनिवार्य था। "साइबर सुरक्षा" शब्द में इंटरनेट पर सूचना सुरक्षा, इलेक्ट्रॉनिक संचालन सुरक्षा, नेटवर्क सुरक्षा और एप्लिकेशन सुरक्षा शामिल है। साइबर सुरक्षा में शत्रुतापूर्ण हमलों, हैकिंग, डेटा चोरी और तोड़फोड़ के खिलाफ सभी इंटरनेट से जुड़े इलेक्ट्रॉनिक उपकरणों पर डेटा और जानकारी की सुरक्षा के लिए उपयोग की जाने वाली रणनीतियाँ शामिल हैं। सभी इलेक्ट्रॉनिक गतिविधियों और अनुप्रयोगों को किसी न किसी तरह की साइबर सुरक्षा की आवश्यकता होती है, जिसमें वेबसाइट, वित्तीय संस्थान (जैसे बैंक और बैंक खाते), उपग्रह संचालन (सैन्य मिशन सहित) और ड्रोन नियंत्रण शामिल हैं।

बोगावे (2022) समकालीन और गतिशील डिजिटल परिदृश्य में, साइबर सुरक्षा जोखिम उद्यमों, संगठनों और लोगों की परिसंपत्तियों और सूचनाओं को खतरे में डालते हैं। साइबर खतरों के बढ़ने से डेटा उल्लंघन की संभावना बढ़ रही है, जिससे संगठन के ब्रांड और वित्तीय प्रदर्शन को काफी नुकसान पहुँच रहा है। संगठन की परिसंपत्तियों और सूचनाओं की सुरक्षा के लिए सुरक्षा प्रोटोकॉल स्थापित किए जाने चाहिए। इस उद्देश्य को प्राप्त करने का सबसे कुशल तरीका एक संपूर्ण साइबर सुरक्षा योजना के क्रियान्वयन के माध्यम से है। 406 चोरों के लिए एक प्रमुख लक्ष्य है जो वैध बैंकों जैसी नकली वेबसाइटों या फ़िशिंग ईमेल का उपयोग करके उपयोगकर्ताओं के खातों में घुसपैठ कर सकते हैं। निगमों और लोगों से संवेदनशील जानकारी प्राप्त करने में हैकर्स की बढ़ती हुई परिष्कार के कारण हाल के वर्षों में डेटा उल्लंघन की घटनाओं में वृद्धि हुई है। साइबर अपराध ऑनलाइन बैंकिंग की सुरक्षा के लिए एक बढ़ता हुआ खतरा पैदा करता है, जिससे ग्राहकों के लिए यह पता लगाना मुश्किल हो जाता है कि उनकी जानकारी हैक हुई है या नहीं। यह शोधपत्र ऑनलाइन बैंकिंग और लेन-देन से जुड़े साइबर सुरक्षा जोखिमों में वर्तमान रुझानों की जांच करता है।

माझी, डॉ. (2022). भारतीय बैंकिंग व्यवसाय ऐतिहासिक रूप से स्थापित है, और यह स्पष्ट है कि महत्वपूर्ण परिवर्तन केवल उदारीकरण की अवधि के दौरान ही हुए हैं। भारतीय बैंकिंग प्रणाली को नैतिक प्रथाओं, वित्तीय चुनौतियों और कॉर्पोरेट प्रशासन सहित प्रभावी रूप से नियंत्रित और देखरेख की जाती है। इसे देश के केंद्रीय बैंक, अर्थात् भारतीय रिजर्व बैंक द्वारा नियंत्रित और सावधानीपूर्वक देखरेख की जाती है। प्रौद्योगिकी में सुधार ने निस्संदेह भारतीय बैंकिंग क्षेत्र को बढ़ते रुझानों और आवश्यक परिचालन सुधारों के साथ संरेखित किया है। प्रौद्योगिकी की तीव्र प्रगति ने बैंकिंग उद्योग को पर्याप्त अवसर प्रदान किए हैं, जिससे बैंक सूचना प्रौद्योगिकी क्रांति के प्राथमिक लाभार्थियों में से एक बन गए हैं। NEFT (नेशनल इलेक्ट्रॉनिक फंड ट्रांसफर) जैसी तकनीक का उपयोग करके इंटरनेट लेनदेन में वृद्धि। RTGS (रियल-टाइम ग्रांस् सेटलमेंट), ECS (इलेक्ट्रॉनिक क्लियरिंग सर्विस), और मोबाइल लेनदेन बैंकिंग और वित्तीय मामलों में स्थापित तकनीक का उदाहरण हैं। भारतीय रिजर्व बैंक वित्तीय स्थिरता सुनिश्चित करने के लिए इंटरनेट बैंकिंग के कानूनी अनुपालन की जांच कर रहा है। इसके विपरीत, सुरक्षा जोखिम इंटरनेट बैंकिंग को काफी प्रभावित करते हैं। जैसे-जैसे तकनीक आगे बढ़ रही है, साइबर अपराध आभासी क्षेत्र को तेजी से खतरे में डाल रहे हैं, क्योंकि व्यक्ति और व्यवसाय इंटरनेट पर अपनी विशेष निर्भरता के कारण खतरनाक गति से इसके शिकार बन रहे हैं। इंटरनेट और अन्य तकनीकों के उपयोग ने दुनिया भर में साइबर अपराधियों के हमलों की संभावना को बढ़ा दिया है, जिससे वित्तीय गतिविधियों पर काफी असर पड़ रहा है। साइबर अपराधों में उल्लेखनीय वृद्धि के कारण, बैंकिंग उद्योग चोरी, फ़िशिंग, मैलवेयर संक्रमण, हैकिंग और इसी तरह की गतिविधियों की घटनाओं का केंद्र बन गया है। यह अध्ययन भारत में बैंकिंग उद्योग को प्रभावित करने वाले साइबर अपराधों के विभिन्न रूपों के तकनीकी आयामों का विश्लेषण करने का प्रयास करता है और इस क्षेत्र के अंदर इन साइबर अपराधों को कम करने के लिए प्रासंगिक सिफारिशें प्रदान करता है।

गोम्स (2022) इंटरनेट ने बैंकिंग उद्योग में क्रांति की शुरुआत की है, पिछले दो दशकों के दौरान परिचालन विधियों को बदल दिया है। अब व्यक्तियों के पास स्थानीय बैंक शाखा में जाने की आवश्यकता के बिना अपनी पसंद के स्थान से वित्तीय लेनदेन करने की क्षमता है। ई-बैंकिंग वित्तीय प्रणाली का एक अनिवार्य घटक बन गया है और अधिकांश व्यक्तियों के लिए लेनदेन का एक प्रचलित साधन बन गया है। एक उपयोगकर्ता के पास विभिन्न ऑनलाइन बैंकिंग तकनीकों के माध्यम से वित्तीय प्रबंधन के लिए कई तरह की संभावनाएँ हैं। हालाँकि इंटरनेट बैंकिंग ग्राहकों की सहायता करती है, लेकिन उन्हें अपने खातों को साइबर अपराधियों और हैकर्स से सुरक्षित

रखने के लिए सतर्क रहना चाहिए, क्योंकि सभी ऑनलाइन गतिविधियाँ सुरक्षा खतरों के लिए अतिसंवेदनशील होती हैं। अधिकांश बैंकिंग वेबसाइटों द्वारा अपनी जानकारी की सुरक्षा के लिए उपयोग किए जाने वाले इंटरनेट सुरक्षा प्रोटोकॉल विकसित हो रहे साइबर खतरों के संबंध में पुराने हो चुके हैं। इन मुद्दों ने अन्य पक्षों और हैकर्स द्वारा व्यक्तिगत वित्तीय जानकारी तक अनधिकृत पहुँच को सुगम बनाया है। डेटा उल्लंघनों को रोकने के लिए कई सुरक्षा तंत्रों के अस्तित्व के बावजूद, इन प्रणालियों के अंदर अंतर्निहित कमज़ोरियाँ बनी हुई हैं। इस शोध लेख का उद्देश्य भारत में ऑनलाइन बैंकिंग में साइबर सुरक्षा चिंताओं की व्यापकता और इन मुद्दों के बारे में उपभोक्ताओं के ज्ञान और उनके द्वारा उपयोग की जाने वाली निवारक कार्रवाइयों की जाँच करना है। हमारा अध्ययन ज्यादातर मूल डेटा पर आधारित है।

मानसी सुतार (2022) सूचना प्रौद्योगिकी के क्षेत्र में साइबर सुरक्षा एक महत्वपूर्ण भूमिका निभाती है। सूचना सुरक्षा सुनिश्चित करना निस्संदेह समकालीन समाज में सबसे महत्वपूर्ण मुद्दों में से एक के रूप में उभरा है। इंटरनेट के उपयोग ने व्यक्तियों और व्यवसायों को बाहरी हमलों के प्रति संवेदनशील बना दिया है। साइबर चिंताएँ ज्यादातर सूचना प्रौद्योगिकी क्षेत्र को प्रभावित करती हैं, जिसमें मैलवेयर, वायरस, सोशल इंजीनियरिंग और अन्य सहित कई प्रकार के शत्रुतापूर्ण हमले शामिल हैं। COVID-19 महामारी के दौरान, इंटरनेट पर निर्भरता काफी बढ़ गई है। यह शोध महामारी के दौरान साइबर हमलों की गति का विश्लेषण करता है और वित्तीय उद्योग पर उनके महत्वपूर्ण प्रभाव को प्रदर्शित करता है।

राय, डॉ. (2023). वित्तीय प्रौद्योगिकी, या फिनटेक, एक विस्तारित व्यवसाय है जिसने हाल के वर्षों में वित्तीय सेवा क्षेत्र को बदल दिया है। फिनटेक के उद्भव ने पारंपरिक बैंकिंग प्रक्रियाओं को बाधित कर दिया है, जिससे नए और आविष्कारशील समाधानों का विकास हुआ है। साइबर सुरक्षा हमलों की आवृत्ति और जटिलता बढ़ गई है, बैंकिंग उद्योग साइबर हमलावरों के लिए प्राथमिक लक्ष्य बन गया है। फिनटेक संगठनों के पास संवेदनशील डेटा की बड़ी मात्रा के कारण अलग-अलग साइबर सुरक्षा चिंताएँ हैं। साइबर सुरक्षा उल्लंघन के परिणाम महत्वपूर्ण हो सकते हैं, जिसमें वित्तीय नुकसान, प्रतिष्ठा को नुकसान और उपभोक्ता विश्वास का क्षरण शामिल है। यह शोध अध्ययन वित्तीय प्रौद्योगिकी (फिनटेक) और साइबर सुरक्षा के बीच संबंध का विश्लेषण करता है। फिनटेक एक उभरता हुआ व्यवसाय है जिसने उपभोक्ताओं को नए और आसान समाधान प्रदान करके वित्तीय सेवा क्षेत्र को बदल दिया है। फिर भी, प्रौद्योगिकी पर बढ़ती निर्भरता ने साइबर सुरक्षा खतरों और हमलों पर चिंताओं को बढ़ा दिया है। रिपोर्ट वित्तीय क्षेत्र में फिनटेक

की प्रगति और इसके बढ़ते महत्व की जांच करती है, साथ ही वित्तीय जानकारी की गोपनीयता, अखंडता और उपलब्धता की सुरक्षा के लिए मजबूत साइबर सुरक्षा प्रोटोकॉल की आवश्यकता पर भी ध्यान देती है। इसका उद्देश्य फिनटेक और साइबर सुरक्षा के अभिसरण की जांच करना है, जिसमें फिनटेक सेवाओं के उपयोग से उत्पन्न होने वाली कठिनाइयों और संभावनाओं पर जोर दिया गया है। लेख फिनटेक से जुड़ी कमज़ोरियों और खतरों की जांच करता है, जैसे डेटा उल्लंघन, धोखाधड़ी और साइबर हमले। यह इन खतरों को कम करने के लिए फिनटेक फर्मों द्वारा उपयोग की जाने वाली कई तकनीकों और उपकरणों का विश्लेषण करता है, जिसमें एन्क्रिप्शन, फ़ायरवॉल और बायोमेट्रिक्स शामिल हैं। यह अध्ययन फिनटेक क्षेत्र में वर्तमान साइबर सुरक्षा परिदृश्य और साइबर सुरक्षा को बेहतर बनाने की रणनीतियों की समझ का विस्तार करेगा। रिपोर्ट फिनटेक क्षेत्र के नियामक ढांचे और क्लाउड डेटा सुरक्षा और गोपनीयता की रक्षा के लिए अधिकारियों द्वारा लागू की गई कार्रवाइयों की जांच करती है। यह फिनटेक क्षेत्र की देखरेख और साइबर जोखिमों से बचाने में सरकारी संस्थाओं के कार्य की जांच करता है। अध्ययन अंततः फिनटेक और साइबर सुरक्षा के वैश्विक परिप्रेक्ष्य और भविष्य में अंतर्दृष्टि प्रदान करता है, सुरक्षा उपायों को बेहतर बनाने के लिए ब्लॉकचेन और कृत्रिम बुद्धिमत्ता जैसी नई तकनीकों की क्षमता पर प्रकाश डालता है।

सईद एस (2023) यह व्यवस्थित साहित्य विश्लेषण कॉर्पोरेट लकाईलापन प्राप्त करने के लिए डिजिटल परिवर्तन (DT) और साइबर सुरक्षा के निहितार्थों की जांच करता है। डिजिटल परिवर्तन संगठनात्मक प्रक्रियाओं को सूचना प्रौद्योगिकी समाधानों में परिवर्तित करना है, जिससे संभावित रूप से कंपनी के कई पहलुओं में पर्याप्त परिवर्तन हो सकते हैं। कृत्रिम बुद्धिमत्ता, बड़ा डेटा और एनालिटिक्स, ब्लॉकचेन और क्लाउड कंप्यूटिंग सहित उभरती हुई प्रौद्योगिकियाँ वैश्विक डिजिटल परिवर्तन को बढ़ावा देती हैं, जबकि इस परिवर्तन में लगी फर्मों के लिए साइबर सुरक्षा संबंधी चिंताएँ बढ़ जाती हैं। यह साहित्य सर्वेक्षण लेख दुर्भावनापूर्ण गतिविधियों या उपयोगकर्ताओं से संवेदनशील जानकारी को बदलने, नष्ट करने या जबरन वसूली करने की कोशिश करने वाले हमलावरों द्वारा अनधिकृत पहुँच के कारण होने वाले व्यवधानों को रोकने के लिए डिजिटल परिवर्तन कार्यान्वयन के दौरान साइबर सुरक्षा खतरों की गहन समझ की आवश्यकता पर जोर देता है। साइबर सुरक्षा डिजिटल परिवर्तन के लिए महत्वपूर्ण है क्योंकि यह साइबर हमलों से डिजिटल संपत्तियों की सुरक्षा करती है। इस अध्ययन में PRISMA दृष्टिकोण का उपयोग करके एक व्यवस्थित साहित्य समीक्षा का उपयोग किया गया। साहित्य अध्ययन से पता चला कि

डिजिटल परिवर्तन दक्षता और उत्पादन को बढ़ाता है जबकि डेटा उल्लंघनों और साइबर हमलों सहित साइबर सुरक्षा खतरों से जुड़ी नई समस्याओं को पेश करता है। हम डिजिटल परिवर्तन को अपनाने से जुड़ी संभावित कमजोरियों को संबोधित करके समाप्त करते हैं और मजबूत साइबर सुरक्षा रणनीतियों के माध्यम से इन जोखिमों को प्रबंधित करने के लिए उद्यमों को समाधान प्रदान करते हैं। यह दस्तावेज़ चरणबद्ध साइबर सुरक्षा तैयारी दृष्टिकोण की वकालत करता है, ताकि वाणिज्यिक संगठन प्रभावी रूप से डिजिटल परिवर्तन कर सकें।

लेस्माना (2023) आर्थिक परिवर्तन में डिजिटल प्रौद्योगिकी का उपयोग डिजिटल अर्थव्यवस्था के अंदर नई प्रौद्योगिकियों और विशेषताओं के आगमन से उत्पन्न होने वाले नए खतरे और जोखिम प्रदान कर सकता है। अर्थव्यवस्था के निष्पादक और नियामक के रूप में सरकारों के लिए डिजिटल आर्थिक परिवर्तन के बीच राष्ट्रीय अर्थव्यवस्था की सुरक्षा के लिए संभावित खतरों और खतरों को पहचानना आवश्यक है। राष्ट्रीय आर्थिक सुरक्षा के लिए जोखिमों को कम करने और खतरों को खत्म करने के लिए तैयार और निष्पादित उपायों की प्रभावशीलता लागू की गई नीतियों की गुणवत्ता और सटीकता पर निर्भर है। डिजिटल अर्थव्यवस्था में साइबर खतरों से जुड़े जोखिमों और कमजोरियों का आकलन करने के लिए एक संपूर्ण कार्यप्रणाली आवश्यक है और इसमें सभी आर्थिक गतिविधियों, विशेष रूप से आर्थिक ढांचे में प्रतिभागियों के बीच बातकाई शामिल होनी चाहिए।

सलमान (2023) प्रौद्योगिकी और इंटरनेट एक्सेस पर बढ़ती निर्भरता के कारण साइबर सुरक्षा लोगों, निगमों और सरकारों के लिए एक आवश्यक मुद्दा बनकर उभरी है। यह अध्ययन मैलवेयर, रैनसमवेयर और फ़िशिंग सहित साइबर हमलों द्वारा प्रस्तुत कई खतरों की जांच करता है, जो संवेदनशील जानकारी तक पहुँच प्राप्त करने या सिस्टम को नुकसान पहुँचाने के लिए सुरक्षा कमजोरियों का फ़ायदा उठाते हैं। यह डिजिटल सिस्टम की सुरक्षा और आवश्यक संचालन की निरंतरता को बनाए रखने के लिए व्यापक रक्षात्मक तरीकों की आवश्यकता को रेखांकित करता है। दस्तावेज़ साइबर हमलों की प्रगति पर जोर देता है, जो बुनियादी वायरस से लेकर उन्नत राज्य प्रायोजित हमलों तक होता है, और साइबर सुरक्षा को मजबूत करने के लिए आवश्यक घटकों को चित्रित करता है, जैसे कि खतरे का शमन, घटना प्रबंधन और उपयोगकर्ता शिक्षा। यह पेपर तकनीकी नवाचारों, विधायी संरचनाओं और राष्ट्रीय और अंतर्राष्ट्रीय दोनों स्तरों पर सहयोगी पहलों के माध्यम से साइबर सुरक्षा के लिए एक सक्रिय दृष्टिकोण की वकालत करता है।

सिंह (2023) साइबर सुरक्षा सूचना प्रौद्योगिकी क्षेत्र के लिए महत्वपूर्ण है। उपहार दिवस पर सबसे अधिक दबाव वाली समस्याओं में से एक अब डेटा सुरक्षा है। साइबर सुरक्षा के बारे में हमारी प्राथमिक चिंता साइबर अपराधों की बढ़ती व्यापकता है। कई सरकारें और उद्यम इन साइबर अपराधों को विफल करने के लिए विभिन्न उपायों को लागू कर रहे हैं। कई सुरक्षा उपायों के कार्यान्वयन के बावजूद, कई व्यक्तियों में अभी भी साइबर सुरक्षा को लेकर काफी डर है। इस पेपर का प्राथमिक फोकस उभरती प्रौद्योगिकियों में साइबर सुरक्षा का सामना करने वाली दूसरी चुनौती है। यह साइबर सुरक्षा तकनीकों, नैतिकता और डोमेन के भीतर लगातार बदलते रुझानों में नवीनतम प्रगति पर भी प्रकाश डालता है। सूचना प्रौद्योगिकी क्षेत्र में साइबर सुरक्षा महत्वपूर्ण है। यह पेपर मुख्य रूप से समकालीन प्रौद्योगिकी में साइबर सुरक्षा द्वारा सामना की जाने वाली चुनौतियों की जांच करता है। यह साइबर सुरक्षा तकनीकों, नैतिकता और डोमेन के भीतर नए रुझानों में नवीनतम प्रगति पर भी जोर देता है। उपहार दिवस के साथ एक महत्वपूर्ण मुद्दा डेटा सुरक्षा सुनिश्चित करना था। साइबर सुरक्षा ज्यादातर "साइबर अपराध" की धारणा को उजागर करती है, जो दैनिक आधार पर उल्लेखनीय रूप से बढ़ रही है। कई सरकारें और उद्यम इन साइबर अपराधों को विफल करने के लिए विविध तरीकों का उपयोग कर रहे हैं। कई सुरक्षा उपायों के लागू होने के बावजूद, कई व्यक्तियों में साइबर सुरक्षा को लेकर काफी डर बना हुआ है। कई सरकारें और उद्यम इन साइबर अपराधों को विफल करने के लिए विभिन्न उपायों को लागू कर रहे हैं। कई सुरक्षा उपायों के लागू होने के बावजूद, कई व्यक्तियों में अभी भी साइबर सुरक्षा को लेकर काफी डर बना हुआ है। यह अध्ययन बड़े पैमाने पर समकालीन प्रौद्योगिकी की साइबर सुरक्षा का सामना करने वाली चुनौतियों की जांच करता है। यह साइबर सुरक्षा तकनीकों, नैतिकता और डोमेन के भीतर लगातार विकसित हो रहे रुझानों में नवीनतम प्रगति पर भी प्रकाश डालता है।

अकेलो (2023) समकालीन नेटवर्क और डेटा-केंद्रित वातावरण में संगठनात्मक सूचना सुरक्षा एक महत्वपूर्ण मुद्दा है। जैसे-जैसे साइबर हमले अधिक लगातार और परिष्कृत होते जा रहे हैं, फर्मों को अपने संवेदनशील डेटा की गोपनीयता, अखंडता और उपलब्धता के लिए पर्याप्त जोखिम का सामना करना पड़ रहा है। यह दस्तावेज़ कॉर्पोरेट सूचना सुरक्षा से जुड़ी प्रमुख विशेषताओं और मुद्दों का अवलोकन प्रस्तुत करता है। यह बाहरी हमलों से बचाव के लिए फायरवॉल, घुसपैठ का पता लगाने वाली प्रणाली, एन्क्रिप्शन तकनीक और सुरक्षित कोडिंग पद्धतियों सहित कड़े सुरक्षा प्रोटोकॉल स्थापित करने की आवश्यकता को रेखांकित करता है।

यह सुरक्षा घटनाओं की कुशलतापूर्वक पहचान करने और उनका समाधान करने के लिए निरंतर निगरानी, खतरे की खुफिया जानकारी के प्रसार और घटना प्रतिक्रिया क्षमताओं की आवश्यकता को रेखांकित करता है। यह सर्वेक्षण उपयोगकर्ता के ज्ञान, प्रशिक्षण और सुरक्षा नीतियों और प्रक्रियाओं के अनुपालन के महत्व को दर्शाता है। अंदरूनी खतरों के जोखिम को कम करने और समग्र सुरक्षा स्थिति को बढ़ाने के लिए उद्यमों के अंदर सुरक्षा-केंद्रित संस्कृति विकसित करने की आवश्यकता को संबोधित किया गया है। बदलते खतरे का परिदृश्य, जिसमें उन्नत सतत खतरे, शून्य-दिन की कमजोरियाँ, तथा IoT और AI जैसी उभरती प्रौद्योगिकियों की सुरक्षा से संबंधित मुद्दे शामिल हैं, इन चुनौतियों से निपटने और निवारक रणनीतियों की प्रभावकारिता में सुधार करने के लिए निरंतर अनुसंधान और नवाचार की आवश्यकता को रेखांकित करता है।

शुक्र (2023) रोजमर्रा की गतिविधियों में इंटरनेट ऑफ थिंग्स (IoT) के तेजी से विस्तार ने संभावित साइबर सुरक्षा कमजोरियों के बारे में महत्वपूर्ण चिंताएँ पैदा की हैं। नतीजतन, सक्रिय और सक्रिय प्रतिक्रियाओं की वास्तविक आवश्यकता है। यह पत्र विभिन्न IoT उपकरणों से जुड़े वर्तमान साइबर सुरक्षा चिंताओं और खतरों का व्यापक साहित्य मूल्यांकन करता है। इसके अतिरिक्त, यह संरचनात्मक रूपरेखाओं के साथ-साथ प्रस्तावित उपाय भी प्रस्तुत करता है। इसके अलावा, यह विभिन्न तरीकों से संभावित जोखिमों का पता लगाने और उनकी पहचान करने में सहायता करता है। इसके अलावा, यह IoT से संबंधित औद्योगिक और आर्थिक क्षेत्रों में शोध की कमियों को उजागर करके योगदान देता है। हमारे परिणाम संकेत देते हैं कि IoT प्रणालियों में प्राथमिक चिंताएँ साइबर अपराध और गोपनीयता की समस्याएँ हैं। इसके विपरीत, आर्टिफिशियल इंटेलिजेंस साइबर सुरक्षा को बढ़ाने के लिए जबरदस्त संभावनाएँ प्रदान करता है। हालाँकि, कुछ खतरे, जैसे कि प्रमाणीकरण और गोपनीयता को लक्षित करने वाले, मौजूदा उपायों के कार्यान्वयन से अनसुलझे रहते हैं। इसके लिए वास्तव में प्रस्तावित बचावों के अधिक शोध और अनुभवजन्य परीक्षण की आवश्यकता है।

पेत्रु-क्रिस्टियन (2023) इस अध्ययन का उद्देश्य विकासशील जटिलता को स्पष्ट करना है, समकालीन साइबर युद्धों और उनके कई प्रभावों के बारे में पूरी जानकारी की तत्काल आवश्यकता पर प्रकाश डालना है। यह विश्लेषणात्मक उपकरणों की एक सरणी के साथ ऐसा करने का प्रयास करता है। 2011 से 2020 के दशक में, 50 उल्लेखनीय साइबर घटनाएँ साइबर जोखिम और सुरक्षा के क्षेत्र में महत्वपूर्ण केस स्टडी रही हैं। इन केस स्टडीज़ का विश्लेषण साइबर सुरक्षा के व्यापक प्रभावों और कठिनाइयों को समझने के लिए एक अलग दृष्टिकोण प्रदान करता

है। इसके अतिरिक्त, 2011 से 2020 तक के 50 केस स्टडीज़ में से प्रत्येक अलग-अलग कठिनाइयाँ, परिणाम और अंतर्दृष्टि प्रस्तुत करता है। उनका संयुक्त शोध पारंपरिक साइबर सुरक्षा समाधानों की अपर्याप्तता पर जोर देता है, प्रत्येक घटना के जटिल प्रभावों को रेखांकित करता है, दोनों तत्काल आर्थिक दृष्टि से और दीर्घकालिक विश्वास और प्रतिष्ठा संबंधी विचारों के संबंध में। इस शोध का उद्देश्य इन उदाहरणों के विवरणों की जाँच करना, स्थापित सुरक्षा ढाँचों की जाँच करना और साइबर निरोध दृष्टिकोणों की प्रभावकारिता का मूल्यांकन करना है।

सिंह, प्रभात. (2023) हम एक समकालीन, डिजिटल और वैश्वीकृत दुनिया में रहते हैं। जहाँ दक्षता और सुविधा प्रबल है, हालाँकि यह आसानी एक कीमत पर आती है। ई-बैंकिंग कई लाभ प्रदान करती है; फिर भी, यह चुनौतियों या मुद्दों से रहित नहीं है। ऐसा ही एक मुद्दा बैंकिंग उद्योग के अंदर साइबर सुरक्षा बनाए रखना है। यह अध्ययन साइबर खतरों के कई आयामों पर चर्चा करता है। भारत में साइबर सुरक्षा के लिए नियामक ढांचा। यह पेपर भारत में साइबर सुरक्षा के लिए अलग-अलग कानूनों की आवश्यकता पर अंतर्दृष्टि प्रदान करता है।

शेखर (2023) 21वीं सदी में, इंटरनेट तकनीक को बेहतरीन प्रदर्शन के लिए बढ़ाया गया है और सभी उपयोगकर्ताओं द्वारा इसका व्यापक रूप से उपयोग किया जाता है। डिजिटल बैंकिंग क्षेत्र शीर्ष पांच में है और लगातार NEFT, Google Pay और Ponape जैसी ऑनलाइन तकनीकों का उपयोग करता है। ऑनलाइन बैंकिंग के बढ़ते उपयोग के बावजूद, बैंकिंग उद्योग के भीतर साइबर अपराध पिछले कुछ वर्षों में बढ़ रहे हैं। यह कहा गया है कि 50% साइबर अपराध एटीएम, डेबिट कार्ड और ऑनलाइन बैंकिंग से जुड़े हैं। बैंकिंग उद्योग अन्य उद्योगों की तुलना में अधिक बार साइबर हमलों का सामना कर रहा है। यह अध्ययन बैंकिंग उद्योग में साइबर हमलों और ऐसे खतरों के खिलाफ साइबर सुरक्षा को बढ़ाने के तरीकों की जांच करता है।

भारद्वाज, शशांक. (2023). भारतीय बैंकिंग क्षेत्र ने प्रौद्योगिकी उन्नति के कारण उभरते रुझानों और महत्वपूर्ण परिचालन परिवर्तनों के अनुकूल खुद को ढाल लिया है। विकास की आवश्यकता द्वारा प्रस्तुत पर्याप्त अवसरों के कारण बैंक आईटी क्रांति के महत्वपूर्ण लाभार्थी रहे हैं। डिजिटल लेनदेन में तेजी से वृद्धि। बैंकिंग क्षेत्र ने अब NEFT, RTGS, ECS, मोबाइल बैंकिंग, UPI, ब्लॉकचेन, फिनटेक, क्लाउड कंप्यूटिंग, आर्टिफिशियल इंटेलिजेंस, बिग डेटा और वर्चुअल रियलिटी जैसी उभरती हुई तकनीकों के एकीकरण की ओर अपना ध्यान केंद्रित किया है, जो दर्शाता है कि किस हद तक तकनीक ने भारतीय बैंकिंग क्षेत्र के भीतर वित्तीय प्रणाली को बढ़ाया

है (मित्तल, 2020; तिवारी एट अल., 2021)। अवसरों में जोखिम शामिल हैं, और सफलता की अपनी बाधाएँ हैं (मित्तल और गौतम 2023)। "साइबर अपराध" शब्द आपराधिक शब्दावली में अपेक्षाकृत हाल ही में जोड़ा गया है, जो मुख्य रूप से 1990 के दशक के उत्तरार्ध में वित्तीय क्षेत्र में प्रौद्योगिकी की शुरूआत के साथ प्रमुखता प्राप्त कर रहा था। यह शोध अध्ययन मुख्य रूप से साइबर अपराधों के तकनीकी आयामों, वित्तीय उद्योग पर उनके प्रभाव और संबंधित मुद्दों और नतीजों को संबोधित करता है। इसके अलावा, यह आगामी खतरों के खिलाफ बेहतर और अधिक भरोसेमंद सुरक्षा उपायों की आवश्यकता को रेखांकित करता है। परिणामस्वरूप, जैसे-जैसे कंप्यूटर और इंटरनेट तकनीक तेज़ी से आगे बढ़ी, दुनिया भर में अपराधों की एक नई श्रेणी उभरी जिसे "साइबर अपराध" कहा जाता है। साइबर अपराध के प्रकार और पैटर्न समय के साथ और अधिक जटिल और परिष्कृत होते गए हैं। पिछले दशक में, बैंक और वित्तीय संस्थान हैकर्स के निशाने पर रहे हैं। इस संबंध में बदलाव की संभावना कम है; अधिकांश साइबर अपराधी उद्यम ज्यादातर मौद्रिक प्रोत्साहनों से प्रेरित रहते हैं। यह लेख मुख्य रूप से वित्तीय संस्थानों को प्रभावित करने वाले विभिन्न साइबर अपराधों और उनके परिणामों के तकनीकी पहलुओं की जाँच करता है। यह उन खतरे के वैक्टरों की भी जाँच करता है जो इन अपराधों को सक्षम करते हैं और भविष्य के साइबर हमलों को कम करने के उपाय तैयार करते हैं, जिससे ऐसे हमलों के खिलाफ सुरक्षा बढ़ जाती है।

रूपारेलिया, करिश्मा. (2023). बैंकिंग और वित्तीय सेवाओं की अर्थव्यवस्था में एक गतिशील भूमिका होती है। समकालीन बैंकिंग समाधान उन्नत तकनीक का उपयोग करते हैं, जिससे बैंकिंग के दृष्टिकोण से ग्राहक सुविधा और लागत दक्षता में वृद्धि होती है। नतीजतन, बैंकों को वित्तीय लेनदेन की अखंडता बनाए रखने और उपभोक्ता गोपनीयता की रक्षा करने के लिए बाध्य किया जाता है। फिर भी, इन उन्नत तकनीकों के उपयोग से साइबर सुरक्षा जोखिमों में उल्लेखनीय वृद्धि हुई है। बैंकिंग उद्योग द्वारा सामना किए जाने वाले साइबर जोखिम और खतरों को साइबर बीमा के अधिग्रहण से कम किया जा सकता है। साइबर बीमा व्यवसायों और व्यक्तियों को इंटरनेट से संबंधित खतरों से सुरक्षा प्रदान करता है। इस पत्र का उद्देश्य भारत में बैंकिंग उद्योग के सामने आने वाले बढ़ते साइबर सुरक्षा खतरों की जांच करना और इस क्षेत्र के लिए साइबर बीमा के महत्व का विश्लेषण करना है। यह अध्ययन भारतीय बीमा फर्मों द्वारा पेश किए जाने वाले कई साइबर बीमा मॉडलों का भी विश्लेषण करता है।

सी.पी., कृष्णा. (2024). डिजिटल बैंकिंग की तीव्र प्रगति ने साइबर सुरक्षा खतरों में वृद्धि की है, जिससे वित्तीय संस्थान और उनके ग्राहक खतरे में हैं। यह अध्ययन डिजिटल बैंकिंग में महत्वपूर्ण साइबर सुरक्षा चिंताओं, उनके परिणामों और रोकथाम के विकल्पों की जांच करता है। अध्ययन में अनुभवजन्य केस स्टडी और डेटा व्याख्या शामिल है, जो वर्तमान सुरक्षा समाधानों की प्रभावकारिता के बारे में जानकारी प्रदान करता है। विविध साइबर सुरक्षा चिंताओं, बदलते खतरे के माहौल और इन जोखिमों को कम करने में प्रौद्योगिकी के कार्य की गहन जांच प्रस्तुत की गई है। यह अध्ययन नियामक अनुपालन, नीतिगत सुझावों और साइबर सुरक्षा में उभरते रुझानों की जांच करता है।

पॉल (2024) यह सार बैंकिंग उद्योग के भीतर साइबर सुरक्षा का सारांश प्रस्तुत करता है, जिसमें भारतीय संस्थानों के लिए इसके महत्व, समस्याओं और निवारक रणनीतियों पर जोर दिया गया है। साइबर सुरक्षा में नेटवर्क सुरक्षा, एप्लिकेशन सुरक्षा और सूचना सुरक्षा जैसे क्षेत्रों सहित डिजिटल संपत्तियों को अवांछित पहुँच से सुरक्षित रखना शामिल है। भारतीय बैंकों को कई साइबर खतरों का सामना करना पड़ता है, जैसे फ़िशिंग योजनाएँ, डेटा उल्लंघन और रैनसमवेयर हमले, जिनके लिए मल्टी-फ़ैक्टर प्रमाणीकरण, नियमित सुरक्षा ऑडिट और स्टाफ़ प्रशिक्षण पहले जैसे कड़े निवारक उपायों की आवश्यकता होती है। साइबर जोखिमों से सफलतापूर्वक निपटने के लिए सेक्टर और सरकारी संस्थाओं के बीच सहयोग को ज़रूरी माना जाता है। तेज़ी से बदलते डिजिटल माहौल में बैंकिंग उद्योग में विश्वास, प्रतिष्ठा और स्थिरता को बनाए रखने के लिए साइबर सुरक्षा को महत्वपूर्ण माना जाता है।

इकबाल (2024) अध्ययन लेख का सारांश दें, साइबर सुरक्षा में नए रुझानों और संभावित मुद्दों को समझने के महत्व पर जोर दें। उद्देश्यों, दृष्टिकोण और प्रमुख परिणामों की जांच करें। उभरते साइबर खतरों से निपटने और डिजिटल बुनियादी ढांचे की सुरक्षा के लिए सक्रिय रणनीतियों की आवश्यकता पर प्रकाश डालें।

मूंदड़ा, आदर्श (2024). इस शोध का उद्देश्य वित्तीय संस्थानों पर साइबर अपराध के हानिकारक प्रभावों की जांच करना और इसके परिणामों को कम करने के लिए एक मजबूत साइबर सुरक्षा ढांचे का विकास करना है। हाल ही में बैंक इसके प्राथमिक लक्ष्य रहे हैं। भारत में कई बैंक अक्सर बड़े पैमाने पर मैलवेयर हमलों के अधीन होते हैं, जो निजी और संवेदनशील जानकारी से समझौता करते हैं और काफी वित्तीय नुकसान का कारण बनते हैं। इस शोध का उद्देश्य यह पहचानना है

कि कौन से उद्योग क्षेत्र साइबर हमलों के लिए अधिक संवेदनशील हैं और साइबर सुरक्षा नीतियों के विकास और अनुकूलन को सुनिश्चित करना है। रिपोर्ट में विभिन्न साइबर खतरों और अपराधों की केस स्टडी जांच शामिल है, जिसके कारण काफी वित्तीय नुकसान हुआ है, साथ ही सरकारी वेबसाइटों, शैक्षणिक प्रकाशनों और शोध पत्रों सहित विभिन्न इंटरनेट संसाधनों से प्राप्त द्वितीयक डेटा विश्लेषण भी शामिल है। यह लेख साइबर शासन के बारे में अंतर्दृष्टि प्रदान करेगा जो वित्तीय संस्थानों, बैंकों और बड़े पैमाने पर समाज को लाभान्वित करेगा।

शर्मा (2024) कोविड-19 के उभरने के बाद से, बैंकिंग उद्योग ने बैक-एंड और फ्रंट-एंड दोनों गतिविधियों में व्यापक डिजिटलीकरण किया है। नई तकनीक के आगमन से साइबर हमलों की आवृत्ति में लगातार वृद्धि हुई है। ऑनलाइन वित्तीय संस्थानों के प्रचलन ने रैनसमवेयर, फ़िशिंग हमले, गोपनीयता के मुद्दे और कई अन्य समस्याओं को जन्म दिया है। ऑनलाइन और मोबाइल दोनों सेवाएँ अपर्याप्त सुरक्षा उपाय प्रदर्शित करती हैं, जबकि साइबर खतरे प्रचलित हो रहे हैं। बैंकिंग उद्योग लगातार वित्तीय लाभ चाहने वाले हैकर्स का ध्यान आकर्षित करता है। यह शोध भारतीय बैंकिंग क्षेत्र पर साइबर अपराध के हानिकारक प्रभाव, साइबर जोखिमों को कम करने के लिए डिज़ाइन किए गए वर्तमान साइबर सुरक्षा ढाँचे और भारतीय बैंकिंग उद्योग की सुरक्षा के लिए रणनीतियों की जाँच करता है। शोध प्रकाशनों, शोध पत्रों, सरकारी पोर्टलों और समाचार वेबसाइटों सहित कई इंटरनेट स्रोतों से प्राप्त द्वितीयक डेटा का उपयोग करता है। हाल के वर्षों में पर्याप्त वित्तीय नुकसान के परिणामस्वरूप साइबर अपराधों के केस स्टडी भी आवश्यक हैं। यह लेख साइबर सुरक्षा रणनीतियों की जाँच करेगा जो सुरक्षा बढ़ाने के लिए रोके जा सकने वाले साइबर हमलों को कम करने में वित्तीय संस्थानों, बैंकों और समाज की सहायता कर सकती हैं।

शेहाब (2024) प्रौद्योगिकी हमारे जीवन के हर पहलू में महत्वपूर्ण है, खासकर वित्तीय उद्योग में। उन्नत प्रौद्योगिकियों ने बैंकिंग परिचालन में एक बड़ा परिवर्तन किया है। प्रौद्योगिकी के नापाक उपयोग के परिणामस्वरूप सुरक्षा उल्लंघन, उपभोक्ता विश्वास का हास, वित्तीय अस्थिरता और कई प्रकार की आपराधिकता होती है। यह लेख बैंकों और वित्तीय संगठनों के साथ जुड़ते समय विचार करने के लिए मुख्य खतरों और बाधाओं की जांच करता है। बैंकिंग और वित्तीय संस्थानों के क्षेत्र पर प्रचलित जोखिमों और हमलों की पहचान करने के लिए साहित्य के एक बड़े हिस्से की जांच की जाएगी, साथ ही उपयुक्त शमन रणनीतियों और प्रतिक्रियाओं के साथ। यह पत्र बैंकों और वित्तीय सेवा संस्थानों की वास्तुकला में कमजोरियों की जांच करता है जो उद्योग पर हमलों को तेज कर रहे हैं और बैंकिंग प्रणाली, लोगों और संगठनों को प्रभावित कर रहे हैं। इन 35

परियोजनाओं के सुरक्षा विश्लेषण से पता चलता है कि सुरक्षा बचाव और डेटा नियंत्रण उपायों में कमजोरियों के कारण साइबर हमले लगातार बैंकिंग उद्योग को निशाना बनाते हैं। मैलवेयर हमले बैंकों और वित्तीय संगठनों के लिए मुख्य खतरे हैं। सबसे सफल शमन रणनीतियों में बैंकों और वित्तीय संस्थानों के बीच सूचनाओं का आदान-प्रदान और आदान-प्रदान शामिल है, साथ ही कार्ड जारीकर्ताओं और उपयोगकर्ताओं द्वारा उपयोग की जाने वाली सर्वोत्तम प्रथाएँ भी शामिल हैं। कई पूर्व शोधों ने बैंकों और वित्तीय संस्थानों पर खतरों के प्रभाव को कम करने के साथ-साथ उन खतरों को कम करने के लिए एक प्रभावी दृष्टिकोण प्रदान किया है जिन्हें मौजूदा शमन रणनीतियों द्वारा संबोधित नहीं किया जा सकता है। बैंकों और वित्तीय सेवाओं के डेटा और सर्वेक्षणों के आधार पर, बैंकिंग और वित्तीय क्षेत्र में साइबर सुरक्षा जोखिमों और खतरों का निरंतर मूल्यांकन किया जा रहा है। रामी शेहब एट अल. का दावा है कि मौजूदा नियम और विनियम बैंकों और वित्तीय सेवा फर्मों की प्रणालियों को पर्याप्त रूप से सुरक्षित करने में विफल हैं।

भट्टाचार्य, सौरभ. (2024)। बैंकिंग क्षेत्र को साइबर अपराध से गंभीर खतरों का सामना करना पड़ रहा है, जिसके कारण इसके प्रभावों और साइबर सुरक्षा में भविष्य के रुझानों को समझने के लिए एक व्यापक विश्लेषण की आवश्यकता है। शोध साइबर खतरों की निरंतर वृद्धि और भारतीय वित्तीय बुनियादी ढांचे पर साइबर हमलों के हानिकारक प्रभाव को रेखांकित करता है। रिपोर्ट साइबर अपराध में वृद्धि, वित्तीय सेवा क्षेत्र के सामने आने वाली चुनौतियों और साइबर सुरक्षा में नवीन रणनीतियों की तत्काल आवश्यकता की जांच करती है। साइबर नियमों का पालन करना और हाल के घटनाक्रमों के बारे में जानकारी रखना जोखिमों को कम करने और बैंकिंग उद्योग की सुरक्षा के लिए महत्वपूर्ण है, क्योंकि साइबर हमले अधिक परिष्कृत हैं। लेखक बैंकिंग क्षेत्र में साइबर हमलों से निपटने के लिए समकालीन तकनीकों और रणनीतियों का प्रस्ताव करता है।

गोविंदराज (2024) भारत के बैंकिंग और वित्तीय उद्योग के तेजी से बदलते परिवेश में, साइबर अपराध एक महत्वपूर्ण खतरे के रूप में सामने आया है, जो आर्थिक स्थिरता और ग्राहक विश्वास को खतरे में डाल रहा है। यह लेख भारत के वित्तीय संस्थानों को प्रभावित करने वाली वर्तमान साइबर अपराध अर्थव्यवस्था का विश्लेषण करता है, साइबर अपराधियों से खतरों के स्पेक्ट्रम की जांच करता है, इन जोखिमों को कम करने के लिए संस्थानों द्वारा इस्तेमाल की जाने वाली रणनीति और आर्थिक विकास और उपभोक्ता इंटरैक्शन के लिए व्यापक प्रभाव डालता है। साइबर अपराधी सुरक्षा प्रोटोकॉल को दरकिनार करने के लिए उन्नत तरीकों का उपयोग करते हैं, जिससे

प्रभावित संगठनों को काफी वित्तीय नुकसान और प्रतिष्ठा को नुकसान होता है। यह रिपोर्ट साइबर अपराध के सामान्य प्रकारों, जैसे फ़िशिंग, रैनसमवेयर और उन्नत लगातार खतरों को वर्गीकृत करती है, और क्षेत्र की परिचालन लकाईलापन और वित्तीय स्थिरता पर उनके प्रभावों का मूल्यांकन करती है। अध्ययन बैंकों और वित्तीय संस्थानों द्वारा उपयोग किए जाने वाले रक्षात्मक तरीकों की जांच करता है, जो खतरे का पता लगाने और प्रतिक्रिया प्रक्रियाओं को बेहतर बनाने के लिए क्षेत्र के भीतर साइबर सुरक्षा प्रौद्योगिकी, नियामक ढांचे और सहयोगी पहलों में सुधार पर जोर देता है। इसके अलावा, यह आर्थिक विकास पर साइबर अपराध के प्रभावों की जांच करता है, इस बात पर प्रकाश डालता है कि कैसे चल रहे सुरक्षा उल्लंघन निवेशकों के विश्वास को खत्म कर सकते हैं और वित्तीय समावेशन पहलों को बाधित कर सकते हैं। रिपोर्ट ग्राहक संबंधों के लिए निहितार्थों की जांच करती है, इस बात पर ध्यान केंद्रित करती है कि साइबर घटनाएं उपभोक्ता विश्वास को कैसे प्रभावित करती हैं और ग्राहकों के विश्वास को पुनः प्राप्त करने और बनाए रखने के लिए संस्थानों को क्या कदम उठाने चाहिए। यह अध्ययन साइबर जोखिमों और वित्तीय स्थिरता के बीच संबंधों की जांच करता है ताकि साइबर अपराध के खिलाफ क्षेत्र की लकाईलापन बढ़ाने और सुरक्षित बैंकिंग वातावरण को बढ़ावा देने के लिए अंतर्दृष्टि प्रदान की जा सके।

शंकर (2024) आज की डिजिटल रूप से आपस में जुड़ी दुनिया में, बैंकिंग उद्योग अपने उपभोक्ताओं को सुचारू ऑनलाइन सेवाएँ प्रदान करने के लिए प्रौद्योगिकी पर बहुत अधिक निर्भर करता है। यह अध्याय बैंकिंग उद्योग के सामने आने वाले कई खतरों की गहन जाँच करता है, जिसमें तीन प्रमुख परिसंपत्तियों पर ध्यान केंद्रित किया गया है: ऑनलाइन बैंकिंग एक्सेस डिवाइस, नेटवर्क इंफ्रास्ट्रक्चर और केंद्रीकृत डेटा सेंटर/सर्वर। रिपोर्ट आंतरिक हमलों की जाँच करती है, अंदरूनी लोगों द्वारा प्रस्तुत जोखिमों को स्वीकार करती है और संभावित स्थितियों में अंतर्दृष्टि प्रदान करती है। अध्याय एक यथार्थवादी परिदृश्य को दर्शाता है जो बैंकिंग क्षेत्र में पहचाने गए खतरों और कमजोरियों के उपयोग का उदाहरण देता है। परिदृश्य स्पष्ट करता है कि कैसे समझौता किए गए उपकरण, नेटवर्क घुसपैठ और शोषित डेटा सेंटर कमजोरियों के परिणामस्वरूप संवेदनशील वित्तीय जानकारी लीक हो सकती है। अध्याय विविध सुरक्षा मुद्दों का विश्लेषण करके बैंकिंग उद्योग के भीतर जटिल सुरक्षा वातावरण को स्पष्ट करता है।

जैन (2024) वित्तीय सेवाओं का तेजी से डिजिटलीकरण डिजिटल बैंकिंग उद्योग के लिए ग्राहकों की संवेदनशील जानकारी की सुरक्षा में कई मुद्दे प्रस्तुत करता है। यह शोध पत्र डिजिटल बैंकिंग उद्योग के भीतर साइबर सुरक्षा चिंताओं की व्यापक जांच करता है। यह खतरों के कई स्रोतों पर

जोर देता है और पाठकों को साइबर खतरों के विभिन्न रूपों के बारे में सूचित करेगा जिनका वे सामना कर सकते हैं। यह अध्ययन साइबर धोखाधड़ी से बचने के लिए कई साइबर सुरक्षा रणनीतियों के उपयोग को भी संबोधित करता है। शोध ने डिजिटल बैंकिंग में समकालीन साइबर खतरों पर ध्यान केंद्रित किया और गहराई से जांच की कि धोखेबाज इन साइबर खतरों को कैसे अंजाम देते हैं। टैब्लॉइड ने अपने पाठकों को साइबर धोखाधड़ी के बारे में RBI की सिफारिशों के बारे में बताया। बैंकिंग उद्योग के भीतर साइबर धोखाधड़ी से बचाव के लिए कोई अलग विनियमन मौजूद नहीं है; इसलिए, ऐसे सभी अपराध सूचना प्रौद्योगिकी अधिनियम 2000 के तहत शासित होते हैं। रिपोर्ट ने बैंकिंग उद्योग के अंदर साइबर अपराध की जांच के लिए एक अलग जांच निकाय की स्थापना का प्रस्ताव रखा। दस्तावेज़ 2021 में एकीकृत लोकपाल प्रणाली के तहत RBI द्वारा स्थापित शिकायत निवारण साइट के बारे में बैंक के ग्राहकों को सूचित करने पर जोर देता है।

अफ़ज़ल (2024) साइबर अपराध में खतरनाक वृद्धि भारत में वित्तीय संस्थानों के लिए एक बड़ा खतरा है, खासकर बैंकों को प्रभावित कर रही है क्योंकि वे ई-बैंकिंग जैसे इंटरनेट-आधारित प्लेटफ़ॉर्म पर बहुत अधिक निर्भर हैं। अध्ययनों से लगातार पता चला है कि बैंक साइबर हमलों के लिए सबसे अधिक संवेदनशील उद्योगों में से एक हैं। यह शोध साइबर-सुरक्षा और प्रौद्योगिकी स्वीकृति मॉडल (TAM) के दृष्टिकोणों को एकीकृत करता है ताकि भारत में ई-बैंकिंग ग्राहकों के इन प्लेटफ़ॉर्म का उपयोग करने के इरादों पर साइबर धोखाधड़ी के प्रभाव की जांच की जा सके। परिणाम ई-बैंकिंग उपभोक्ताओं की साइबर सुरक्षा की समझ और ई-बैंकिंग सेवाओं का उपयोग करने की उनकी प्रवृत्ति के बीच एक अनुकूल संबंध दर्शाते हैं। उपयोगकर्ताओं की व्यवहारिक सुरक्षा की डिग्री साइबर सुरक्षा खतरों के बारे में उनके ज्ञान और जागरूकता से प्रभावित होती है। निष्कर्ष TAM ढांचे के साथ संरेखित होते हैं, यह प्रदर्शित करते हुए कि साइबर सुरक्षा ज्ञान, जागरूकता और व्यवहारिक सुरक्षा जैसे चार उपभोक्ताओं की ई-बैंकिंग प्रणालियों का उपयोग करने की इच्छा को बहुत प्रभावित करते हैं। साइबर धोखाधड़ी की बढ़ती घटनाओं को देखते हुए, ई-बैंकिंग ग्राहकों के बीच साइबर सुरक्षा जागरूकता में सुधार करना आवश्यक है। इससे न केवल उनके बैंक खाते सुरक्षित रहेंगे, बल्कि ई-बैंकिंग सेवाओं के प्रति उनकी स्वीकार्यता और विश्वास भी बढ़ेगा।

भुजंगाराव नायडू, पैचा. (2024)। यह शोध ऑनलाइन बैंकिंग और लेन-देन के सामने आने वाली उभरती साइबर सुरक्षा समस्याओं की गहन जांच पर केंद्रित है। डिजिटल युग में, चूंकि ऑनलाइन

वित्तीय सेवाएं हमारे रोजमर्रा के जीवन का आधार बनती जा रही हैं, इसलिए साइबर हमलों से जुड़े खतरों को समझना, उनका मूल्यांकन करना और उन्हें कम करना आवश्यक है। अध्ययन के लक्ष्यों में कई प्रासंगिक विषय शामिल हैं, जैसे कि फ़िशिंग, मैलवेयर, पहचान की चोरी और डेटा उल्लंघन, साथ ही विनियामक और अनुपालन चुनौतियाँ, मोबाइल बैंकिंग भेद्यताएँ, अंदरूनी जोखिम और विकासशील तकनीकों के प्रभाव। इस अध्ययन का उद्देश्य इन चुनौतियों का विश्लेषण करके व्यक्तियों, वित्तीय संस्थानों और विनियामक निकायों के लिए मूल्यवान अंतर्दृष्टि और व्यावहारिक सिफारिशें प्रदान करना है, अंततः समकालीन डिजिटल वित्तीय वातावरण में ऑनलाइन बैंकिंग और लेन-देन की सुरक्षा और विश्वसनीयता को बढ़ाने की कोशिश करना है।

दास (2024) भारतीय बैंकिंग प्रणाली, जिसकी शुरुआत पहले बैंक ऑफ़ हिंदुस्तान से हुई थी, ने राष्ट्रीयकरण, उदारीकरण और विलय के माध्यम से प्रगति की है, जिससे सेवा दक्षता, स्वचालन और परिचालन लागत में कमी आई है। बैंक यूपीआई और भीम जैसी डिजिटल भुगतान प्रणाली शुरू करके डिजिटलीकरण को प्राथमिकता दे रहे हैं, जबकि एनईएफटी, ईसीएस, आरटीजीएस और प्रीपेड कार्ड के माध्यम से कैशलेस समाज की वकालत कर रहे हैं। डिजिटल परिवर्तन परिचालन दक्षता, ग्राहक अनुभव और प्रतिस्पर्धी लाभ में सुधार करना चाहता है। प्रमुख डोमेन में डिजिटल प्लेटफ़ॉर्म, प्रक्रिया स्वचालन, कृत्रिम बुद्धिमत्ता, मशीन लर्निंग, रोबोट, अनुकूलित ग्राहक अनुभव, संधारणीय बैंकिंग प्रथाएँ, एक चुस्त कार्यबल और दूरस्थ नौकरी के अवसर शामिल हैं। तकनीकी सुधार बैंकों और वित्तीय संस्थानों पर साइबर हमलों को बढ़ा रहे हैं, जिसके परिणामस्वरूप गोपनीयता और फ़िशिंग संबंधी चिंताएँ हैं। वित्तीय डेटा की सुरक्षा, धोखाधड़ी को रोकने और सिस्टम की अखंडता को बनाए रखने के लिए साइबर सुरक्षा तकनीक आवश्यक है। महत्वपूर्ण तत्वों में परिष्कृत खतरे का पता लगाना, सहयोग, क्रांति-प्रतिरोधी एन्क्रिप्शन, कृत्रिम बुद्धिमत्ता, मशीन लर्निंग, एक साइबर सुरक्षा कार्यबल, एक शून्य-विश्वास वास्तुकला और घटना प्रतिक्रिया और सुरक्षा के लिए निरंतर निगरानी शामिल हैं।

चट्टा (2024) बटुए में नोटों की तुलना में प्लास्टिक कार्ड की संख्या अधिक होती है। भारतीय बैंकिंग क्षेत्र में परिवर्तन का श्रेय आईटी क्रांति को जाता है जिसका उद्देश्य विकसित और उभरते दोनों देशों के साथ प्रतिस्पर्धात्मकता को बढ़ाना है, जिसमें कई विनियामक कारक शामिल हैं, जिसके परिणामस्वरूप व्यवसाय के भीतर व्यापक बैंकिंग स्वचालन हुआ है। KPMG-CII विश्लेषण से संकेत मिलता है कि भारत में 2025 तक तीसरा सबसे बड़ा बैंकिंग बाजार और 2020 तक पांचवां सबसे बड़ा बैंकिंग बाजार बनने की क्षमता है। भारत के बैंकिंग क्षेत्र का मूल्य 81 ट्रिलियन रुपये

है और यह अन्य देशों के साथ प्रतिस्पर्धा में बने रहने के लिए उन्नत इंटरनेट अवसंरचना का उपयोग कर रहा है। भारतीय बैंकिंग प्रणाली में 26 सार्वजनिक क्षेत्र के बैंक, 20 निजी क्षेत्र के बैंक, 43 विदेशी बैंक, 61 क्षेत्रीय ग्रामीण बैंक (RRB) और 90,000 से अधिक ऋण सहकारी समितियाँ शामिल हैं। ऑनलाइन बैंकिंग की ओर बदलाव भारत की उभरती गतिशीलता से और बढ़ गया है, जिसे 2020 तक दुनिया के सबसे युवा देशों में से एक होने का अनुमान है, जिसकी औसत आयु 29 वर्ष है। यह युवा जनसांख्यिकी तकनीकी रूप से कुशल है और वास्तविक समय की इंटरनेट जानकारी चाहता है। आने वाले वर्षों में ऑनलाइन बैंकिंग ग्राहकों की अनुमानित तेज़ वृद्धि के साथ, ये सिस्टम हैकर्स और साइबर अपराधियों के लिए तेज़ी से प्रमुख लक्ष्य बन रहे हैं। बैंकिंग संस्थानों को ग्राहकों के विश्वास और संतुष्टि को बनाए रखते हुए ऑनलाइन बैंकिंग सिस्टम की सुरक्षा सुनिश्चित करने के लिए व्यापक प्रक्रियाओं को लागू करना चाहिए। साइबर सुरक्षा खतरों से बचाव के लिए, बैंकिंग संस्थानों को प्रभावी और कुशल ग्राहक जागरूकता कार्यक्रम स्थापित करने चाहिए, क्योंकि साइबर खतरों से सुरक्षा ऑनलाइन बैंकिंग सिस्टम के बारे में जागरूकता के स्तर पर निर्भर करती है, न कि केवल बैंक द्वारा स्थापित सुरक्षा उपायों और प्रथाओं पर निर्भर करती है। यह बैंकिंग प्रणाली की गोपनीयता और अखंडता को बनाए रखने के लिए वित्तीय संगठनों की क्षमता को जटिल बनाता है। अध्ययन उपयोगकर्ताओं के बीच ऑनलाइन बैंकिंग खतरों के बारे में जागरूकता का मूल्यांकन करेगा और उम्र और लिंग के आधार पर जागरूकता में किसी भी अंतर का आगे विश्लेषण करेगा।

डेलॉन, एल. (2024) यह रिपोर्ट भारत में वाणिज्यिक बैंकों द्वारा सामना की जाने वाली साइबर सुरक्षा कठिनाइयों की जांच करती है, जिसमें ऑनलाइन बैंकिंग सेवाओं से संबंधित साइबर खतरों पर विशेष जोर दिया गया है। भारत में दुनिया भर में साइबर अपराध की घटनाओं में वृद्धि के बावजूद, इन साइबर सुरक्षा मुद्दों से संबंधित समझ और राष्ट्रीय विनियमों में महत्वपूर्ण कमी है। अध्ययन संस्थागत और राष्ट्रीय दोनों स्तरों पर भारतीय वाणिज्यिक बैंकों की साइबर सुरक्षा तत्परता को प्रभावित करने वाले प्रमुख निर्धारकों का पता लगाने का प्रयास करता है। प्राथमिक लक्ष्य महत्वपूर्ण साइबर सुरक्षा खतरों का विश्लेषण करना, डिजिटल परिवर्तन के दौरान साइबर सुरक्षा जोखिमों को कम करने में नेतृत्व की भूमिका की जांच करना और साइबर सुरक्षा ढांचे और हितधारक जागरूकता को बेहतर बनाने के लिए समाधान प्रदान करना है। 2014 से 2024 तक प्रकाशित द्वितीयक सहकर्मि-समीक्षित साहित्य की व्यापक समीक्षा की गई। साहित्य अध्ययन में साइबर जोखिम में कमी और परिवर्तनकारी नेतृत्व के लिए सिस्टम थ्योरी मॉडल सहित कई विचार

शामिल थे। शोध में उद्योग को प्रभावित करने वाले तीन प्राथमिक साइबर हमले पाए गए: फ़िशिंग, सेवा से इनकार/वितरित सेवा से इनकार (DoS/DDoS), और रैनसमवेयर। इसने साइबर जागरूकता को बढ़ावा देने और डिजिटल संस्कृति में बदलाव को सुविधाजनक बनाने में परिवर्तनकारी नेतृत्व के आवश्यक कार्य पर जोर दिया। भारत में संभावित कार्यान्वयन के लिए कड़े कानून, सार्वजनिक-निजी भागीदारी के माध्यम से सूचना साझा करना और आधुनिक प्रौद्योगिकी में निवेश सहित अन्य देशों की रणनीतियों पर विचार किया गया। रिपोर्ट में कड़े राष्ट्रीय नियमों की स्थापना, बैंक कर्मियों की दक्षताओं में वृद्धि और जोखिम प्रबंधन के लिए सिस्टम थ्योरी मॉडल के उपयोग की वकालत की गई है।

अन्वेषा चक्रवर्ती (2024) भारतीय बैंकिंग उद्योग के तेजी से डिजिटल परिवर्तन ने वित्तीय सेवाओं में बेजोड़ आसानी और दक्षता ला दी है, जबकि साथ ही इसे उन्नत साइबर हमलों के प्रति संवेदनशील बना दिया है। यह लेख भारतीय बैंकिंग में बदलती साइबर सुरक्षा कठिनाइयों का विश्लेषण करता है, जिसमें फ़िशिंग, मैलवेयर, पहचान की चोरी और परिष्कृत AI-संचालित हमलों जैसे महत्वपूर्ण खतरों पर जोर दिया गया है। इस शोध में उपभोक्ता विश्वास, संगठनात्मक प्रदर्शन और परिचालन लकाईलेपन पर इन जोखिमों के प्रभावों की जांच करने के लिए गुणात्मक साहित्य समीक्षा और मात्रात्मक सर्वेक्षण विश्लेषण को एकीकृत करते हुए मिश्रित-पद्धति दृष्टिकोण का उपयोग किया गया। इसके अलावा, यह साइबर हमलों के खिलाफ़ एक रक्षक और संभावित सुविधाकर्ता के रूप में आर्टिफिशियल इंटेलिजेंस (AI) के दोहरे कार्य को रेखांकित करता है। मशीन लर्निंग एल्गोरिदम और न्यूरल नेटवर्क जैसी AI-संचालित तकनीकों का उपयोग करके, बैंक अपने खतरे का पता लगाने, रोकथाम और प्रतिक्रिया क्षमताओं में सुधार कर सकते हैं। AI-संचालित साइबर हमलों द्वारा प्रस्तुत नैतिक और कानूनी कठिनाइयाँ मजबूत शासन संरचनाओं और वित्तीय संस्थानों के बीच बेहतर समन्वय की आवश्यकता को उजागर करती हैं। इस अध्ययन के परिणाम एक व्यापक साइबर सुरक्षा योजना की आवश्यकता पर प्रकाश डालते हैं जिसमें भारतीय बैंकिंग उद्योग के डिजिटल भविष्य की सुरक्षा के लिए परिष्कृत एआई प्रौद्योगिकी, उपभोक्ता शिक्षा और अंतर्राष्ट्रीय सहयोग को शामिल किया गया है।

कोवाचेविक (2024) कृत्रिम बुद्धिमत्ता (AI) में तेजी से हुई प्रगति ने कई क्षेत्रों में, विशेष रूप से बैंकिंग में, दक्षता और आर्थिक प्रतिस्पर्धा में सुधार के लिए नई संभावनाएँ पैदा की हैं। कृत्रिम बुद्धिमत्ता की एक शाखा, मशीन लर्निंग (ML), कंप्यूटर को व्यापक डेटासेट से अनुकूलन और सीखने, निर्णय लेने, धोखाधड़ी का पता लगाने और ग्राहक सेवा स्वचालन को बदलने में सक्षम

बनाती है। फिर भी, ये प्रगति नई चिंताएँ भी प्रस्तुत करती हैं, विशेष रूप से साइबर सुरक्षा के क्षेत्र में। डेटा विषाक्तता और चोरी के हमलों सहित प्रतिकूल हमले, परिणामों को बदलने या महत्वपूर्ण जानकारी को खतरे में डालने के लिए खामियों का फायदा उठाकर मशीन लर्निंग मॉडल के लिए महत्वपूर्ण खतरे पैदा करते हैं। यह शोध AI तकनीकों की दोहरे उपयोग की विशेषताओं पर जोर देता है, जिसका उपयोग नापाक व्यक्तियों द्वारा किया जा सकता है। लेख इन कठिनाइयों से निपटने के लिए सुरक्षा, विश्वास, लकाईलापन और मजबूती जैसी आवश्यक विशेषताओं को शामिल करने वाले मशीन लर्निंग मॉडल बनाने की आवश्यकता को रेखांकित करता है। ये क्षमताएँ जोखिम शमन और बैंकिंग उद्योग में AI तकनीक के सुरक्षित उपयोग के लिए महत्वपूर्ण हैं, जहाँ वित्तीय डेटा की सुरक्षा अत्यंत महत्वपूर्ण है। परिणाम बेहतर साइबर सुरक्षा ढाँचों और रक्षात्मक रणनीतियों में चल रही प्रगति की महत्वपूर्ण आवश्यकता को उजागर करते हैं। इस अध्ययन का उद्देश्य बैंकिंग उद्योग में एआई के समुचित समावेश को सुगम बनाना है, इसके लिए इसकी संभावनाओं और खतरों दोनों की जांच की जाएगी, ताकि उभरते हुए सरोकारों को कम करते हुए नवाचार को बढ़ावा दिया जा सके।

सिंह (2024) सूचना सुरक्षा क्षेत्र में मैलवेयर, फ़िशिंग, कृत्रिम बुद्धिमत्ता, मशीन लर्निंग और क्रिप्टोकॉरेंसी सहित नए और विकासशील साइबर सुरक्षा खतरों का प्रसार देखा जा रहा है। उद्यमों में साइबर सुरक्षा पेशेवरों की कमी ने लोकतंत्र, पूंजीवाद और व्यक्तिगत गोपनीयता जैसे सिद्धांतों में जनता के भरोसे को लेकर आशंकाओं को बढ़ा दिया है। डेटा सुरक्षा के लिए महत्वपूर्ण और बढ़ते खतरों में वर्तमान में रैनसमवेयर जैसे मैलवेयर, फ़िशिंग सहित सोशल इंजीनियरिंग हमले, संवेदनशील जानकारी से समझौता करने वाले क्लाउड मिसकॉन्फ़िगरेशन, सॉफ़्टवेयर और हार्डवेयर आपूर्ति श्रृंखला के भीतर कमज़ोरियाँ, गोपनीय डेटा तक पहुँच रखने वाले दुर्भावनापूर्ण या लापरवाह अंदरूनी लोग और तेज़ी से विकसित हो रही तकनीकों में अपर्याप्त सुरक्षा शामिल हैं। इन कई खतरों का मुकाबला करने के लिए उपयोगकर्ता शिक्षा, पहुँच सीमाएँ, एन्क्रिप्शन, निगरानी और अपडेट और पैच किए गए सिस्टम के रखरखाव सहित एक व्यापक योजना आवश्यक है। संगठनों को सुरक्षा जोखिमों की सक्रिय रूप से पहचान करनी चाहिए और उनका प्रबंधन करना चाहिए क्योंकि हमलावर अपने डेटा और सिस्टम को उल्लंघनों से बचाने के लिए अधिक कुशल हो जाते हैं, जिसके परिणामस्वरूप वित्तीय नुकसान, प्रतिष्ठा को नुकसान और कानूनी परिणाम हो सकते हैं।

राधिका के.जी. (2024)समकालीन डिजिटल युग में, प्रौद्योगिकी उद्यमों और संगठनों को ग्राहकों को गुणवत्तापूर्ण सेवाएँ प्रदान करने के अपने उद्देश्य को पूरा करने में महत्वपूर्ण रूप से सहायता करती है। कृत्रिम बुद्धिमत्ता वैश्विक बाजारों में तेज़ी से बदलाव ला रही है। बैंकिंग उद्योग सहित कई क्षेत्रों में AI तकनीक की जाँच की गई है। हाल के वर्षों में, भारत में बैंकिंग में AI का उपयोग बढ़ा है। कृत्रिम बुद्धिमत्ता को मानव बुद्धि से जुड़ी संज्ञानात्मक गतिविधियों को निष्पादित करने की तकनीक की क्षमता के रूप में परिभाषित किया जाता है, जिसमें धारणा, तर्क, सीखना, पर्यावरणीय संपर्क, समस्या-समाधान और यहाँ तक कि रचनात्मकता भी शामिल है। व्यक्तिगत प्रबंधन सेवाओं, क्रेडिट सूचना सेवाओं, अक्सर पूछे जाने वाले प्रश्न (FAQ) सेवाओं और वित्तीय सहायता सेवाओं में उल्लेखनीय सफलता प्राप्त करते हुए, एल्गोरिदम का उपयोग करके बैंकिंग सिस्टम में कृत्रिम बुद्धिमत्ता का उपयोग किया जाता है। बैंकिंग मशीन के समग्र प्रदर्शन में सुधार अब कृत्रिम बुद्धिमत्ता के उपयोग के माध्यम से प्राप्त किया जाता है। बैंकिंग क्षेत्र कई बदलावों का अनुभव कर रहा है, जिसमें ग्राहक को मूल प्रेरणा के रूप में महत्व दिया गया है। तकनीक-प्रेमी ग्राहक जो अक्सर उन्नत तकनीक का उपयोग करते हैं, वे चाहते हैं कि बैंक निर्बाध अनुभव प्रदान करें। इन अपेक्षाओं को पूरा करने के लिए, बैंकों ने मोबाइल बैंकिंग, इलेक्ट्रॉनिक बैंकिंग और रियल-टाइम मनी ट्रांसफर जैसी सेवाओं को लागू करके खुदरा, सूचना प्रौद्योगिकी और दूरसंचार को शामिल करने के लिए अपने परिचालन दायरे को व्यापक बनाया है। अध्ययन का उद्देश्य आर्टिफिशियल इंटेलिजेंस की अवधारणा की जांच करना, भारतीय बैंकिंग उद्योग के भीतर इसकी संभावनाओं का पता लगाना और इस क्षेत्र में आर्टिफिशियल इंटेलिजेंस की प्रगति का आकलन करना है।

मूंदड़ा (2024)इस शोध का उद्देश्य वित्तीय संस्थानों पर साइबर अपराध के हानिकारक प्रभावों की जांच करना है, साथ ही एक मजबूत साइबर सुरक्षा ढांचे का विकास और इसके परिणामों को कम करने के प्रयास करना है। हाल ही में बैंक इसके प्राथमिक लक्ष्य रहे हैं। भारत में कई बैंक अक्सर बड़े पैमाने पर मेलवेयर हमलों के अधीन होते हैं, जो निजी और संवेदनशील जानकारी से समझौता करते हैं और काफी वित्तीय नुकसान का कारण बनते हैं। इस शोध का उद्देश्य यह पहचानना है कि कौन से उद्योग क्षेत्र साइबर हमलों के लिए अधिक संवेदनशील हैं और साइबर सुरक्षा नीतियों के विकास और अनुकूलन को सुनिश्चित करना है। रिपोर्ट में विभिन्न साइबर खतरों और अपराधों की केस स्टडी जांच शामिल है, जो पहले काफी वित्तीय नुकसान पहुंचा चुके हैं, जिसमें सरकारी वेबसाइटों, पत्रिकाओं और शोध पत्रों सहित विभिन्न इंटरनेट संसाधनों से प्राप्त

द्वितीयक डेटा विश्लेषण शामिल है। यह लेख साइबर शासनों के बारे में अंतर्दृष्टि प्रदान करेगा जो वित्तीय संस्थानों, बैंकों और बड़े पैमाने पर समाज को लाभान्वित करेगा।

कांत, डॉ. (2024). जैसे-जैसे हम एक नए युग की ओर बढ़ रहे हैं, पिछले दशक पर नज़र डालने से हमें सद्भाव और सहयोग द्वारा आकार दिए गए वैश्विक गतिशीलता के जटिल अंतर्संबंध को देखने में मदद मिलती है। दुनिया ने कई कठिनाइयों और सफलताओं का सामना किया है, इस क्रांतिकारी यात्रा में सबसे आगे G20 के साथ, हमारे साझा भविष्य को परिभाषित करने में एक महत्वपूर्ण भूमिका निभा रहा है। यह संपादित कार्य, "भविष्य को आकार देने का एक दशक: वैश्विक सद्भाव, सहयोग और G20," पिछले दशक के दौरान देशों, अर्थव्यवस्थाओं और संस्कृतियों के बीच महत्वपूर्ण अंतःक्रियाओं की गहन जाँच प्रदान करता है। यह पुस्तक पाठकों को वैश्विक सरकार, कूटनीति और हमारे जुड़े हुए विश्व पर G20 के महत्वपूर्ण प्रभाव के जटिल पहलुओं का पता लगाने के लिए आमंत्रित करती है। दुनिया की प्रमुख अर्थव्यवस्थाओं से मिलकर बना G20, अद्वितीय समस्याओं के बीच आशावाद और सहयोग के प्रतीक के रूप में उभरा। आर्थिक संकटों और सार्वजनिक स्वास्थ्य आपदाओं के दौरान संवाद को सुविधाजनक बनाने, समझौते स्थापित करने और अधिक निष्पक्ष और टिकाऊ भविष्य की दिशा में प्रयासों को निर्देशित करने में G20 महत्वपूर्ण रहा है। अध्यायों का यह संकलन, सावधानीपूर्वक संकलित और परिष्कृत, प्रमुख शोधकर्ताओं, राजनेताओं और बुद्धिजीवियों के दृष्टिकोणों को जोड़ता है, जिन्होंने वैश्विक शासन की पेकाईदगियों को स्पष्ट करने के लिए अपने ज्ञान को समर्पित किया है। प्रत्येक अध्याय जलवायु परिवर्तन, तकनीकी नवाचार, समावेशी आर्थिक विकास और सामाजिक न्याय सहित वैश्विक परिदृश्य को प्रभावित करने वाले प्रमुख मुद्दों पर एक अलग दृष्टिकोण प्रस्तुत करता है। कथा कालानुक्रमिक रूप से आगे बढ़ती है, जो G20 के विकास और वैश्विक घटनाओं की बदलती गतिशीलता के लिए इसके अनुकूलन की विस्तृत समझ प्रदान करती है। पीछे मुड़कर देखने पर, हम इस ऐतिहासिक दशक की विशेषता वाली सफलताओं और चुनौतियों की महत्वपूर्ण समझ प्राप्त करते हैं। हम, इस संस्करण के संपादक, अपनी विशेषज्ञता, अंतर्दृष्टि और दृष्टिकोण साझा करने के लिए प्रतिष्ठित लेखकों के प्रति अपनी प्रशंसा व्यक्त करते हैं। उनके सहयोगी प्रयासों ने एक ऐसा संग्रह तैयार किया है जो न केवल अतीत को समेटे हुए है बल्कि भविष्य के लिए एक मार्गदर्शक के रूप में भी कार्य करता है। हम चाहते हैं कि पाठक इन विविध दृष्टिकोणों से बातकाईत करें, चर्चाओं को प्रज्वलित करें जो सीमाओं को पार करती हैं और वैश्विक नागरिकता की भावना को बढ़ावा देती हैं। "भविष्य को आकार देने का एक दशक" घटनाओं के एक साधारण

रिकॉर्ड से परे है; यह पुस्तक सहयोग, समझ और बेहतर दुनिया के लिए अटूट खोज के माध्यम से पनपने वाली लकाईली मानवीय भावना का प्रतीक है। आशा है कि यह पुस्तक वैश्विक शांति, सहयोग और हमारे साझा भाग्य को आकार देने में हमारी सामूहिक जिम्मेदारी के सिद्धांतों के प्रति एक पुनर्जीवित समर्पण को जगाएगी।

सिंह (2024) भारत, एक तेजी से आगे बढ़ रहे देश के रूप में, सुरक्षा जोखिमों के एक जटिल स्पेक्ट्रम का सामना करता है जो इसकी स्थिरता और विकास को खतरे में डालता है। यह लेख भारत के सामने आने वाली कई सुरक्षा चिंताओं की जांच करता है, जिसमें पारंपरिक और अपरंपरागत दोनों घटक शामिल हैं। उनमें से प्रमुख हैं सीमा पार आतंकवाद, क्षेत्रीय विद्रोह और सामाजिक-राजनीतिक तनावों से बढ़े घरेलू संघर्षों की स्थायी चुनौतियाँ। इसके अलावा, साइबर जोखिम एक प्रमुख मुद्दा बन गया है, जिसकी विशेषता महत्वपूर्ण बुनियादी ढाँचे, वित्तीय प्रणालियों और व्यक्तिगत सूचनाओं को लक्षित करके साइबर हमलों में वृद्धि है। प्राकृतिक आपदाओं और संसाधनों की कमी सहित पर्यावरण और जलवायु संबंधी चुनौतियाँ राष्ट्रीय सुरक्षा के लिए काफी खतरे पेश करती हैं। लेख इन खतरों के प्रति भारत की रणनीतिक प्रतिक्रियाओं की एक व्यापक जाँच प्रस्तुत करता है, जिसमें सरकारी नीतियों, सैन्य योजनाओं और राष्ट्रीय सुरक्षा सुनिश्चित करने में खुफिया सेवाओं के कार्य पर जोर दिया गया है। यह अंतरराष्ट्रीय चुनौतियों से निपटने में अंतर्राष्ट्रीय सहयोग और गठबंधनों के महत्व का भी विश्लेषण करता है। यह पत्र आंतरिक सुरक्षा उपायों को मजबूत करने, साइबर लकाईलापन बढ़ाने और एक मजबूत सुरक्षा ढांचा स्थापित करने के लिए सामुदायिक भागीदारी को बढ़ावा देने की आवश्यकता पर जोर देता है। भारत विभिन्न सुरक्षा मुद्दों को दूर करके एक अधिक सुरक्षित, अधिक स्थिर वातावरण बनाना चाहता है, जिससे स्थायी आर्थिक और सामाजिक विकास को बढ़ावा मिले।

परिता कौशिक भाई घाघड़ा (2024) यह शोधपत्र भारतीय बैंकिंग प्रणाली पर फिनटेक के प्रभाव का बारीकी से विश्लेषण करता है। यह जांचता है कि फिनटेक किस तरह डिजिटल भुगतान, ऋण सुलभता और धन प्रबंधन में नवाचार को बढ़ावा देता है, जिससे पारंपरिक बैंकिंग प्रक्रियाओं में क्रांति आती है। अध्ययन में फिनटेक के लाभों पर जोर दिया गया है, जिसमें बेहतर वित्तीय समावेशन, बेहतर ग्राहक सेवा और बढ़ी हुई परिचालन दक्षता शामिल है। इसके अलावा, यह साइबर सुरक्षा खतरों, कानूनी पेकाईदगियों और स्थापित वित्तीय संस्थानों से प्रतिद्वंद्विता जैसी संभावित चुनौतियों से निपटता है। इसके अलावा, रिपोर्ट इस बात की जांच करती है कि भारतीय बैंक फिनटेक फर्मों के साथ सहयोग करने और अपने डिजिटल समाधानों को बढ़ाने जैसे तरीकों

को लागू करके कैसे बदलते माहौल के अनुकूल बन रहे हैं। यह फिनटेक युग में भारतीय बैंकिंग क्षेत्र की भविष्य की समृद्धि के लिए सहयोग और नवाचार के महत्व को रेखांकित करके समाप्त होता है।

ओनुमाडु (2024) वर्तमान में, कई उद्यम निकट-क्षेत्र संचार (NFC) भुगतान प्रणाली का उपयोग करते हैं, जिससे वे उपभोक्ता भुगतानों को तेज़ी से और निर्बाध रूप से संसाधित कर सकते हैं। यह तकनीक साइबर सुरक्षा कमजोरियों को प्रस्तुत करती है जिनका विश्लेषण और शमन करने की आवश्यकता है। यह शोधपत्र NFC लेनदेन से जुड़े साइबर खतरों की जांच करता है और भुगतान उपकरणों पर जोर देते हुए इन जोखिमों के प्रबंधन के तरीकों का विश्लेषण करता है। यह लेख NFC तकनीक, संबंधित सुरक्षा खामियों, गोपनीयता के मुद्दों और धोखाधड़ी गतिविधियों का अवलोकन प्रस्तुत करता है। इसके बाद यह स्मार्टफोन, संपर्क रहित कार्ड और पहनने योग्य उपकरणों जैसी भुगतान तकनीकों की जांच करता है, उनकी विशेषताओं और कमजोरियों पर जोर देता है। शोध आगे जोखिम कम करने के विकल्पों के रूप में एन्क्रिप्शन, प्रमाणीकरण, टोकनाइजेशन, बायोमेट्रिक सत्यापन और धोखाधड़ी का पता लगाने की तकनीकों की जांच करता है। अध्ययन NFC लेनदेन सुरक्षा को स्पष्ट करने के लिए सैद्धांतिक रूपरेखाओं को एकीकृत करता है और हितधारकों के लिए सुझाव प्रस्तुत करता है।

महतो (2024) डिजिटल प्रसारण वातावरण में साइबर सुरक्षा आवश्यक है, जहाँ अखंडता और गोपनीयता सर्वोपरि है। जैसे-जैसे साइबर अपराध की दरें बढ़ती हैं, वैसे-वैसे हमलावरों द्वारा कई उद्योगों में सिस्टम की कमजोरियों का फ़ायदा उठाने के लिए इस्तेमाल किए जाने वाले परिष्कृत तरीके भी बढ़ते हैं। इस लेख का उद्देश्य समाचार क्षेत्र के भीतर संवेदनशील जानकारी, मालिकाना डेटा और परिचालन ढाँचों से संबंधित कड़े साइबर सुरक्षा प्रोटोकॉल की महत्वपूर्ण आवश्यकता पर ज़ोर देना है। व्यवसाय डिजिटल प्लेटफ़ॉर्म की उपलब्धता और उपयोग से जुड़े खतरों के प्रति संवेदनशील हैं, जिसके परिणामस्वरूप संवेदनशील जानकारी तक अवैध पहुँच और नियमित संचालन में रुकावट जैसे गंभीर परिणाम हो सकते हैं। इस अध्ययन का उद्देश्य साइबर सुरक्षा में कई आधुनिक कठिनाइयों को रेखांकित करना और व्यापक और अनुकूलनीय सुरक्षा विधियों की आवश्यकता वाले आगामी खतरों को उजागर करना है। निष्कर्ष तेज़ी से हो रही तकनीकी प्रगति के बीच डिजिटल समाचार क्षेत्र में विश्वास, डेटा सुरक्षा और चल रही व्यवहार्यता के लिए साइबर सुरक्षा के महत्व को रेखांकित करते हैं।

गोनी (2024) यह अकादमिक बहस आधुनिक साइबर खतरों के जटिल वातावरण के बीच वर्तमान साइबर सुरक्षा में भेद्यता विश्लेषण की महत्वपूर्ण आवश्यकता पर प्रकाश डालती है, जिसमें उन्नत मैलवेयर और लक्षित फ़िशिंग विधियाँ शामिल हैं। यह पूरी तरह से व्यवस्थित प्रक्रिया को रेखांकित करता है - जिसमें पहचान, स्कैनिंग, पैठ परीक्षण, जोखिम मूल्यांकन, प्राथमिकता, उपचार और निरंतर निगरानी शामिल है - जो सक्रिय साइबर सुरक्षा रणनीतियों की नींव है। बहस भेद्यता आकलन और घटना प्रतिक्रिया के बीच अन्योन्याश्रित संबंध पर जोर देती है, संभावित नुकसान को कम करने और हमलों को रोकने में उनकी संयुक्त प्रभावकारिता पर प्रकाश डालती है। इसके अलावा, यह साइबर खतरों की विकसित प्रकृति पर प्रकाश डालता है, विरोधियों से आगे निकलने के लिए निरंतर भेद्यता आकलन की आवश्यकता पर बल देता है। यह प्रवचन जागरूकता, शिक्षा और सहयोग के बड़े क्षेत्रों की जांच करने के लिए तकनीकी पहलुओं से आगे बढ़ता है, साइबर सुरक्षा बचाव को मजबूत करने में उनके महत्वपूर्ण महत्व पर प्रकाश डालता है। यह अंततः भेद्यता विश्लेषण के संपूर्ण कार्यान्वयन को बढ़ावा देता है, इसे साइबर सुरक्षा की नींव के रूप में स्थापित करता है और हितधारकों को सतर्कता और उन्नत सुरक्षात्मक उपायों के साथ जटिल डिजिटल वातावरण को पार करने में सक्षम बनाता है।

अलसैफ़ (2024) यह रिपोर्ट साइबर सुरक्षा अनुसंधान पहलों की एक विस्तृत श्रृंखला की जांच करती है, जिसमें इंटरनेट ऑफ थिंग्स (IoT) और कनेक्टेड वाहन सुरक्षा जैसे उभरते डोमेन शामिल हैं, साथ ही मैलवेयर और डिस्ट्रिब्यूटेड डेनियल ऑफ सर्विस (DDoS) हमलों जैसी अधिक पारंपरिक चिंताएँ भी शामिल हैं। शोधकर्ता डीप लर्निंग और मशीन लर्निंग सहित कई तरीकों का उपयोग करते हैं, जबकि स्पष्ट डेटासेट विवरणों और झूठे सकारात्मक और नकारात्मक के निहितार्थों पर सावधानीपूर्वक विचार करते हैं। सटीकता और प्रासंगिक संज्ञान विशेष रूप से इंटरनेट ऑफ थिंग्स की सुरक्षा के लिए आवश्यक हैं। तेजी से खतरे का पता लगाना स्वचालन और प्रभावकारिता पर निर्भर करता है, जिसमें जेनेटिक एल्गोरिदम, वुल्फ ऑप्टिमाइज़ेशन और नए मॉडल जैसी नवीन तकनीकों के एकीकरण द्वारा दिखाई गई प्रगति के प्रति समर्पण शामिल है। सुविधा चयन, सटीकता और निष्पादन अवधि के बीच संतुलन हासिल करना एक बड़ी कठिनाई है। समान बेंचमार्क डेटासेट की उपलब्धता से तुलनीय आकलन की सुविधा मिलती है। अंतिम उद्देश्य सुरक्षा उपायों को मजबूत करना और डिजिटल विश्वास को बढ़ाना है। यह अवलोकन साइबर सुरक्षा के लगातार विकसित होते परिदृश्य की जांच करने के लिए जानकारी और संसाधन प्रदान करता है।

वासिहुन सेमा एडमस (2024) साइबर सुरक्षा एक सर्वोपरि समस्या के रूप में उभरी है, जिसके कारण शोधकर्ताओं, शिक्षाविदों और कंपनियों को सूचना प्रणालियों की गोपनीयता और सुरक्षा की रक्षा करने पर ध्यान केंद्रित करना आवश्यक हो गया है। डिजिटलीकरण की बढ़ती इच्छा के परिणामस्वरूप, व्यक्ति और संगठन दोनों ही हमेशा विकसित होते साइबर जोखिमों का सामना करते हैं। यह लेख साइबर सुरक्षा में वर्तमान प्रगति, समस्याओं, रणनीतियों, परिस्थितियों और दुनिया भर के रुझानों की व्यापक जांच प्रस्तुत करता है। साइबर सुरक्षा में प्रतिस्पर्धात्मक बढ़त बनाए रखने के लिए, हमने क्षेत्र में नवीनतम रुझानों, समस्याओं और उन्नति की पहचान करने के लिए एक गहन अध्ययन किया। इसके अलावा, हम साइबर सुरक्षा के भविष्य के प्रक्षेपवक्र की जांच करते हैं, बढ़ते साइबर सुरक्षा खतरे के परिदृश्य से निपटने के लिए संभावित रणनीतियों और तरीकों की रूपरेखा तैयार करते हैं, साथ ही साइबर खतरे की प्रतिक्रियाओं का पता लगाने और स्वचालन के लिए आर्टिफिशियल इंटेलिजेंस (AI) और मशीन लर्निंग (ML) जैसे उभरते रुझान और नवाचारों की भी जांच करते हैं। यह निबंध साइबर पारिस्थितिकी तंत्र के भीतर हितधारकों के बीच निरंतर अपनाने और सहयोग के महत्व पर जोर देता है।

रेहान, अबू. (2024). अधिक जुड़े हुए डिजिटल परिदृश्य में, साइबर सुरक्षा लोगों, निगमों और सरकारों को कई साइबर हमलों से बचाने के लिए आवश्यक हो गई है। यह अध्ययन पत्र डिजिटल युग में साइबर सुरक्षा का व्यापक विश्लेषण प्रस्तुत करता है, जो जोखिमों का मूल्यांकन करने और बचाव को बढ़ाने पर ध्यान केंद्रित करता है। दस्तावेज़ साइबर सुरक्षा को परिभाषित करने और इसकी ऐतिहासिक प्रगति की जांच करने से शुरू होता है, समकालीन संदर्भ में इसके महत्व पर जोर देता है। यह बाद में मैलवेयर हमलों, फ़िशिंग, सेवा से इनकार (DoS) हमलों, अंदरूनी खतरों और उन्नत लगातार खतरों (APTs) सहित साइबर खतरों की कई श्रेणियों को वर्गीकृत और जांचता है। साइबर खतरों का मूल्यांकन भेद्यता मूल्यांकन, पैठ परीक्षण और खतरे की खुफिया जानकारी जैसे तरीकों से किया जाता है। अध्ययन साइबर सुरक्षा को बढ़ाने के तरीकों की जांच करता है, जिसमें रक्षा-गहन पद्धतियाँ, एन्क्रिप्शन, नेटवर्क सुरक्षा और घटना प्रतिक्रिया प्रक्रियाएं शामिल हैं। विनियामक अनुपालन और गोपनीयता कानून सहित कानूनी और नैतिक पहलुओं की पूरी तरह से जांच की जाती है। साइबर सुरक्षा में मानवीय तत्व का विश्लेषण किया जाता है, जिसमें कर्मियों के प्रशिक्षण, जागरूकता पहल और उपयोगकर्ता व्यवहार की समझ की आवश्यकता पर प्रकाश डाला जाता है। लेख में महत्वपूर्ण बुनियादी ढांचे में साइबर सुरक्षा और अंतरराष्ट्रीय सहयोग और साइबर कूटनीति की आवश्यकता पर भी चर्चा की गई है। लेख में कृत्रिम बुद्धिमत्ता,

ब्लॉकचेन और क्वांटम क्रिप्टोग्राफी सहित आगामी प्रौद्योगिकियों और साइबर सुरक्षा पर उनके संभावित प्रभाव की जांच की गई है।

अहमद (2024) कंपनी परिवर्तन में बढ़े हुए डिजिटलीकरण ने पर्याप्त लाभ दिए हैं, साथ ही सूचना सुरक्षा के लिए नई समस्याएं भी पेश की हैं। यह अध्ययन डिजिटल परिवर्तन अवधि के दौरान सामने आई साइबर सुरक्षा चिंताओं की जांच करना चाहता है, जो सूचना प्रणालियों पर केंद्रित है। उपयोग की गई शोध तकनीक इन कठिनाइयों की गहन समझ प्राप्त करने के लिए साहित्य और केस स्टडीज की गहन समीक्षा है। यह अध्ययन डिजिटल परिवर्तन के कार्यान्वयन में साइबर सुरक्षा से जुड़े कई महत्वपूर्ण मुद्दों की पहचान करता है, जिसमें मैलवेयर हमले, फ़िशिंग, अपर्याप्त नेटवर्क सुरक्षा और गोपनीयता उल्लंघन शामिल हैं। कारण विश्लेषण से पता चला कि अपर्याप्त प्रशिक्षण और सुरक्षा जागरूकता, सूचना प्रणालियों में खराब डिज़ाइन के साथ, प्राथमिक जोखिम कारक थे। यह अध्ययन व्यापक कार्मिक प्रशिक्षण, सतर्क सुरक्षा निरीक्षण और सुरक्षा खतरों के बारे में समय पर अलर्ट सहित सूचना प्रणालियों के अंदर मजबूत सुरक्षा प्रोटोकॉल स्थापित करने में सक्रिय उपायों की आवश्यकता को रेखांकित करता है। बढ़ते वैश्विक खतरों को संबोधित करने में संगठनों, सरकारों और संबंधित संस्थाओं के बीच सहयोग के महत्व पर जोर दिया गया।

डॉ. सविता एस. पाटिल (2025) बैंकिंग में साइबर सुरक्षा में कंप्यूटर परिसंपत्तियों, सूचना और नेटवर्क को अवांछित पहुँच से बचाने के साथ-साथ व्यवसाय निरंतरता और आपदा रिकवरी तैयारी सुनिश्चित करने की रणनीतियाँ शामिल हैं। इसमें सूचना सुरक्षा, अनुप्रयोग सुरक्षा, नेटवर्क सुरक्षा और आपदा रिकवरी शामिल हैं। बैंकों पर साइबर हमले के परिणामस्वरूप गंभीर परिणाम हो सकते हैं, जिसमें वित्तीय नुकसान, महत्वपूर्ण डेटा उल्लंघन, परिचालन व्यवधान, ब्रांड प्रतिष्ठा को नुकसान, कानूनी विवाद और नियामक जुर्माना शामिल हैं। भारतीय बैंकिंग उद्योग में नियामक अनुपालन वित्तीय स्थिरता को बढ़ाने, ग्राहकों की सुरक्षा करने और बैंकिंग प्रणाली की अखंडता और दक्षता को बनाए रखने का प्रयास करता है। भारतीय बैंकिंग उद्योग में, साइबर सुरक्षा बोर्ड और कार्यकारी पर्यवेक्षण साइबर जोखिमों को सीमित करने, संवेदनशील डेटा की सुरक्षा करने और वित्तीय प्रणालियों की लकाईलापन बनाए रखने के लिए शासन के आवश्यक तत्व हैं। साइबर जोखिम प्रबंधन के लिए एक संपूर्ण और सक्रिय रणनीति की आवश्यकता होती है, जिसमें कई संगठनात्मक इकाइयों में समन्वय और साइबर सुरक्षा में विकसित साइबर जोखिमों और सर्वोत्तम प्रथाओं के बारे में जानकारी प्राप्त करने के लिए समर्पण शामिल है। यह पेपर साइबर अपराधों के कई चरणों, श्रेणियों, प्रवृत्तियों और समस्याओं की जांच करता है, साथ ही भारत सरकार को

साइबर अपराधों को कम करने और भारतीय बैंकिंग उद्योग के अंदर वित्तीय सुरक्षा की रक्षा करने के लिए क्या उपाय करने चाहिए।

श्रीमती शशिकला केजी, श्री रमेश एपी (2025) साइबर सुरक्षा समकालीन अस्तित्व के लिए उतनी ही महत्वपूर्ण हो गई है जितनी कि वह तकनीक जिसकी वह सुरक्षा करना चाहती है। दोनों मूल रूप से एक दूसरे से जुड़े हुए हैं - हमारी आर्थिक स्थिरता, राष्ट्रीय सुरक्षा और सामाजिक संरचना अब डिजिटल तकनीकों पर काफी हद तक निर्भर करती है। नतीजतन, राष्ट्रीय हितों की सुरक्षा, आर्थिक सफलता सुनिश्चित करने और जनता के विश्वास को बनाए रखने के लिए साइबर सुरक्षा आवश्यक है। उपसर्ग "साइबर" कंप्यूटर और सूचना युग से संबंधित किसी व्यक्ति, विचार या इकाई को दर्शाता है। कुबेरनेट्स नाम, "स्टीयरमैन" या "गवर्नर" के लिए ग्रीक शब्द से उत्पन्न हुआ, नॉर्बर्ट वीनर की "साइबरनेटिक्स" की अवधारणा के माध्यम से प्रमुखता प्राप्त हुई। जिस डिजिटल वातावरण से हम हर दिन गुजरते हैं, उसे साइबरस्पेस कहा जाता है, जिसे साइबर कानूनों के रूप में जाने जाने वाले कानूनों के ढांचे द्वारा विनियमित किया जाता है। ये नियम सभी इंटरनेट उपयोगकर्ताओं पर लागू होते हैं, जिन्हें कभी-कभी "नेटिज़न्स" कहा जाता है, और राष्ट्रीय सीमाओं को पार करते हैं, इसलिए सार्वभौमिक अधिकार क्षेत्र की एक प्रणाली बनाते हैं। साइबर अपराध में ऐसे आपराधिक व्यवहार शामिल हैं जिनमें कंप्यूटर या तो प्राथमिक लक्ष्य होता है (जैसा कि हैकिंग, फ़िशिंग या स्पैमिंग में देखा जाता है) या अन्य अपराधों (जैसे बाल पोर्नोग्राफी या घृणा अपराध) को अंजाम देने के लिए एक साधन के रूप में उपयोग किया जाता है। ऐसे अपराधों में व्यक्तिगत जानकारी का अवैध अधिग्रहण, मालिकाना खुफिया जानकारी की चोरी या प्रौद्योगिकी का अन्य शोषणकारी या दुर्भावनापूर्ण उपयोग शामिल हो सकता है। इस अध्ययन पत्र का उद्देश्य डिजिटल युग में भारतीय बैंकों द्वारा सामना की जाने वाली साइबर सुरक्षा कठिनाइयों का विश्लेषण करना है। शोध का उद्देश्य साइबर अपराधों और उनके परिणामों के बारे में जनता के ज्ञान का आकलन करना है, जो बढ़ी हुई डिजिटल साक्षरता और संस्थागत सुरक्षा की तत्काल आवश्यकता पर जोर देता है।

ख्यात (2025) स्वतंत्रता के बाद से भारत में बैंकिंग क्षेत्र का काफी विस्तार हुआ है, जिसकी संपत्ति \$2.67 ट्रिलियन से अधिक है। देश में दुनिया की सबसे बड़ी खुदरा बैंकिंग और वित्तीय सेवा संस्थाओं में से एक है। फिर भी, उद्योग साइबर सुरक्षा कमजोरियों, वित्तीय धोखाधड़ी, गैर-निष्पादित परिसंपत्तियों और अन्य जैसे खतरों का सामना करता है। सरकार ने बैंकों का राष्ट्रीयकरण किया है और निजी निवेश को प्रोत्साहित किया है, जिससे भारत दुनिया भर में पाँचवीं

सबसे बड़ी अर्थव्यवस्था बन गया है। यह रिपोर्ट सरकार द्वारा डिजिटलीकरण पर जोर दिए जाने के कारण भारतीय बैंकिंग उद्योग के सामने आने वाली समस्याओं की पहचान करती है। यह अध्ययन दर्शाता है कि बैंकिंग और वित्तीय उद्योग में समस्याएँ तीव्र हुई हैं, जबकि RBI और सरकार एक साथ जागरूकता बढ़ा रहे हैं। दुनिया ऐसे खतरों की बढ़ती श्रृंखला का सामना कर रही है जो बढ़ते वैश्वीकरण, तकनीकी प्रगति और जटिल अंतर-निर्भरता वाले युग में सुरक्षा की पारंपरिक धारणाओं से परे हैं। ये अपरंपरागत खतरे भौगोलिक सीमाओं को पार करते हैं और पूरे क्षेत्रों, राष्ट्रों और वैश्विक समुदाय की स्थिरता और कल्याण को खतरे में डालते हैं। यह प्रवचन अपरंपरागत खतरों, उनके द्वारा पेश की जाने वाली जटिलताओं और समाधान खोजने में सहयोग की आवश्यकता की जाँच करता है। गैर-पारंपरिक खतरों में कई तरह की चिंताएँ शामिल हैं जो हाल के वर्षों में और भी महत्वपूर्ण हो गई हैं। पारिस्थितिकी तंत्र, अर्थव्यवस्था और जोखिम में पड़े लोगों पर इसके व्यापक प्रभावों के कारण जलवायु परिवर्तन एक गंभीर मुद्दा है। गंभीर मौसम की घटनाओं की बढ़ती घटनाएँ, समुद्र का बढ़ता स्तर और भोजन और पानी की आपूर्ति में गड़बड़ी इन परिवर्तनों को कम करने और उनके अनुकूल होने के लिए वैश्विक पहल की आवश्यकता को उजागर करती है। COVID-19 महामारी स्वास्थ्य सेवा के बुनियादी ढाँचे की कमज़ोरी और सार्वजनिक स्वास्थ्य की वैश्विक अंतर्संबंधता को उजागर करती है। ये घटनाएँ तैयारी, अंतर्राष्ट्रीय सहयोग और स्वास्थ्य सेवा संसाधनों तक समान पहुँच की आवश्यकता को रेखांकित करती हैं। वैश्विक वित्तीय क्षेत्र संगठनों, बाज़ारों और साधनों का एक जटिल और परस्पर जुड़ा हुआ नेटवर्क है जो विश्व अर्थव्यवस्था का समर्थन करता है। यह जटिल प्रणाली कई जोखिमों और चुनौतियों के प्रति संवेदनशील है जो विश्वास को अस्थिर और नष्ट कर सकती हैं। सितंबर 2021 में मेरे अंतिम अपडेट के अनुसार, यह परिचय वैश्विक वित्तीय उद्योग के सामने आने वाले मुख्य खतरों का अवलोकन प्रदान करता है। वैश्विक वित्तीय पारिस्थितिकी तंत्र को साइबर सुरक्षा खतरों, परिचालन कमजोरियों, बाज़ार में उतार-चढ़ाव, भू-राजनीतिक अस्थिरता और ऋण स्तरों और विनियामक पालन से संबंधित मुद्दों सहित कई तरह की बाधाओं का सामना करना पड़ता है। ये जोखिम, विभिन्न स्तरों पर, वित्तीय संकटों को भड़काने, बाज़ारों को बाधित करने और वैश्विक आर्थिक विकास को प्रभावित करने की क्षमता रखते हैं। इस बदलते परिदृश्य में, वित्तीय संस्थानों, नियामकों और बाज़ार के खिलाड़ियों को सतर्क और लकाईला होना चाहिए। प्रभावी जोखिम प्रबंधन, नियामक निगरानी, प्रौद्योगिकी नवाचार और अंतर्राष्ट्रीय सहयोग इन खतरों का सामना करने और उन्हें कम करने में आवश्यक तत्व हैं। यह निबंध इन समस्याओं का अन्वेषण करेगा,

तथा उनकी प्रकृति, परिणामों तथा इस जटिल क्षेत्र से निपटने के लिए अपनाई गई रणनीतियों के बारे में अंतर्दृष्टि प्रदान करेगा।

इब्राहिम (2025) वित्तीय उद्योग ने साइबर सुरक्षा जोखिमों में अभूतपूर्व वृद्धि देखी है, जो अधिक परिष्कृत और लक्षित हमलों की व्यापक वैश्विक प्रवृत्ति को दर्शाता है। वित्तीय सेवाओं में चल रहे डिजिटल संक्रमण ने साइबर घटनाओं के प्रति क्षेत्र की संवेदनशीलता को बढ़ा दिया है, जिससे हितधारकों के बीच महत्वपूर्ण चिंताएँ पैदा हुई हैं। यह लेख वित्तीय क्षेत्र में बदलते साइबर सुरक्षा जोखिमों का विस्तृत विश्लेषण प्रदान करता है, जिसमें फ़िशिंग, रैनसमवेयर, अंदरूनी खतरे और उन्नत लगातार खतरे (APT) शामिल हैं। यह आधुनिक शमन समाधानों की भी जाँच करता है, जिसमें नियामक अनुपालन, ज़ीरो ट्रस्ट आर्किटेक्चर, AI-संचालित खतरे का पता लगाना और घटना प्रतिक्रिया ढाँचे पर प्रकाश डाला गया है। शोध उद्योग के सर्वोत्तम अभ्यासों को स्पष्ट करने और मजबूत साइबर सुरक्षा प्राप्त करने में चल रही समस्याओं को इंगित करने के लिए पाठ विश्लेषण और केस स्टडी सहित मिश्रित-विधियों के दृष्टिकोण का उपयोग करता है। परिणाम वित्तीय संस्थानों में एक सक्रिय, बहुआयामी और अनुकूलनीय साइबर सुरक्षा रणनीति की आवश्यकता पर जोर देते हैं। प्रौद्योगिकी नवाचार को रणनीतिक शासन के साथ एकीकृत करके, उद्योग अपने बुनियादी ढाँचे को मजबूत कर सकता है और बढ़ते डिजिटल जोखिमों के बीच हितधारकों का विश्वास बनाए रख सकता है।

मधुमिता (2025) इंटेलिजेंट बैंकिंग सिस्कोरिटी सिस्टम परियोजना का उद्देश्य एक परिष्कृत सुरक्षा ढाँचा विकसित करना है जो अत्याधुनिक तकनीक के उपयोग के माध्यम से क्लाउड की जानकारी और बैंकिंग लेनदेन की सुरक्षा करता है। पारंपरिक सुरक्षा समाधान अपर्याप्त हैं क्योंकि साइबर खतरे परिष्कृत होते जा रहे हैं। सिस्टम में एक गतिशील और कुशल सुरक्षा समाधान प्रदान करने के लिए एंड-टू-एंड एन्क्रिप्शन, बायोमेट्रिक पहचान, मशीन लर्निंग और आर्टिफिशियल इंटेलिजेंस (AI) शामिल हैं। AI-संचालित धोखाधड़ी का पता लगाने वाला सिस्टम असामान्य व्यवहार का पता लगाने और वास्तविक समय में आसन्न धोखाधड़ी को रोकने के लिए लगातार लेनदेन पैटर्न की जांच करता है। हालाँकि MFA बढ़ी हुई सुरक्षा प्रदान करता है, फिंगरप्रिंट स्कैनिंग और चेहरे की पहचान का उपयोग करके बायोमेट्रिक प्रमाणीकरण प्रभावी रूप से उपयोगकर्ता को प्रमाणित करता है। ब्लॉकचेन तकनीक सुरक्षित, पारदर्शी और अपरिवर्तनीय लेनदेन लॉगिंग प्रदान करती है। ब्लॉकचेन तकनीक का उपयोग यह सुनिश्चित करने के लिए किया जाता है कि लेनदेन लॉग सुरक्षित, पारदर्शी और अपरिवर्तनीय हैं। सिस्टम सुरक्षा

उल्लंघनों के त्वरित समाधान की सुविधा के लिए वास्तविक समय की खतरे की निगरानी, विसंगति की पहचान और स्वचालित घटना प्रतिक्रिया प्रदान करेगा। इस परियोजना का उद्देश्य सुरक्षा को बढ़ाना, उपभोक्ता विश्वास को बढ़ावा देना, नियामक अनुपालन सुनिश्चित करना और एक सुरक्षित और कुशल बैंकिंग अनुभव प्रदान करना है।

हैरिस (2025) वित्तीय सेवाओं के तेजी से डिजिटलीकरण ने दक्षता, पहुंच और ग्राहक सुविधा को बढ़ाया है। इस बदलाव ने फ़िशिंग प्रयासों, रैनसमवेयर, पहचान की चोरी और डेटा उल्लंघनों जैसी महत्वपूर्ण साइबर सुरक्षा चिंताओं को भी जन्म दिया है। साइबर अपराधी लगातार डिजिटल बैंकिंग सिस्टम की कमज़ोरियों का फ़ायदा उठाते हैं, जिसका लक्ष्य वित्तीय संस्थान और ग्राहक दोनों हैं। विनियामक प्राधिकरण और वित्तीय संस्थान बहु-कारक प्रमाणीकरण (MFA), कृत्रिम बुद्धिमत्ता (AI)-वर्धित धोखाधड़ी का पता लगाने और ब्लॉकचेन-आधारित सुरक्षा उपायों सहित परिष्कृत सुरक्षा ढाँचे अपना रहे हैं। यह लेख डिजिटल बैंकिंग में प्रमुख साइबर सुरक्षा खतरों, वित्तीय संस्थानों और ग्राहकों पर उनके प्रभावों और सुरक्षित बैंकिंग लेनदेन की गारंटी देने के लिए सबसे हाल के शमन उपायों की जाँच करता है।

सेले, एनएन और केंडा, एस. (2025), इस शोध का उद्देश्य डिजिटल बैंकिंग को अपनाने में बाधा डालने वाले साइबर सुरक्षा खतरों की पहचान करना और बैंकिंग क्षेत्र के भीतर साइबर सुरक्षा जोखिमों को कम करने के लिए स्थायी तरीके प्रदान करना है। डिजिटल बैंकिंग को अपनाने पर साइबर सुरक्षा खतरों और जोखिमों के प्रभाव के बारे में अनुभवजन्य जानकारी को मात्रात्मक रूप से संश्लेषित करने के लिए एक व्यवस्थित साहित्य समीक्षा का उपयोग किया गया था। कुल 84 पत्रों का मूल रूप से मूल्यांकन किया गया था, और इस व्यवस्थित समीक्षा के लिए चयन और समावेशन मानदंडों के आवेदन के बाद, 58 अध्ययनों को शामिल किया गया था। चुने गए प्रकाशनों ने लगातार पहचान की चोरी, मैलवेयर हमलों, फ़िशिंग और विशिंग को डिजिटल बैंकिंग को अपनाने में बाधा डालने वाले महत्वपूर्ण साइबर सुरक्षा मुद्दों के रूप में उजागर किया। यह शोध देश के नवजात बैंकिंग क्षेत्र में साइबर सुरक्षा पर थोड़े से साहित्य को बढ़ाता है, जिसकी उद्योग द्वारा अब तक अनुभव किए गए कई उल्लंघनों के कारण तत्काल आवश्यकता है।

पेत्रोव (2025) यह शोध ग्रे कास्ट आयरन EN-GJL-250 के साथ सैंड-कास्टिंग मोल्ड के गुरुत्वाकर्षण भरने के लिए एक सिमुलेशन मॉडल प्रस्तुत करता है। द्रव प्रवाह, मोल्ड भरने की विशेषताओं और दोष निर्माण की संभावना, जिसमें क्रिस्टलीकरण के दौरान धातु के सिकुड़ने से

उत्पन्न होने वाली रिक्तियाँ और छिद्र शामिल हैं, पर एक परीक्षण किया गया। सिमुलेशन में धातु कास्टिंग संचालन के मॉडलिंग के लिए डिज़ाइन किए गए विशेषज्ञ सॉफ़्टवेयर का उपयोग किया गया। कार्यक्रम कास्टिंग मोल्ड के भरने के दौरान द्रव गतिशीलता और तापमान की स्थिति के सिमुलेशन की सुविधा देता है। निष्कर्ष द्रव प्रवाह गतिशीलता और धातु क्रिस्टलीकरण पर स्प्रू सिस्टम डिज़ाइन, डालने का तापमान और कास्टिंग ज्यामिति के प्रभाव को इंगित करते हैं। सिमुलेशन अशांति और तापमान ढाल के अवलोकन की सुविधा देता है, जिससे दोष-प्रवण स्थानों की पहचान करने में सहायता मिलती है। इस शोध के निष्कर्ष कुछ कास्टिंग की गुणवत्ता को बढ़ा सकते हैं और सीमित संख्या में उच्च गुणवत्ता वाली कास्टिंग के उत्पादन के लिए उपयुक्त तकनीक के चयन में सहायता कर सकते हैं।

सिंह (2025) हाल के वर्षों में इंटरनेट ऑफ थिंग्स (IoT) में महत्वपूर्ण सुधार हुए हैं, जिसके परिणामस्वरूप डिजिटल दुनिया में एक आदर्श परिवर्तन हुआ है। फिर भी, इन तकनीकी प्रगति ने नई चिंताएँ प्रस्तुत की हैं, खासकर साइबर सुरक्षा में। IoT डिवाइस, जो आंतरिक रूप से इंटरनेट से जुड़े होते हैं, कई प्रकार के हमलों के प्रति संवेदनशील होते हैं। इसके अलावा, IoT सेवाएँ अक्सर संवेदनशील उपयोगकर्ता जानकारी का प्रबंधन करती हैं जिसका दुरुपयोग दुष्ट व्यक्तियों या अवैध सेवा प्रदाताओं द्वारा किया जा सकता है। IoT पारिस्थितिकी तंत्रों का विस्तार और पारंपरिक और क्लाउड-आधारित प्रणालियों का विलय मानकीकृत मानकों की कमी के कारण अलग-अलग सुरक्षा कमज़ोरियाँ पैदा करता है। प्लेटफ़ॉर्म-एज़-ए-सर्विस (PaaS) और इंफ्रास्ट्रक्चर-एज़-ए-सर्विस (IaaS) मॉडल द्वारा सुगम क्लाउड-आधारित IoT सिस्टम लकाईलापन और मापनीयता प्रदान करते हैं जबकि साथ ही साथ बढ़ी हुई सुरक्षा कमज़ोरियों को भी पेश करते हैं। इन प्रणालियों और पारंपरिक IoT उपकरणों के बीच जटिल परस्पर क्रिया डेटा अखंडता और उपयोगकर्ता गोपनीयता की सुरक्षा के लिए मजबूत समाधानों की आवश्यकता होती है। यह लेख IoT उपकरणों और सेवाओं के व्यापक कार्यान्वयन से संबंधित तत्काल सुरक्षा मुद्दों पर जोर देता है। हम भविष्य की कठिनाइयों की भविष्यवाणी और योजना बनाते हुए वर्तमान सुरक्षा कमियों को दूर करने के लिए प्रभावी तरीके सुझाते हैं। यह लेख वर्तमान में IoT सेवाओं के सामने आने वाली प्रमुख सुरक्षा चिंताओं का व्यापक विश्लेषण प्रस्तुत करता है। हम इन खतरों को कम करने के लिए सक्रिय उपायों का प्रस्ताव करते हैं, जिससे IoT उपकरणों और सेवाओं की समग्र सुरक्षा बढ़ जाती है।

गोराई (2025) यह शोधपत्र साइबर सुरक्षा के महत्वपूर्ण कार्य की जांच करता है। वर्तमान आधुनिकीकरण गोपनीयता और सूचना के संरक्षण को एक कठिन चुनौती बना चुका है। 'साइबर सुरक्षा' शब्द एक अनुकूल अवधारणा के रूप में उभरा है; हालाँकि, इसकी सटीक परिभाषा अभी भी मायावी है; इसे अक्सर गुमनामी, सूचना विनिमय, ज्ञान प्राप्ति और निगरानी की धारणाओं के साथ जोड़ दिया गया है। समकालीन सूचना परिदृश्य के विकासशील बुनियादी ढांचे की सुरक्षा के लिए डेटा सुरक्षा ढांचे की तत्काल आवश्यकता है। आईसीटी बुनियादी ढांचा सभी आवश्यक राष्ट्रीय बुनियादी ढांचे के मूल तत्व के रूप में कार्य करता है। दुनिया भर में चल रही ई-गवर्नेंस और ई-कॉमर्स पहल एक भरोसेमंद साइबर सुरक्षा बुनियादी ढांचे के प्रतिमान का उपयोग करती हैं। इस निबंध का उद्देश्य इस विकास और भारत के संबंध में इस अध्ययन से उत्पन्न होने वाले संभावित पैटर्न और अनिवार्यताओं का अवलोकन प्रदान करना है।

अध्याय 3 अनुसंधान क्रियाविधि

इस अध्याय में शोध की रूपरेखा, डेटा संग्रहण की विधियाँ, नमूना चयन, उपकरण तथा सांख्यिकीय तकनीकों का वर्णन किया गया है। इसमें अनुसंधान डिजाइन, सैंपल साइज, सैंपलिंग तकनीक और डेटा विश्लेषण के लिए प्रयुक्त सांख्यिकीय विधियों (जैसे Chi-square, आदि) को स्पष्ट किया गया है। यह अध्याय यह सुनिश्चित करता है कि शोध वैज्ञानिक एवं व्यवस्थित तरीके से किया गया है।

3.1 अनुसंधान डिजाइन

शोध डिजाइन एक व्यापक योजना है जो शोध परियोजना के उद्देश्यों को परिभाषित करती है और उन उद्देश्यों को पूरा करने के लिए जो भी इच्छाएं पूरी की जानी हैं, उनके लिए दिशानिर्देश प्रदान करती है। दूसरे शब्दों में, यह शोध परियोजना को पूरा करने के लिए एक सामान्य योजना है। डिजाइन शोधकर्ताओं को विषय के लिए उपयुक्त शोध विधियों को परिष्कृत करने और उपलब्धि के लिए अपने स्वयं के अध्ययन स्थापित करने की अनुमति देता है।

3.2 डेटा संग्रह प्रक्रियाएं

डेटा संग्रह एक समेकित प्रणाली के माध्यम से स्पष्ट चर पर डेटा एकत्र करने और मात्रा निर्धारित करने की प्रक्रिया है, ताकि प्रासंगिक प्रश्नों के उत्तर देकर परिणामों का मूल्यांकन किया जा सके। डेटा को दो तरीकों से एकत्र किया जा सकता है, अर्थात् द्वितीयक डेटा संग्रह विधियाँ और प्राथमिक डेटा संग्रह विधियाँ।

प्राथमिक डेटा:

मौजूदा शोध के लिए प्राथमिक डेटा को एंड-टू-एंड प्रश्नावली और उपयोगकर्ताओं के साक्षात्कारों से एकत्र किया गया था। पहले से परीक्षण किए गए और कोड किए गए प्रोग्राम किए गए उद्देश्यों को प्राप्त करने के लिए, उन उपयोगकर्ताओं के साथ व्यक्तिगत साक्षात्कार के माध्यम से जो साइबर सुरक्षा के नियमों को जानते हैं और भारत के महाराष्ट्र राज्य के बांद्रा, कुर्ला और अंधेरी में अपने दैनिक दिनचर्या में वित्तीय और गैर-वित्तीय लेनदेन का उपयोग करते हैं।

शोध के लिए सुलभ साधनों से शोध विषय का अध्ययन करने के लिए प्रश्नावली, साक्षात्कार और टेलीफोन/मोबाइल का प्रमुख रूप से उपयोग किया जाता है, फलस्वरूप इन उपकरणों को सूचना एकत्र करने के लिए उपयुक्त प्राथमिक स्रोतों के रूप में स्थापित किया गया है।

द्वितीयक डेटा:

द्वितीयक डेटा या द्वितीयक सूचना डेटा/सूचना का पूरक प्रकार है, जो सेकेंड-हैंड सूचना रिकॉर्ड का संयोजन है। इसमें डेटा या सूचना किसी के द्वारा किसी उद्देश्य के लिए पहले से ही एकत्रित की जाती है और वर्तमान समस्याओं के लिए उपलब्ध होती है। और इस द्वितीयक डेटा का अधिकांश भाग प्रासंगिक, शुद्ध या मूल डेटा नहीं होता है

3.3 डेटा संग्रहण के लिए उपकरण

डेटा संग्रह या डेटा का संग्रह अनुसंधान की प्रक्रिया में एक महत्वपूर्ण चरण हो सकता है। डेटा एकत्र करने के लिए आप जो उपकरण चुनते हैं, वह इस बात पर निर्भर करेगा कि आप किस तरह का डेटा एकत्र करना चाहते हैं और आप इसे कैसे एकत्र करने की योजना बना रहे हैं।

इस शोध को तैयार करने में कई सामान्य डेटा संग्रह उपकरणों का उपयोग किया गया:

- प्रश्नावली
- बैठक
- व्याख्याओं
- सरकारी स्रोत
- प्रयोगशाला प्रयोग
- इलेक्ट्रॉनिक मेल या इलेक्ट्रॉनिक संदेश

3.4 नमूना डिजाइन

नमूनाकरण डिज़ाइन एक गणितीय फ़ंक्शन है जो आपको यह संभावना देता है कि एक निश्चित नमूना लिया जाएगा। चूँकि नमूनाकरण लगभग सभी शोध परियोजनाओं का आधार है, इसलिए नमूनाकरण डिज़ाइन का अध्ययन सांख्यिकी का एक महत्वपूर्ण हिस्सा है। प्रत्यक्ष अध्ययन एक खंड-आधारित अध्ययन हो सकता है। नतीजतन, नमूनाकरण तकनीक और नमूनाकरण डिज़ाइन

समय पर लक्ष्य प्राप्त करने में महत्वपूर्ण भूमिका निभाते हैं। नमूना डिजाइन एक विशेष जनसंख्या आकार का नमूना प्राप्त करने के लिए क्रिस्टल प्रोजेक्ट है।

3.5 नमूनाकरण तकनीक / प्रक्रिया

- निरीक्षण का सही मार्जिन महत्वपूर्ण है या यूँ कहें कि विशेष साक्ष्य महत्वपूर्ण है
- असंभावना मानक भी किसी विशेष आधार का कारण हो सकता है।
- ऐसी स्थिति में, जब हम नमूना सन्निकटन बढ़ाते हैं, सटीकता में सुधार हो सकता है।

3.6 नमूने का आकार

उपरोक्त सूत्र का उपयोग करके आवश्यक नमूना आकार 720 है। सर्वेक्षण इन उत्तरदाताओं की प्रतिक्रियाओं के आधार पर पूरा किया गया है। इसलिए डेटा विश्लेषण के लिए 726 उपयोगकर्ताओं / उत्तरदाताओं पर विचार किया गया।

3.7 नमूनाकरण / जांच तकनीक

स्रोतों की सूकाई से आदर्श परीक्षण इकाई चुनने के लिए कई जांच पद्धतियाँ उपलब्ध हैं। साथ दिए गए खंड उपलब्ध विभिन्न जांच तकनीकों पर संक्षिप्त जानकारी देते हैं। उपयुक्त परीक्षण प्रक्रिया का उपयोग जांच के लिए वास्तविक एजेंट के चयन की पुष्टि करता है। परीक्षण विशेषज्ञ को जनसंख्या सीमा का सटीक आकलन करने की अनुमति देता है। इस प्रकार, निरीक्षण में बड़ी संख्या में परीक्षणों में से कुछ एजेंट परीक्षणों का चयन करना शामिल है, जो बड़ी संख्या की तुलना में अस्पष्ट डेटा, परिस्थिति या परिणाम की प्रबलता के अनुमान या पूर्वानुमान का कारण बन जाते हैं।

3.8 अध्ययन के लिए प्रयुक्त नमूना डिजाइन

अध्ययन के लिए इस्तेमाल किया गया नमूनाकरण डिज़ाइन एक सरल यादृच्छिक नमूनाकरण प्रक्रिया है। चूँकि हम विभिन्न आयु और आय समूहों से उपयोगकर्ताओं (उत्तरदाताओं) का चयन करने में रुचि रखते थे, इसलिए हमने एक-चरणीय प्रक्रिया अपनाई। अध्ययन के लिए नमूने सरल यादृच्छिक नमूनाकरण द्वारा चुने गए थे और बांद्रा, कुर्ला और अंधेरी क्षेत्र के 726 उत्तरदाताओं से डेटा प्राप्त किया गया था।

3.9 डेटा विश्लेषण और परिकल्पना परीक्षण पूरा करना

डेटा विश्लेषण मुख्य रूप से वर्णनात्मक और भिन्न सांख्यिकीय परीक्षणों का उपयोग करके किया जाता है। डेटा को प्रस्तुत करने के लिए अभिव्यंजक सांख्यिकी और चार्ट / ग्राफ़ का उपयोग किया जाता है, जबकि अनुमानात्मक सांख्यिकी का उपयोग परिकल्पना का परीक्षण करने के लिए किया जाता है। डेटा विश्लेषण करने के लिए विभिन्न वर्णनात्मक और विभिन्न सांख्यिकीय परीक्षणों का उपयोग किया जाता है। वर्णनात्मक सांख्यिकी के साथ ग्राफ़ का उपयोग डेटा प्रस्तुत करने के लिए किया जाता है जबकि अनुमानात्मक सांख्यिकी का उपयोग परिकल्पना का परीक्षण करने के लिए किया जाता है।

- काई स्क्वायर टेस्ट
- एनोवा

3.10 सांख्यिकीय निष्कर्षों के लिए उपकरण कास्ट-ऑफ

सांख्यिकी में उपयोग किए जाने वाले उपकरण SPSS हैं। IBM SPSS (सामाजिक विज्ञान के लिए सांख्यिकी पैकेज) दुनिया का अग्रणी सांख्यिकीय सॉफ्टवेयर है जो अनियोजित विश्लेषण, परिकल्पना परीक्षण और पूर्वानुमान विश्लेषण के उपयोग के माध्यम से अनुसंधान और व्यावसायिक जटिलताओं को सुलझाने में मदद करता है। IBM SPSS 23 का उपयोग डेटा को पहचानने, रुझानों का विश्लेषण करने, पूर्वानुमान लगाने और धारणा को मान्य करने और सही निर्णय लेने के लिए किया जाता है। प्रौद्योगिकी के समय में सांख्यिकीय निष्कर्ष खोजने के लिए कुछ उपकरण हैं जो SPSS, IBM, SPSS हैं। SPSS अग्रणी सांख्यिकीय सॉफ्टवेयर है जो हमें विश्लेषण करने और शोध करने में मदद करता है।

अध्याय 4 डेटा विश्लेषण

इस अध्याय में एकत्रित डेटा का सांख्यिकीय विश्लेषण प्रस्तुत किया गया है। इसमें लिंग, आयु, शिक्षा स्तर आदि के आधार पर साइबर सुरक्षा जागरूकता, डिजिटल भुगतान, ऑनलाइन धोखाधड़ी, डेटा सुरक्षा, केवाईसी अपडेट, भुगतान गेटवे चयन जैसी विभिन्न समस्याओं और व्यवहारों का विश्लेषण किया गया है। विभिन्न तालिकाओं और परीक्षणों के माध्यम से यह दर्शाया गया है कि साइबर सुरक्षा से संबंधित चुनौतियाँ समाज के विभिन्न वर्गों को किस प्रकार प्रभावित करती हैं।

यह अध्याय मात्रात्मक और गुणात्मक दोनों तरह के डेटा के विश्लेषण से संबंधित है। प्राथमिक डेटा इंटरनेट बैंकिंग के ग्राहकों के उपयोग, अपने बैंक खाते में साइबर अपराध का अनुभव करने वाले और पीड़ित बनने वाले ग्राहकों और साइबर अपराध का अनुभव न करने वाले या गैर-पीड़ित लोगों के संबंध में एकत्र किया गया था। इसमें पीड़ितों और गैर-पीड़ितों दोनों की साइबर अपराध की धारणा और उनके बैंकों से उनकी अपेक्षाओं का विश्लेषण शामिल है। इसमें पाँच बैंक अधिकारियों, पाँच पीड़ितों, एक साइबर सेल अपराध शाखा पुलिस अधिकारी और एक नैतिक हैकर के साक्षात्कार और इन साक्षात्कारों का विश्लेषण भी शामिल है।

तालिका 4. लिंग

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
पुरुष	432	59.5	59.5	59.5
महिला	294	40.5	40.5	100.0
कुल	726	100.0	100.0	

लिंग के आधार पर उत्तरदाताओं का वर्गीकरण ऊपर दी गई तालिका 4.1 में प्रस्तुत किया गया है। आंकड़ों से पता चलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएं थीं।

तालिका 4. आयु

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
18 से 25	317	43.7	43.7	43.7
25 से 46	379	52.2	52.2	95.9
46 से 60	28	3.9	3.9	99.7
60 से ऊपर	2	.3	.3	100.0
कुल	726	100.0	100.0	

उत्तरदाताओं का आयु के आधार पर वर्गीकरण ऊपर दी गई तालिका 4.2 में प्रस्तुत किया गया है। आंकड़ों से पता चलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18-25

आयु वर्ग के थे, 379 25-46 आयु वर्ग के थे, 28 46-60 आयु वर्ग के थे और 2 60 वर्ष से अधिक आयु के थे।

तालिका 4. शिक्षा

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
एचएससी तक	53	7.3	7.3	7.3
डिप्लोमा	6	.8	.8	8.1
स्नातक	277	38.2	38.2	46.3
स्नातकोत्तर	362	49.9	49.9	96.1
पीएच.डी.	12	1.7	1.7	97.8
चार्टर्ड एकाउंटेंट	14	1.9	1.9	99.7
रिसर्च स्कॉलर	2	.3	.3	100.0
कुल	726	100.0	100.0	

शिक्षा के आधार पर उत्तरदाताओं का वर्गीकरण ऊपर दी गई तालिका 4.3 में प्रस्तुत किया गया है। आंकड़ों से पता चलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 53 एचएससी तक शिक्षित थे, उनमें से 6 ने डिप्लोमा किया था, 277 स्नातक थे, 362 विभिन्न धाराओं में स्नातकोत्तर थे, 12 पीएचडी धारक थे, 14 चार्टर्ड अकाउंटेंट थे और 2 शोध छात्र थे।

तालिका 4. उपकरणों का नियमित उपयोग

उपकरण	उत्तरदाताओं की संख्या	को PERCENTAGE
स्मार्ट फोन	694	95.6
मैक	70	9.6
टैबलेट	72	9.9
पीसी	284	39.1

उपरोक्त तालिका 4.4 से यह निर्धारित किया जा सकता है कि 70 उत्तरदाता मैक उपयोगकर्ता थे, 284 उत्तरदाता पर्सनल कंप्यूटर (पीसी) के उपयोगकर्ता थे, 694 उत्तरदाता स्मार्ट फोन उपयोगकर्ता थे और 72 उत्तरदाता टैबलेट के उपयोगकर्ता थे।

तालिका 4. आपका पीसी किस ऑपरेटिंग सिस्टम (ओएस) का उपयोग करता है?

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
विंडोज़	609	83.9	83.9	83.9
लबादा	46	6.3	6.3	90.2
लागू नहीं	66	9.8	9.8	100.0
कुल	726	100.0	100.0	

उपरोक्त तालिका 4.5 से यह पता चलता है कि 609 उत्तरदाता अपने-अपने पर्सनल कंप्यूटर में विंडोज ऑपरेटिंग सिस्टम और 46 उत्तरदाता मैकिन्टोश ऑपरेटिंग सिस्टम का इस्तेमाल कर रहे थे। हालाँकि, 66 उत्तरदाता पर्सनल कंप्यूटर का इस्तेमाल बिल्कुल नहीं कर रहे थे।

तालिका 4. आपका फ़ोन किस ऑपरेटिंग सिस्टम का उपयोग करता है?

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
एंड्रॉयड	611	84.2	84.2	84.2
आईओएस (एप्पल)	111	15.3	15.3	99.4
विंडोज़	4	.6	.6	100.0
कुल	726	100.0	100.0	

उपरोक्त तालिका 4.6 से यह निर्धारित किया जा सकता है कि शोध में शामिल 726 उत्तरदाताओं में से 611 उत्तरदाताओं ने अपने-अपने फोन पर एंड्रॉयड ऑपरेटिंग सिस्टम, 111 उत्तरदाताओं ने आईफोन ऑपरेटिंग सिस्टम और 4 उत्तरदाताओं ने विंडोज ऑपरेटिंग सिस्टम का इस्तेमाल किया। प्रतिशत के संदर्भ में, 84 प्रतिशत उत्तरदाताओं ने एंड्रॉयड ऑपरेटिंग सिस्टम, 15 प्रतिशत उत्तरदाताओं ने आईफोन ऑपरेटिंग सिस्टम और 1 प्रतिशत उत्तरदाताओं ने अपने-अपने फोन पर विंडोज ऑपरेटिंग सिस्टम का इस्तेमाल किया। इसलिए, एंड्रॉयड ऑपरेटिंग सिस्टम का इस्तेमाल करने वाले उत्तरदाताओं की संख्या आईओएस और विंडोज ऑपरेटिंग सिस्टम का इस्तेमाल करने वालों से अधिक थी।

तालिका 4. आपका टैबलेट किस ऑपरेटिंग सिस्टम (OS) का उपयोग करता है?

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
एंड्रॉयड	250	34.4	34.4	34.4
आईओएस (एप्पल)	143	19.7	19.7	54.1
विंडोज़	24	3.3	3.3	57.4
लागू नहीं	309	42.6	42.6	100.0
कुल	726	100.0	100.0	

उपरोक्त तालिका 4.7 से यह पता चलता है कि 250 उत्तरदाता एंड्रॉयड ऑपरेटिंग सिस्टम, 143 उत्तरदाता आईफोन ऑपरेटिंग सिस्टम और 24 उत्तरदाता अपने-अपने टैबलेट में विंडोज ऑपरेटिंग सिस्टम का इस्तेमाल कर रहे थे। हालाँकि, 309 उत्तरदाता टैबलेट का इस्तेमाल नहीं कर रहे थे।

तालिका 4. क्या आप पारंपरिक तरीकों की तुलना में ऑनलाइन लेनदेन को प्राथमिकता देते हैं?

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
हाँ	619	85.3	85.3	85.3
नहीं	107	14.7	14.7	100.0
कुल	726	100.0	100.0	

ऊपर दी गई तालिका 4.8 में पारंपरिक तरीकों की तुलना में ऑनलाइन लेनदेन को प्राथमिकता दी गई है। तालिका 4.9 से यह पता चलता है कि 619 उत्तरदाता पारंपरिक तरीकों की तुलना में ऑनलाइन लेनदेन को प्राथमिकता देते हैं। हालाँकि, 107 उत्तरदाता अभी भी ऑनलाइन की तुलना में पारंपरिक तरीकों को प्राथमिकता देते हैं।

तालिका 4. आप कितनी बार ऑनलाइन लेनदेन करते हैं?

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
दैनिक	112	15.4	15.4	15.4
साप्ताहिक	220	30.3	30.3	45.7
महीने के	394	54.3	54.3	100.0
कुल	726	100.0	100.0	

तालिका 4.9 से यह निर्धारित किया जा सकता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 112 उत्तरदाता दैनिक आधार पर ऑनलाइन लेनदेन करते हैं, 220 उत्तरदाता साप्ताहिक आधार पर ऑनलाइन लेनदेन करते हैं और 394 उत्तरदाता मासिक आधार पर ऑनलाइन लेनदेन करते हैं।

तालिका 4. आप आमतौर पर किस प्रकार के ऑनलाइन लेनदेन को पसंद करते हैं?

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
वित्तीय	183	25.2	29.0	29.0
दोनों	449	61.8	71.0	100.0
कुल	632	87.1	100.0	
गुम	94	12.9		
कुल	726	100.0		

तालिका 4.10 से यह निर्धारित किया जा सकता है कि 183 उत्तरदाता गैर-वित्तीय लेनदेन की तुलना में वित्तीय लेनदेन को प्राथमिकता देते हैं और 94 उत्तरदाता वित्तीय लेनदेन की तुलना में गैर-वित्तीय लेनदेन को प्राथमिकता देते हैं। हालाँकि, 449 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन करते समय वित्तीय और गैर-वित्तीय दोनों लेनदेन समान रूप से महत्वपूर्ण हैं। प्रतिशत

के संदर्भ में, 25 प्रतिशत उत्तरदाता गैर-वित्तीय लेनदेन की तुलना में वित्तीय लेनदेन को प्राथमिकता देते हैं और 13 प्रतिशत उत्तरदाता वित्तीय लेनदेन की तुलना में गैर-वित्तीय लेनदेन को प्राथमिकता देते हैं। हालांकि, 62 प्रतिशत उत्तरदाताओं का मानना है कि ऑनलाइन लेनदेन करते समय वित्तीय और गैर-वित्तीय लेनदेन समान रूप से महत्वपूर्ण हैं। इसलिए, जिन उत्तरदाताओं को लगा कि ऑनलाइन लेनदेन करते समय वित्तीय और गैर-वित्तीय लेनदेन समान रूप से महत्वपूर्ण हैं, उनकी संख्या गैर-वित्तीय लेनदेन की तुलना में वित्तीय लेनदेन और वित्तीय लेनदेन की तुलना में गैर-वित्तीय लेनदेन को प्राथमिकता देने वालों से अधिक है।

तालिका 4.10 आपने इनमें से कौन से वित्तीय लेनदेन किए हैं?

लेन-देन	उत्तरदाताओं की संख्या	को PERCENTAGE
एनईएफटी/आरटीजीएस भेजना	397	54.68
नकद जमा	362	49.86
नकद निकासी	385	53.03
एक खाते से दूसरे खाते में धन का स्थानांतरण	426	58.68
प्रेषण	62	8.54
विदेशी मुद्रा	56	7.71
प्रतिभूति	58	7.99

उपरोक्त तालिका 4.10 में उत्तरदाताओं द्वारा सामान्यतः किए जाने वाले वित्तीय लेनदेन दिखाए गए हैं। तालिका 4.10 से यह निर्धारित किया जा सकता है कि 395 उत्तरदाता NEFT/RTGS भेजने के लिए ऑनलाइन वित्तीय लेनदेन का उपयोग करते हैं, 362 उत्तरदाता नकद जमा भेजने के लिए ऑनलाइन वित्तीय लेनदेन का उपयोग करते हैं, 385 उत्तरदाता नकद निकासी के लिए ऑनलाइन वित्तीय लेनदेन का उपयोग करते हैं, 426 उत्तरदाता एक खाते से दूसरे खाते में धन हस्तांतरण के लिए ऑनलाइन वित्तीय लेनदेन का उपयोग करते हैं, 62 उत्तरदाता प्रेषण के लिए ऑनलाइन वित्तीय लेनदेन का उपयोग करते हैं, 56 उत्तरदाता विदेशी मुद्रा के लिए ऑनलाइन वित्तीय लेनदेन का उपयोग करते हैं और 58 उत्तरदाता प्रतिभूतियों के लिए ऑनलाइन वित्तीय लेनदेन का उपयोग करते हैं।

तालिका 4. इनमें से आपने कौन से गैर-वित्तीय लेनदेन किए हैं?

लेन-देन	उत्तरदाताओं की संख्या	को PERCENTAGE
---------	--------------------------	------------------

ग्राहक विवरण जैसे मोबाइल नम्बर, पता आदि अद्यतन करना।	451	62.12
खाता खोलना और खाता बंद करना	254	34.99
तुला राशि जाँच	507	69.83
खाता विवरण प्रिंट करना	256	35.26
चेक बुक/पास बुक जारी करना	231	31.82
केवाईसी अपडेट	319	43.94

ऊपर दी गई तालिका 4.11 में उत्तरदाताओं द्वारा आम तौर पर किए जाने वाले गैर-वित्तीय लेनदेन दिखाए गए हैं। तालिका 4.11 से यह पता चलता है कि 451 उत्तरदाता ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को अपडेट करने के लिए ऑनलाइन गैर-वित्तीय लेनदेन का उपयोग करते हैं, 254 उत्तरदाता खाता खोलने और खाता बंद करने के लिए ऑनलाइन गैर-वित्तीय लेनदेन का उपयोग करते हैं, 507 उत्तरदाता शेष राशि की जांच के लिए ऑनलाइन गैर-वित्तीय लेनदेन का उपयोग करते हैं, 256 उत्तरदाता खाता विवरण प्रिंट करने के लिए ऑनलाइन गैर-वित्तीय लेनदेन का उपयोग करते हैं, 231 उत्तरदाता चेक बुक/पासबुक जारी करने के लिए ऑनलाइन गैर-वित्तीय लेनदेन का उपयोग करते हैं और 319 उत्तरदाता केवाईसी अपडेट के लिए ऑनलाइन गैर-वित्तीय लेनदेन का उपयोग करते हैं।

तालिका 4. ऑनलाइन लेनदेन में आपको किन चुनौतियों का सामना करना पड़ता है?

चुनौतियां	उत्तरदाताओं	प्रतिशत
ऑनलाइन धोखाधड़ी और चार्जबैक	334	46.01
डेटा सुरक्षा	411	56.61
अंतर्राष्ट्रीय ऑनलाइन भुगतान	87	11.98
भुगतान गेटवे चुनना	171	23.55
बहुमुद्रा भुगतान स्वीकार करना	56	7.71
डिजिटल भुगतान विफलता	355	48.90

ऊपर दी गई तालिका 4.12 ऑनलाइन लेनदेन (वित्तीय और गैर-वित्तीय) करते समय उत्तरदाताओं द्वारा सामना की जाने वाली चुनौतियों को दर्शाती है। तालिका 4.13 से, यह निर्धारित किया जा सकता है कि 334 उत्तरदाताओं को ऑनलाइन धोखाधड़ी और चार्ज बैक की चुनौती का सामना करना पड़ा, 411 उत्तरदाताओं को डेटा सुरक्षा की चुनौती का सामना करना पड़ा, 87 उत्तरदाताओं को अंतर्राष्ट्रीय ऑनलाइन भुगतान की चुनौती का सामना करना पड़ा, 171 उत्तरदाताओं को भुगतान गेटवे चुनने की चुनौती का सामना करना पड़ा, 56 उत्तरदाताओं को

बहु-मुद्रा भुगतान स्वीकार करने की चुनौती का सामना करना पड़ा और 355 उत्तरदाताओं को डिजिटल भुगतान विफलता की चुनौती का सामना करना पड़ा।

तालिका 4. यह भावना कि ऑनलाइन सुरक्षा महत्वपूर्ण है

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
हाँ	680	93.7	93.7	93.7
कुछ हद तक महत्वपूर्ण.	36	5.0	5.0	98.6
नहीं	10	1.4	1.4	100.0
कुल	726	100.0	100.0	

ऊपर दी गई तालिका 4.13 ऑनलाइन लेनदेन के महत्व पर उत्तरदाताओं की धारणाओं को दर्शाती है। तालिका 4.13 से यह निर्धारित किया जा सकता है कि 680 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन महत्वपूर्ण हैं, 36 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन कुछ हद तक महत्वपूर्ण हैं। हालांकि, 10 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन बिल्कुल भी महत्वपूर्ण नहीं हैं।

तालिका 4. ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
पूरी तरह।	195	26.9	26.9	26.9
थोड़ा	451	62.1	62.1	89.0
बिल्कुल नहीं	80	11.0	11.0	100.0
कुल	726	100.0	100.0	

ऊपर दी गई तालिका 4.14 ऑनलाइन लेनदेन में सुरक्षा नियमों के बारे में उत्तरदाताओं की चिंता और जागरूकता को दर्शाती है। तालिका 4.14 से, यह निर्धारित किया जा सकता है कि 195 उत्तरदाता ऑनलाइन लेनदेन में सुरक्षा नियमों के बारे में चिंतित थे और पूरी तरह से जागरूक थे, 451 उत्तरदाता थोड़े चिंतित थे और ऑनलाइन लेनदेन में सुरक्षा नियमों के बारे में आंशिक रूप से जागरूक थे। हालांकि, 80 उत्तरदाता ऑनलाइन लेनदेन में सुरक्षा नियमों के बारे में चिंतित नहीं थे और बिल्कुल भी जागरूक नहीं थे।

तालिका 4. ऑनलाइन लेनदेन करते समय क्या सुरक्षित रूप से साझा किया जा सकता है?

दस्तावेज़	उत्तरदाताओं	को PERCENTAGE
आधार	313	43.11

कड़ाही	158	21.76
बैंक खाता संख्या	118	16.25
क्रेडिट/डेबिट कार्ड विवरण	117	16.12
इनमें से कोई नहीं	147	20.25

उपरोक्त तालिका 4.15 उत्तरदाताओं की धारणाओं को दर्शाती है कि ऑनलाइन लेनदेन के दौरान क्या सुरक्षित रूप से साझा किया जा सकता है। तालिका 4.15 से, यह सर्वेक्षण में निर्धारित किया जा सकता है, 313 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन करते समय आधार कार्ड को सुरक्षित रूप से साझा किया जा सकता है, 158 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन करते समय पैन को सुरक्षित रूप से साझा किया जा सकता है, 118 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन करते समय बैंक खाता संख्या को सुरक्षित रूप से साझा किया जा सकता है और 117 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन करते समय क्रेडिट / डेबिट कार्ड का विवरण सुरक्षित रूप से साझा किया जा सकता है। हालांकि, 147 उत्तरदाताओं की राय थी कि ऑनलाइन लेनदेन करते समय उपर्युक्त में से कोई भी लेनदेन सुरक्षित रूप से साझा नहीं किया जा सकता है।

4.1 ऑनलाइन खतरों से जुड़े जोखिम के बारे में उत्तरदाताओं की धारणा:

ऑनलाइन खतरों से जुड़े जोखिम के बारे में उत्तरदाताओं की धारणा को मापने के लिए, उत्तरदाताओं से पाँच-बिंदु पैमाने पर अपने विचार प्रस्तुत करने के लिए कहा गया, जिसमें 1 कोई जोखिम नहीं दर्शाता जबकि 5 बहुत अधिक जोखिम दर्शाता है। विश्लेषण का परिणाम नीचे दी गई तालिका में प्रस्तुत किया गया है:

तालिका 4. आपको ऑनलाइन खतरों से खतरा होने की भावना

	एन	अर्थ	मानक व्यतिक्रम
मेलवेयर	622	3.50	1.104
फ़िशिंग	667	3.53	1.080
डेटा लीक	675	3.70	1.067
डोक्सिंग	643	3.52	1.104

उपरोक्त तालिका 4.16 से पता चलता है कि उत्तरदाताओं का मानना है कि मेलवेयर को ऑनलाइन खतरों के लिए सबसे कम जोखिम माना जाता है (सबसे कम औसत स्कोर), जबकि डेटा लीक को सबसे अधिक जोखिम माना जाता है (सबसे अधिक औसत स्कोर)।

तालिका 4. आप जिन लोगों के लिए ज़िम्मेदार हैं (यानी परिवार के सदस्य) को ऑनलाइन खतरों से कितना जोखिम महसूस करते हैं

	एन	अर्थ	मानक व्यतिक्रम
मैलवेयर	726	3.19	1.358
फ़िशिंग	726	3.30	1.276
डेटा लीक	726	3.38	1.398
डोक्सिंग	726	3.36	1.290

उपरोक्त तालिका 4.17 से पता चलता है कि उत्तरदाताओं का मानना है कि मैलवेयर से उन लोगों के लिए ऑनलाइन खतरों का सबसे कम जोखिम (सबसे कम औसत स्कोर) है जिनके लिए आप जिम्मेदार हैं, जबकि डेटा लीक को सबसे अधिक जोखिम (उच्चतम औसत स्कोर) माना जाता है।

तालिका 4. उत्तरदाता निम्नलिखित के बारे में चिंतित हैं?

	एन	अर्थ	मानक व्यतिक्रम
व्यक्तिगत डेटा चोरी और अन्य लोगों द्वारा उपयोग किया जाना	726	3.3361	1.53488
व्यक्तिगत डेटा वेबसाइटों या कंपनियों से एकत्र किया जाता है और तीसरे पक्ष को बेचा जा रहा है	726	3.3733	1.48549
बैंक विवरण गलत या नकली ऑनलाइन लेनदेन के माध्यम से चुराए जाते हैं	726	3.4890	1.46660
स्पाइवेयर से संक्रमित जो बिना जानकारी के मेरे बारे में जानकारी एकत्रित करता है	726	3.2934	1.52067
एडवेयर से चिंतित हैं?	726	3.3664	1.46053

ऊपर दी गई तालिका 4.18 से पता चलता है कि उत्तरदाताओं को स्पाइवेयर से संक्रमित होने की सबसे कम चिंता थी जो उनके बारे में बिना जाने ही जानकारी एकत्र करता है (सबसे कम औसत स्कोर)। हालाँकि, उत्तरदाताओं के इसी समूह ने अपने बैंक विवरण के चोरी होने की सबसे अधिक चिंता दिखाई। खराब या नकली ऑनलाइन लेनदेन (सबसे अधिक औसत स्कोर)।

तालिका 4. उत्तरदाता निम्नलिखित के बारे में चिंतित हैं

	एन	अर्थ	मानक व्यतिक्रम
रैंसमवेयर	726	3.1763	1.50925
प्रत्युत्तरदाता की जानकारी के बिना विभिन्न उपकरणों के माध्यम से देखा जाना	726	3.3485	1.45594
सरकारी हस्तक्षेप	726	3.2218	1.44666

आपके द्वारा देखी जाने वाली वेबसाइटों के साथ स्थान की जानकारी साझा की जा रही है	726	3.3623	1.51121
--	-----	--------	---------

ऊपर दी गई तालिका 4.19 से पता चलता है कि उत्तरदाताओं को रैनसमवेयर के बारे में सबसे कम चिंता थी (सबसे कम औसत स्कोर)। हालांकि, उत्तरदाताओं के इसी समूह ने अपनी लोकेशन की जानकारी को उन वेबसाइटों के साथ साझा किए जाने के बारे में सबसे अधिक चिंता दिखाई, जिन पर वे जाते हैं (सबसे अधिक औसत स्कोर)।

तालिका 4. मैलवेयर (वायरस, दुर्भावनापूर्ण/अवांछित प्रोग्राम, एडवेयर, आदि) पिछले बारह महीनों में उत्तरदाता के डिवाइस पर स्वयं इंस्टॉल होना

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
हाँ	407	56.1	56.1	56.1
नहीं	319	43.9	43.9	100.0
कुल	726	100.0	100.0	

पिछले 12 महीनों में उनके कंप्यूटर में मैलवेयर अपने आप इंस्टॉल हो गया। तालिका 4.20 से, यह निर्धारित किया जा सकता है कि शामिल 726 उत्तरदाताओं में से, 407 उत्तरदाताओं की राय थी कि पिछले 12 महीनों में उनके कंप्यूटर में मैलवेयर अपने आप इंस्टॉल हो गया था। हालांकि, 319 उत्तरदाताओं की राय थी कि पिछले 12 महीनों में उनके कंप्यूटर में मैलवेयर अपने आप इंस्टॉल नहीं हुआ था।

तालिका 4. पिछले बारह महीनों में आपके कंप्यूटर में मौजूद वायरस को हटाने के लिए की गई कार्रवाई

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
	319	43.9	43.9	43.9
ड्राइव को फॉर्मेट किया और बैकअप के माध्यम से डेटा को पुनर्स्थापित किया	52	7.2	7.2	51.1
एंटी-वायरस स्थापित किया गया।	239	32.9	32.9	84.0
डिवाइस को अनलॉक करने के लिए फिरोती का भुगतान किया गया, क्योंकि मैलवेयर रैनसमवेयर था।	3	.4	.4	84.4
डिवाइस की मरम्मत के लिए किसी को भुगतान किया	49	6.7	6.7	91.2
डिवाइस को बदल दिया गया	7	1.0	1.0	92.1
कोई कार्रवाई नहीं की गई	43	5.9	5.9	98.1
अन्य वायरस हटाने वाले प्रोग्राम का उपयोग किया	14	1.9	1.9	100.0

ऊपर दी गई तालिका 4.21 में उत्तरदाताओं द्वारा अपने कंप्यूटर से मैलवेयर हटाने के लिए की गई कार्रवाई को दर्शाया गया है। तालिका 4.21 से, यह निर्धारित किया जा सकता है कि 52 उत्तरदाताओं ने ड्राइव को फॉर्मेट किया था और डेटा को पुनर्स्थापित करने के लिए बैकअप का उपयोग किया था, 239 उत्तरदाताओं ने एंटी-वायरस इंस्टॉल किया था, 03 उत्तरदाताओं ने डिवाइस को अनलॉक करने के लिए फिरौती का भुगतान किया था (यदि मैलवेयर रैनसमवेयर था), 49 उत्तरदाताओं ने डिवाइस की मरम्मत के लिए किसी को भुगतान किया था, 07 उत्तरदाताओं ने डिवाइस को बदल दिया था, 43 उत्तरदाताओं ने कोई कार्रवाई नहीं की और 14 उत्तरदाताओं ने अन्य वायरस हटाने वाले प्रोग्राम का उपयोग किया। हालाँकि, 319 उत्तरदाता ऐसे थे जिनके कंप्यूटर में पिछले 12 महीनों में कभी भी मैलवेयर इंस्टॉल नहीं हुआ था।

तालिका 4. डिवाइस को खतरों से बचाने के लिए की गई कार्रवाई

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
हाँ	618	85.1	85.1	85.1
नहीं	108	14.9	14.9	100.0
कुल	726	100.0	100.0	

ऊपर दी गई तालिका 4.22 से पता चलता है कि उत्तरदाताओं ने अपने डिवाइस को खतरों से बचाने के लिए कोई कार्रवाई की थी या नहीं। तालिका 4.22 से यह पता चलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 618 इस बात से सहमत हैं कि उन्होंने अपने डिवाइस को खतरों से बचाने के लिए कोई कार्रवाई की थी। हालाँकि, 108 उत्तरदाताओं ने अपने डिवाइस को खतरों से बचाने के लिए कोई कार्रवाई नहीं की थी।

तालिका 4. इनमें से आप कौन सी (यदि कोई हो) कार्रवाई करते हैं?

	एन	अर्थ	मानक व्यतिक्रम
मेरा डिवाइस पासवर्ड से सुरक्षित है	726	1.1501	.35745
कंप्यूटर पर एंटी-वायरस स्थापित किया	617	1.2204	.58112
सक्षम फ़ायरवॉल	617	1.3096	.60554
डिवाइस का बैकअप महीने में कम से कम एक बार बाहरी हार्ड-ड्राइव पर लिया गया	617	1.6629	.84887
नियमित आधार पर महीने में एक बार डिवाइस का ऑनलाइन बैकअप लें।	617	1.6840	.77854
ब्राउज़र प्लगइन्स (ऐड-ऑन) का उपयोग किया गया है जो ऑनलाइन ब्राउज़िंग को सुरक्षित बनाने के लिए डिज़ाइन किए गए हैं	617	1.6499	.80822

विज्ञापन अवरोधक का उपयोग किया	617	1.7455	.80487
अन्य सुरक्षा अनुप्रयोगों का उपयोग किया	617	1.6467	.75483
अन्य कार्रवाई की	617	1.6548	.79514

ऊपर दी गई तालिका 4.23 में उत्तरदाताओं द्वारा अपने डिवाइस को खतरों से बचाने के लिए की गई कार्रवाई को दर्शाया गया है। ऊपर दी गई तालिका 4.23 से पता चलता है कि उत्तरदाताओं को अपने कंप्यूटर पर एंटी-वायरस इंस्टॉल करने में सबसे कम दिलचस्पी थी (सबसे कम औसत स्कोर) ताकि वे अपने डिवाइस को खतरों से बचा सकें। हालाँकि, उत्तरदाताओं के उसी समूह ने ऐड-ब्लॉकर (सबसे अधिक औसत स्कोर) का उपयोग करने में सबसे अधिक रुचि दिखाई।

तालिका 4. अपने डिवाइस की सुरक्षा के लिए कोई कार्रवाई न करना

	आवृत्ति	प्रतिशत	वैधप्रतिशत	संचयीप्रतिशत
	617	85.0	85.0	85.0
अनजान, ये काम कैसे करें	36	5.0	5.0	89.9
मुझे लगता है कि मुझे किसी सुरक्षा की आवश्यकता नहीं है	26	3.6	3.6	93.5
ऐसा करने का कभी अवसर नहीं मिला/ऐसा करने के बारे में कभी सोचा नहीं	23	3.2	3.2	96.7
मुझे लगता है कि एंटीवायरस इंस्टॉल करने से मेरा कंप्यूटर धीमा हो जाएगा	24	3.3	3.3	100.0
कुल	726	100.0	100.0	

ऊपर दी गई तालिका 4.24 से यह निर्धारित किया जा सकता है कि 36 उत्तरदाता अपने डिवाइस की सुरक्षा के लिए कोई कदम नहीं उठाते क्योंकि उन्हें नहीं पता कि वे कार्रवाइयें कैसे करनी हैं, 26 उत्तरदाता अपने डिवाइस की सुरक्षा के लिए कोई कदम नहीं उठाते क्योंकि उन्हें लगता है कि उन्हें किसी सुरक्षा की आवश्यकता नहीं है, 23 उत्तरदाता अपने डिवाइस की सुरक्षा के लिए कोई कदम नहीं उठाते क्योंकि उन्हें ऐसा करने का कभी मौका ही नहीं मिला और 23 उत्तरदाता अपने डिवाइस की सुरक्षा के लिए कोई कदम नहीं उठाते क्योंकि उनका मानना है कि एंटी-वायरस इंस्टॉल करने से उनके कंप्यूटर धीमे हो सकते हैं। हालाँकि, 617 उत्तरदाता अपने डिवाइस की सुरक्षा के लिए अलग-अलग कदम उठाते हैं।

तालिका 4. यह सुनिश्चित करने के लिए उठाए गए कदम कि उत्तरदाताओं की ऑनलाइन उपस्थिति निजी बनी रहे अर्थात् खाते सुरक्षित रहें।

	आवृत्ति	प्रतिशत	वैध प्रतिशत	संचयी प्रतिशत
हाँ	579	79.8	79.8	79.8
नहीं	147	20.2	20.2	100.0
कुल	726	100.0	100.0	

ऊपर दी गई तालिका 4.25 इस बात पर प्रकाश डालती है कि क्या उत्तरदाता यह सुनिश्चित करने के लिए कदम उठाते हैं कि उनकी ऑनलाइन उपस्थिति निजी बनी रहे और खाते सुरक्षित रहें। तालिका 4.25 से यह निर्धारित किया जा सकता है कि 579 उत्तरदाताओं ने यह सुनिश्चित करने के लिए अलग-अलग उपाय किए हैं कि उनकी ऑनलाइन उपस्थिति निजी बनी रहे और खाते सुरक्षित रहें। हालाँकि, 147 उत्तरदाताओं ने कोई उपाय नहीं किया।

तालिका 4. गतिविधि/ वे कार्डिज़ें जो उत्तरदाता यह सुनिश्चित करने के लिए करते हैं कि उनकी ऑनलाइन उपस्थिति निजी रहे और खाता सुरक्षित रहे

	एन	अर्थ	मानक व्यतिक्रम
सुनिश्चित करें कि पासवर्ड सुरक्षित हैं (उन्हें एक से अधिक स्थानों पर प्रयोग न करें, सुनिश्चित करें कि वे लंबे हों तथा कंप्यूटर के लिए अनुमान लगाना कठिन हो, आदि)	579	2.0207	.43575
यदि आवंटित किया गया हो तो 2-चरणीय सत्यापन का उपयोग किया गया है सुरक्षा के लिए डिज़ाइन किए गए ब्राउज़र प्लग-इन (ऐड-ऑन) का उपयोग किया गया है	579	2.0035	.41593
उपयोगकर्ता की गोपनीयता.	579	2.0587	.64169
प्रयुक्त VPN (वर्चुअल प्राइवेट नेटवर्क)	579	1.7288	.79622
अन्य कार्रवाई की	579	2.0397	.74880

ऊपर दी गई तालिका 4.26 में वे कार्डिज़ें दिखाई गई हैं जो उत्तरदाता यह सुनिश्चित करने के लिए करते हैं कि उनकी ऑनलाइन गतिविधि निजी रहे और उनका खाता सुरक्षित रहे। ऊपर दी गई तालिका 4.26 में विश्लेषण के परिणाम दर्शाते हैं कि सबसे कम उत्तरदाता वर्चुअल प्राइवेट नेटवर्क (सबसे कम औसत स्कोर) का उपयोग करते हैं ताकि यह सुनिश्चित हो सके कि उनकी ऑनलाइन उपस्थिति निजी रहे/खाता सुरक्षित रहे। हालाँकि, अधिकतम उत्तरदाता अपनी गोपनीयता की सुरक्षा के लिए ब्राउज़र प्लग-इन का उपयोग करते हैं (उच्चतम औसत स्कोर)।

4.2 सभी लिंगों में साइबर सुरक्षा नियमों के बारे में जागरूकता:

साइबर सुरक्षा के बारे में जागरूकता में लोगों को कार्रवाई करने के लिए पर्याप्त रूप से जागरूक करना शामिल है। इसके लिए सिर्फ नियमों का एक सेट नहीं, बल्कि सुरक्षा मानसिकता बनाने की ज़रूरत है। संक्षेप में, यह सिर्फ खतरों के बारे में जागरूक होने के बारे में नहीं है, बल्कि खतरों और संगठन और उसके लोगों पर उनके प्रभाव को समझने के बारे में भी है, जिसमें खुद भी शामिल हैं। इस समझ के साथ, उचित कार्रवाई होनी चाहिए। साइबर सुरक्षा के बारे में जागरूकता एक दृष्टिकोण है। यह, शायद, परिस्थितिजन्य जागरूकता का एक विशेष हिस्सा है। इसका मतलब है जागरूक होना और कार्रवाई करना। यह कुछ हद तक "स्ट्रीट इंटेलिजेंस" जैसा है। नीचे दी गई तालिका दिखाती है कि

तालिका 4. साइबर सुरक्षा नियमों के बारे में लिंग के आधार पर जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		लिंग		कुल
		पुरुष	महिला	
पूरी तरह।	गिनती करना	119	76	195
	प्रतिशत (%)	27.5	25.9	26.9
थोड़ा	गिनती करना	261	190	451
	प्रतिशत (%)	60.4	64.6	62.1
बिल्कुल नहीं	गिनती करना	52	28	80
	प्रतिशत (%)	12.0	9.5	11.0
कुल	गिनती करना	432	294	726
	प्रतिशत (%)	100.0	100.0	100.0

उपरोक्त तालिका 4.27 से पता चलता है कि 119 पुरुष और 76 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में पूरी तरह से अवगत थे, 261 पुरुष और 190 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में आंशिक रूप से अवगत थीं। हालाँकि, 52 पुरुष और 28 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में बिल्कुल भी नहीं जानती थीं।

तालिका 4. काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	1.689ए	2	.430
संभावना अनुपात	1.705	2	.426
रैखिक-दर-रैखिक एसोसिएशन	.033	1	.856
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को अस्वीकार नहीं किया गया है क्योंकि $P > 0.05$ (0.430) है। इसलिए, साइबर सुरक्षा नियमों और लिंग के बारे में जागरूकता एक दूसरे से स्वतंत्र हैं।

4.3. सभी आयु वर्गों में साइबर सुरक्षा नियमों के बारे में जागरूकता:

सर्वेक्षण के लिए 18 से लेकर 60 वर्ष से अधिक आयु के विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका विभिन्न आयु समूहों के बीच साइबर सुरक्षा नियमों के बारे में जागरूकता को दर्शाती है।

तालिका 4. आयु वर्ग के अनुसार साइबर सुरक्षा नियमों के बारे में जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		आयु				कुल
		18 से 25	25 से 46	46 से 60	60 से ऊपर	
पूरी तरह	गिनती करना	96	95	2	2	195
	प्रतिशत (%)	30.3	25.1	7.1	100.0	26.9
थोड़ा	गिनती करना	183	252	16	0	451
	प्रतिशत (%)	57.7	66.5	57.1	0.0	62.1
बिल्कुल नहीं	गिनती करना	38	32	10	0	80
	प्रतिशत (%)	12.0	8.4	35.7	0.0	11.0
कुल	गिनती करना	317	379	28	2	726
	प्रतिशत (%)	100.0	100.0	100.0	100.0	100.0

उपरोक्त तालिका 4.29 यह निर्धारित करती है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 96 उत्तरदाता 18 से 25 आयु वर्ग के थे, 95 उत्तरदाता 25 से 46 आयु वर्ग के थे, 02 उत्तरदाता 46 से 60 आयु वर्ग के थे और 02 उत्तरदाता 60 वर्ष और उससे अधिक आयु वर्ग के थे जो ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से पूरी तरह अवगत थे। 18 से 25 आयु वर्ग के 183 उत्तरदाता, 25 से 46 आयु वर्ग के 252 उत्तरदाता और 46 से 60 आयु वर्ग के 16 उत्तरदाता ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से आंशिक रूप से अवगत थे। हालांकि, 18 से 25 आयु वर्ग के 38 उत्तरदाता, 25 से 46 आयु वर्ग के 32 उत्तरदाता और 46 से 60 आयु वर्ग के 10 उत्तरदाता ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से बिल्कुल भी अवगत नहीं थे।

तालिका 4. काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	31.646 ^a	6	.000
संभावना अनुपात	27.492	6	.000

रैखिक-दर-रैखिक एसोसिएशन	3.327	1	.068
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को $P < 0.05$ (0.000) के रूप में खारिज कर दिया गया है। इसलिए, साइबर सुरक्षा नियमों के बारे में जागरूकता और आयु एक दूसरे से स्वतंत्र नहीं हैं।

4.4. शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता:

सर्वेक्षण के लिए अलग-अलग शैक्षणिक पृष्ठभूमि वाले 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका अलग-अलग शैक्षणिक पृष्ठभूमि वाले विभिन्न उत्तरदाताओं के बीच साइबर सुरक्षा नियमों के बारे में जागरूकता को दर्शाती है।

तालिका 4. शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		शिक्षा							कुल
		एचएस सी तक	डिप्लो मा	स्नातक	स्नातकोत्तर	पीएच.डी.	सीए	रिसर्च स्कॉलर	
पूरी तरह	गिनती करना	21	0	69	95	2	8	0	195
	%	39.6	0	24.9	26.2	16.7	57.1	0	26.9
थोड़ा	गिनती करना	22	4	165	246	6	6	2	451
	%	41.5	66.7	59.6	68	50	42.9	100	62.1
बिल्कुल नहीं	गिनती करना	10	2	43	21	4	0	0	80
	%	18.9	33.3	15.5	5.8	33.3	0	0	11
कुल	गिनती करना	53	6	277	362	12	14	2	726
	%	100	100	100	100	100	100	100	100

उपरोक्त तालिका 4.31 में बताया गया है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 195 (21 एच.एस.सी. तक, 69 स्नातक, 95 स्नातकोत्तर, 02 पी.एच.डी. और 08 चार्टर्ड अकाउंटेंट) उत्तरदाता साइबर सुरक्षा नियमों के बारे में चिंतित और पूरी तरह से अवगत थे। 451 (22 एच.एस.सी. तक, 4 डिप्लोमा, 165 स्नातक, 246 स्नातकोत्तर, 06 पी.एच.डी., 06 चार्टर्ड अकाउंटेंट और 02 रिसर्च स्कॉलर) उत्तरदाता भी चिंतित थे, लेकिन साइबर सुरक्षा नियमों के बारे में आंशिक

रूप से जानते थे। हालांकि, 80 (10 एच.एस.सी. तक, 02 डिप्लोमा, 43 स्नातक, 21 स्नातकोत्तर और 04 पी.एच.डी.) उत्तरदाता बिल्कुल भी चिंतित नहीं थे और न ही वे साइबर सुरक्षा नियमों के बारे में जानते थे।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	45.457ए	12	.000
संभावना अनुपात	46.234	12	.000
रैखिक-दर-रैखिक एसोसिएशन	2.264	1	.132
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को $P < 0.05$ (0.000) के रूप में खारिज कर दिया गया है। इसलिए, साइबर सुरक्षा नियमों और शिक्षा के बारे में जागरूकता एक दूसरे से स्वतंत्र नहीं हैं।

4.5. विभिन्न लिंगों के बीच एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.33 लिंग के आधार पर NEFT/RTGS/IMPS भेजने के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **विभिन्न लिंगों में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन**

लिंग		एनईएफटी/आरटीजीएस भेजना		कुल
		नहीं	हाँ	
पुरुष	गिनती करना	216	216	432
	लिंग के भीतर %	50.00	50.00	100.00
महिला	गिनती करना	113	181	294
	लिंग के भीतर %	38.40	61.60	100.00
कुल	गिनती करना	329	397	726
	लिंग के भीतर %	45.30	54.70	100.00

तालिका 4.33 से यह देखा जा सकता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 216 पुरुष NEFT/RTGS/IMPS भेजकर वित्तीय लेन-देन करना पसंद करते हैं जबकि 216 पुरुष NEFT/RTGS/IMPS ऑनलाइन भेजकर वित्तीय लेन-देन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 118

महिलाएँ NEFT/RTGS/IMPS भेजकर वित्तीय लेन-देन करना पसंद करती हैं जबकि 113 महिलाएँ NEFT/RTGS/IMPS ऑनलाइन भेजकर वित्तीय लेन-देन करना पसंद नहीं करती हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीए फ	असिम्प्ट. सिग. (2-पक्षीय)	सटीक हस्ताक्षर.(दो तरफा)	सटीक हस्ताक्षर.(दो तरफा)
पियर्सन काई-स्क्वायर	9.442ए	1	0.002		
निरंतरता सुधार	8.981	1	0.003		
संभावना अनुपात	9.493	1	0.002		
फिशर का सटीक परीक्षण				0.002	0.001
रैखिक-दर-रैखिक एसोसिएशन	9.429	1	0.002		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज करते हैं कि NEFT/RTGS/IMPS का उपयोग और लिंग स्वतंत्र हैं (काई-स्क्वायर 9.422, df 1, $p < 0.05$)। इस प्रकार, NEFT/RTGS/IMPS जैसे वित्तीय लेन-देन का उपयोग व्यक्ति के लिंग पर निर्भर करता है। भारत जैसे देश में, ज़्यादातर महिलाएँ पुरुषों पर निर्भर हैं। इसलिए, NEFT/RTGS/IMPS जैसे वित्तीय लेन-देन का उपयोग व्यक्ति के लिंग पर निर्भर करता है।

4.6. विभिन्न लिंगों के बीच नकद जमा के वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.35 विभिन्न लिंगों द्वारा किए गए नकद जमा के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **विभिन्न लिंगों में नकद जमा के वित्तीय लेनदेन**

			नकद जमा		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	221	211	432
		लिंग के भीतर %	51.2	48.8	100
	महिला	गिनती करना	143	151	294
		लिंग के भीतर %	48.6	51.4	100
	कुल	गिनती करना	364	362	726
		लिंग के भीतर %	50.1	49.9	100

तालिका 4.35 से पता चलता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 211 पुरुष नकद जमा का वित्तीय लेन-देन करना पसंद करते हैं जबकि 221 पुरुष नकद जमा का वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 151 महिलाएँ नकद जमा का वित्तीय लेन-देन करना पसंद करती हैं जबकि 143 महिलाएँ नकद जमा भेजना ऑनलाइन करना पसंद नहीं करती हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

			असिम्प.		
	कीमत	डीएफ	सिग. (दो तरफा)	सटीक सिग. (दो तरफा)	सटीक सिग. (1-पक्षीय)
पियर्सन काई-स्क्वायर	.444 ^a	1	0.505		
निरंतरता सुधार	0.349	1	0.555		
संभावना अनुपात	0.444	1	0.505		
फिशर का सटीक परीक्षण				0.545	0.277
रैखिक-दर-रैखिक एसोसिएशन	0.443	1	0.506		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि नकद जमा का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 0.444, df 1, $p > 0.05$)। इस प्रकार, नकद जमा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है। कोई भी व्यक्ति नकद जमा कर सकता है, चाहे वह परिवार का कमाने वाला सदस्य हो या आश्रित सदस्य। इसलिए, नकद जमा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.7. विभिन्न लिंगों के बीच नकद निकासी के वित्तीय लेनदेन

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.37 विभिन्न लिंगों द्वारा किए गए नकद निकासी के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **विभिन्न लिंगों में नकद निकासी के वित्तीय लेनदेन**

			नकद निकासी		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	211	221	432
		लिंग के भीतर %	48.8	51.2	100
	महिला	गिनती करना	130	164	294

	लिंग के भीतर %	44.2	55.8	100
कुल	गिनती करना	341	385	726
	लिंग के भीतर %	47	53	100

तालिका 4.37 से यह देखा जा सकता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 221 पुरुष नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं जबकि 211 पुरुष ऑनलाइन नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 164 महिलाएँ नकद निकासी के वित्तीय लेन-देन करना पसंद करती हैं जबकि 130 महिलाएँ ऑनलाइन नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करती हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीए फ	असिम्ट. सिग. (1-पक्षीय)	सटीक सिग. (1-पक्षीय)	सटीक सिग. (1-पक्षीय)
पियर्सन काई-स्क्वायर	1.502ए	1	0.22		
निरंतरता सुधार	1.32	1	0.25		
संभावना अनुपात	1.5	1	0.22		
फिशर का सटीक परीक्षण				0.23	0.13
रैखिक-दर-रैखिक एसोसिएशन	1.5	1	0.22		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि नकद निकासी का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 0.444, df 1, $p > 0.05$)। इस प्रकार, नकद निकासी जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है। कोई भी व्यक्ति नकद निकाल सकता है, चाहे वह परिवार का कमाने वाला सदस्य हो या आश्रित सदस्य। इसलिए, नकद निकासी जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.8 विभिन्न लिंगों के बीच एक खाते से दूसरे खाते में धन हस्तांतरण का वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.39 में विभिन्न लिंगों द्वारा एक खाते से दूसरे खाते में किए गए धन हस्तांतरण के वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. विभिन्न लिंगों के बीच एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन

			एक खाते से दूसरे खाते में धन का स्थानांतरण		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	162	270	432
		लिंग के भीतर %	37.5	62.5	100
	महिला	गिनती करना	138	156	294
		लिंग के भीतर %	46.9	53.1	100
कुल		गिनती करना	300	426	726
		लिंग के भीतर %	41.3	58.7	100

तालिका 4.39 के अनुसार सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 270 पुरुष एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेन-देन करना पसंद करते हैं जबकि 162 पुरुष एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करते हैं। इसी तरह, उन 294 महिलाओं में से 156 महिलाएँ एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेन-देन करना पसंद करती हैं जबकि 138 महिलाएँ एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करती हैं।

तालिका 4. काई-स्क्वायर परीक्षण

	कीमत	डीए फ	असिम्प्ट. सिग. (2-पक्षीय)	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)
पियर्सन काई-स्क्वायर	6.428ए	1	0		
निरंतरता सुधार	6	1	0		
संभावना अनुपात	6.4	1	0		
फिशर का सटीक परीक्षण				0	0
रैखिक-दर-रैखिक एसोसिएशन	6.4	1	0		
वैध मामलों की संख्या N	726				

उपरोक्त परीक्षण में शून्य परिकल्पना को $P < 0.05$ (0) के आधार पर अस्वीकृत किया गया है। इसलिए, एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन और लिंग एक दूसरे से स्वतंत्र नहीं हैं।

ऊपर प्रस्तुत किए गए कार्ई-स्कायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार करते हैं कि एक खाते से दूसरे खाते में धन हस्तांतरण का उपयोग और लिंग स्वतंत्र हैं (कार्ई-स्कायर 6.428, df 1, $p < 0.05$)। इसलिए, एक खाते से दूसरे खाते में धन हस्तांतरण जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर करता है। भारत जैसे देश में अधिकांश महिलाएँ पुरुषों पर निर्भर हैं। इसलिए, एक खाते से दूसरे खाते में धन हस्तांतरण जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर करता है।

4.9. विभिन्न लिंगों के बीच धन प्रेषण के वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.41 विभिन्न लिंगों द्वारा किए गए धन प्रेषण के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. विभिन्न लिंगों में धन प्रेषण के वित्तीय लेनदेन

			प्रेषण		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	401	31	432
		लिंग के भीतर %	92.8	7.2	100
	महिला	गिनती करना	263	31	294
		लिंग के भीतर %	89	11	100
कुल		गिनती करना	664	62	726

तालिका 4.41 से पता चलता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 31 पुरुष प्रेषण के वित्तीय लेन-देन करना पसंद करते हैं जबकि 401 पुरुष प्रेषण के वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करते हैं। इसी तरह, उन 294 महिलाओं में से 31 महिलाएँ प्रेषण के वित्तीय लेन-देन करना पसंद करती हैं जबकि 263 महिलाएँ प्रेषण के वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करती हैं।

तालिका 4. कार्ई-स्कायर परीक्षण

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)
पियर्सन कार्ई-स्कायर	2.541ए	1	0.1		
निरंतरता सुधार	2.1	1	0.1		
संभावना अनुपात	2.5	1	0.1		
फिशर का सटीक परीक्षण				0.1	0.1

रैखिक-दर-रैखिक एसोसिएशन	2.5	1	0.1		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए कार्ई-स्कायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि धन प्रेषण का उपयोग और लिंग स्वतंत्र नहीं हैं (कार्ई-स्कायर 2.541, df 1, $p > 0.05$)। इसलिए, धन प्रेषण जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है। धन प्रेषण धन का एक हस्तांतरण है, जो अक्सर एक विदेशी कर्मचारी द्वारा अपने मूल देश में किसी व्यक्ति को किया जाता है। इसलिए, धन प्रेषण जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.10. विभिन्न लिंगों के बीच विदेशी मुद्रा का वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.43 में विभिन्न लिंगों द्वारा किए गए धन प्रेषण के वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. **विभिन्न लिंगों में विदेशी मुद्रा के वित्तीय लेनदेन**

			विदेशी मुद्रा		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	407	25	432
लिंग		लिंग के भीतर %	94.2	5.8	100
	महिला	गिनती करना	263	31	294
		लिंग के भीतर %	90	10	100
कुल		गिनती करना	670	56	726

सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएं थीं। इन 432 पुरुषों में से 25 पुरुष फॉरेक्स के वित्तीय लेन-देन करना पसंद करते हैं जबकि 407 पुरुष ऑनलाइन फॉरेक्स के वित्तीय लेन-देन करना पसंद नहीं करते हैं। इसी तरह, उन 294 महिलाओं में से 31 महिलाएं प्रेषण के वित्तीय लेन-देन करना पसंद करती हैं जबकि 263 महिलाएं ऑनलाइन फॉरेक्स के वित्तीय लेन-देन करना पसंद नहीं करती हैं।

तालिका 4. **कार्ई-स्कायर परीक्षण**

	कीमत	डीए फ	असिम्ट. सिग. (2-पक्षीय)	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)
--	------	----------	----------------------------	------------------------	------------------------

पियर्सन काई-स्क्वायर	5.562ए	1	0		
निरंतरता सुधार	4.9	1	0		
संभावना अनुपात	5.4	1	0		
फिशर का सटीक परीक्षण				0	0
रैखिक-दर-रैखिक एसोसिएशन	5.6	1	0		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के प्रभाव इस शून्य परिकल्पना को खारिज करते हैं कि फॉरेक्स का उपयोग और लिंग स्वतंत्र हैं (काई-स्क्वायर 5.562, डीएफ 1, पी < 0.05)। इसलिए, फॉरेक्स जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर करता है। मुद्रा (फॉरेक्स) विनिमय बाजार को संदर्भित करता है। फॉरेक्स कुछ और नहीं बल्कि ओटीसी बाजार है जिसके दौरान ग्रह की विदेशी मुद्राओं का कारोबार होता है। यह दुनिया के सबसे महत्वपूर्ण और सबसे अधिक तरल बाजारों में से एक है। इसलिए, फॉरेक्स जैसे मौद्रिक लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर करता है। इसलिए, फॉरेक्स जैसे मौद्रिक लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर करता है।

4.11. विभिन्न लिंगों के बीच प्रतिभूतियों का वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.45 विभिन्न लिंगों द्वारा किए गए प्रतिभूतियों के वित्तीय लेनदेन को दर्शाती है।

तालिका 4. विभिन्न लिंगों में प्रतिभूतियों के वित्तीय लेनदेन

			प्रतिभूति		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	406	26	432
लिंग		लिंग के भीतर %	94	6	100
	महिला	गिनती करना	262	32	294
		लिंग के भीतर %	89	11	100
कुल		गिनती करना	668	58	726

तालिका 4.45 से पता चलता है कि 26 पुरुष प्रतिभूतियों का वित्तीय लेनदेन करना पसंद करते हैं जबकि 406 पुरुष प्रतिभूतियों का वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं। इसी

प्रकार, उन 294 महिलाओं में से 32 महिलाएं प्रतिभूतियों का वित्तीय लेनदेन करना पसंद करती हैं जबकि 262 महिलाएं प्रतिभूतियों का वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करती हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीए फ	असिम्ट. सिग. (2-पक्षीय)	सटीक सिग. (दो तरफ़ा)	सटीक सिग. (1- पक्षीय)
पियर्सन काई-स्क्वायर	5.635ए	1	0		
निरंतरता सुधार	5	1	0		
संभावना अनुपात	5.5	1	0		
फिशर का सटीक परीक्षण				0	0
रैखिक-दर-रैखिक एसोसिएशन	5.6	1	0		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किया गया काई-स्क्वायर परीक्षण शून्य परिकल्पना को खारिज करता है, कि प्रतिभूतियों का उपयोग और लिंग स्वतंत्र हैं (काई-स्क्वायर 5.635, df 1, $p < 0.05$)। इसलिए, प्रतिभूतियों जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर करता है। प्रतिभूतियाँ किसी कंपनी या सरकार द्वारा जारी किए जाने वाले परक्राम्य वित्तीय साधन हैं जो किसी विकल्प के लिए स्वामित्व अधिकार, ऋण अधिकार या खरीद, बिक्री या विनिमय अधिकार प्रदान करते हैं। इसलिए, प्रतिभूतियों जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर करता है।

4.12. विभिन्न माध्यमों से एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन:

सर्वेक्षण के लिए अलग-अलग आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.47 में आयु के अनुसार NEFT/RTGS/IMPS भेजने के वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. **विभिन्न आयु वर्गों में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन**

			एनईएफटी/आरटीजीएस भेजना		कुल
			नहीं	हाँ	
आयु	18 से 25	गिनती करना	168	149	317

		आयु के भीतर %	53.0%	47.0%	100.0%
	25 से 46	गिनती करना	152	227	379
		आयु के भीतर %	40.1%	59.9%	100.0%
	46 से 60	गिनती करना	9	19	28
		आयु के भीतर %	32.1%	67.9%	100.0%
	60 से ऊपर	गिनती करना	0	2	2
		आयु के भीतर %	0.0%	100.0%	100.0%
कुल		गिनती करना	329	397	726
		आयु के भीतर %	45.3%	54.7%	100.0%

तालिका 4.47 दर्शाती है कि सर्वेक्षण में 726 उत्तरदाता शामिल थे, जिनमें से 317 18-25 आयु वर्ग के थे, 379 25-46 आयु वर्ग के थे, 28 46-60 आयु वर्ग के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 आयु वर्ग के बीच के लोगों में से 149 एनईएफटी/आरटीजीएस/आईएमपीएस भेजकर वित्तीय लेनदेन करना पसंद करते हैं जबकि 168 एनईएफटी/आरटीजीएस/आईएमपीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 227 एनईएफटी/आरटीजीएस/आईएमपीएस भेजकर वित्तीय लेनदेन करना पसंद करते हैं जबकि 152 एनईएफटी/आरटीजीएस/आईएमपीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 वर्ष की आयु के 19 लोग एनईएफटी/आरटीजीएस/आईएमपीएस भेजकर वित्तीय लेनदेन करना पसंद करते हैं, जबकि 09 लोग एनईएफटी/आरटीजीएस/आईएमपीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	15.317ए	3	.002
संभावना अनुपात	16.125	3	.001
रैखिक-दर-रैखिक एसोसिएशन	14.889	1	.000
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को $P < 0.05$ (0.002) के रूप में खारिज कर दिया गया है। इसलिए, NEFT / RTGS / IMPS भेजने और उम्र के वित्तीय लेनदेन एक दूसरे से स्वतंत्र नहीं

हैं। ऊपर प्रस्तुत किए गए कार्ड-स्क्रायर परीक्षण के परिणाम शून्य परिकल्पना को खारिज करते हैं कि NEFT / RTGS / IMPS का उपयोग और उम्र स्वतंत्र हैं (कार्ड-स्क्रायर 15.317, df 3, $p < 0.05$)। RTGS (रियल-टाइम ग्राँस सेटलमेंट) और NEFT (राष्ट्रीय निधियों का इलेक्ट्रॉनिक हस्तांतरण) इलेक्ट्रॉनिक भुगतान प्रणाली हैं जो लोगों को बैंकों के बीच धन हस्तांतरित करने की अनुमति देते हैं। दोनों प्रणालियों का प्रबंधन भारतीय रिजर्व बैंक द्वारा किया जाता है। यह केवल देश के भीतर धन हस्तांतरण के लिए लागू है। IMPS तत्काल भुगतान सेवा के लिए उपयोग किया जाने वाला एक संक्षिप्त नाम है, इसके उपयोग से इसलिए, एनईएफटी / आरटीजीएस / आईएमपीएस जैसे वित्तीय लेनदेन का उपयोग व्यक्ति की उम्र पर निर्भर करता है।

4.13. विभिन्न आयु वर्गों में नकद जमा के वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.49 में आयु के अनुसार किए गए नकद जमा के वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. विभिन्न आयु वर्गों में नकद जमा के वित्तीय लेन-देन

			नकद जमा		कुल
			नहीं	हाँ	
	18 से 25	गिनती करना	90	227	317
		आयु के भीतर %	28.4%	71.6%	100.0%
	25 से 46	गिनती करना	259	120	379
आयु		आयु के भीतर %	68.3%	31.7%	100.0%
	46 से 60	गिनती करना	15	13	28
		आयु के भीतर %	53.6%	46.4%	100.0%
	60 से ऊपर	गिनती करना	0	2	2
		आयु के भीतर %	0.0%	100.0%	100.0%
कुल		गिनती करना	364	362	726
		आयु के भीतर %	50.1%	49.9%	100.0%

तालिका 4.49 से शुरू करते हुए, सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 317 18-25 आयु वर्ग के बीच के थे, 379 25-46 आयु वर्ग के बीच के थे, 28 46-60 आयु वर्ग के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 आयु वर्ग के बीच के लोगों में से 227 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं जबकि 90 नकद जमा के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 120 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं जबकि 259 नकद जमा के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 आयु वर्ग के लोगों

में से 13 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं जबकि 15 नकद जमा के वित्तीय लेनदेन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2- पक्षीय)
पियर्सन काई-स्क्वायर	112.325ए	3	.000
संभावना अनुपात	116.303	3	.000
रैखिक-दर-रैखिक एसोसिएशन	76.362	1	.000
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार करते हैं, कि नकद जमा का उपयोग और आयु स्वतंत्र हैं (काई-स्क्वायर 112.325, df 3, $p < 0.05$)। इसलिए, नकद जमा जैसे वित्तीय लेनदेन का उपयोग व्यक्ति की आयु पर निर्भर करता है। किसी भी आयु वर्ग के व्यक्ति द्वारा नकद जमा किया जा सकता है। इसलिए, नकद जमा जैसे वित्तीय लेनदेन का उपयोग व्यक्ति की आयु पर निर्भर नहीं करता है।

4.14. विभिन्न आयु वर्गों में नकद निकासी के वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। ऊपर दी गई तालिका 4.51 में आयु के अनुसार किए गए नकद निकासी के वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. **आयु के अनुसार नकद निकासी के वित्तीय लेनदेन**

			नकद निकासी		कुल
			नहीं	हाँ	
आयु	18 से 25	गिनती करना	145	172	317
		आयु के भीतर %	45.7%	54.3%	100.0%
	25 से 46	गिनती करना	182	197	379
		आयु के भीतर %	48.0%	52.0%	100.0%
	46 से 60	गिनती करना	14	14	28
		आयु के भीतर %	50.0%	50.0%	100.0%
	60 से ऊपर	गिनती करना	0	2	2
		आयु के भीतर %	0.0%	100.0%	100.0%
कुल		गिनती करना	341	385	726
		आयु के भीतर %	47.0%	53.0%	100.0%

उपरोक्त तालिका 4.51 आयु के आधार पर किए गए नकद निकासी के वित्तीय लेन-देन को दर्शाती है। उपरोक्त तालिका 4.53 से, 317 उत्तरदाता 18-25 आयु वर्ग के बीच के थे, 379 25-46 आयु वर्ग के बीच के थे, 28 46-60 आयु वर्ग के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 आयु वर्ग के बीच के लोगों में से 172 नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं जबकि 145 नकद जमा के वित्तीय लेन-देन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 197 नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं जबकि 182 नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करते हैं। 46 से 60 आयु वर्ग के लोगों में से 14 नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	2.235ए	3	.525
संभावना अनुपात	3.001	3	.392
रैखिक-दर-रैखिक एसोसिएशन	.136	1	.712
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि नकद निकासी का उपयोग और आयु स्वतंत्र नहीं हैं (काई-स्क्वायर 0.444, df 1, $p > 0.05$)। इस प्रकार, नकद निकासी जैसे वित्तीय लेन-देन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है। किसी भी आयु वर्ग के किसी भी व्यक्ति द्वारा नकद निकाला जा सकता है, भले ही वह व्यक्ति परिवार का कमाने वाला सदस्य हो या आश्रित सदस्य। इसलिए, नकद निकासी जैसे वित्तीय लेन-देन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.15. एक खाते से दूसरे खाते में विभिन्न अवधियों में धन हस्तांतरण के वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.53 विभिन्न आयु समूहों में एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **विभिन्न आयु वर्गों में एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन**

			एक खाते से दूसरे खाते में धन का स्थानांतरण	कुल
			नहीं	हाँ

	18 से 25	गिनती करना	147	170	317
		आयु के भीतर %	46.4%	53.6%	100.0%
	25 से 46	गिनती करना	146	233	379
आयु		आयु के भीतर %	38.5%	61.5%	100.0%
	46 से 60	गिनती करना	7	21	28
		आयु के भीतर %	25.0%	75.0%	100.0%
	60 से ऊपर	गिनती करना	0	2	2
		आयु के भीतर %	0.0%	100.0%	100.0%
कुल		गिनती करना	300	426	726
		आयु के भीतर %	41.3%	58.7%	100.0%

18 से 25 आयु वर्ग के लोगों में से 170 एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 147 एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 233 एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 146 एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 आयु वर्ग के लोगों में से 21 एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 07 एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	9.044ए	3	.029
संभावना अनुपात	9.940	3	.019
रैखिक-दर-रैखिक एसोसिएशन	8.442	1	.004
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को बिल्कुल भी खारिज नहीं करते हैं कि एक खाते से दूसरे खाते में धन हस्तांतरण का उपयोग और आयु स्वतंत्र नहीं हैं (काई-स्क्वायर 9.044, df 3, $p > 0.05$)। इस प्रकार, एक खाते से दूसरे खाते में धन

हस्तांतरण जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है। किसी भी आयु वर्ग के किसी भी व्यक्ति द्वारा धन हस्तांतरित किया जा सकता है, भले ही वह व्यक्ति विजेता सदस्य हो या आश्रित परिवार का सदस्य। इसलिए, एक खाते से दूसरे खाते में धन हस्तांतरण जैसे मौद्रिक लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.16. विभिन्न आयु वर्गों में धन प्रेषण के वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु वर्ग के 726 उत्तरदाताओं से आंकड़े एकत्र किये गए।

तालिका 4. आयु के आधार पर धन प्रेषण के वित्तीय लेनदेन

			प्रेषण		कुल
			नहीं	हाँ	
	18 से 25	गिनती करना	290	27	317
		आयु के भीतर %	91.5%	8.5%	100.0%
आयु	25 से 46	गिनती करना	345	34	379
		आयु के भीतर %	91.0%	9.0%	100.0%
	46 से 60	गिनती करना	27	1	28
		आयु के भीतर %	96.4%	3.6%	100.0%
	60 से ऊपर	गिनती करना	2	0	2
		आयु के भीतर %	100.0%	0.0%	100.0%
कुल		गिनती करना	664	62	726
		आयु के भीतर %	91.5%	8.5%	100.0%

उपरोक्त तालिका 4.55 आयु के आधार पर किए गए धन प्रेषण के वित्तीय लेनदेन को दर्शाती है। तालिका 4.55 के आंकड़ों से यह देखा जा सकता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18-25 आयु वर्ग के बीच के थे, 379 25-46 आयु वर्ग के बीच के थे, 28 46-60 आयु वर्ग के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 आयु वर्ग के बीच के लोगों में से 27 धन प्रेषण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 290 धन प्रेषण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 34 धन प्रेषण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 345 धन प्रेषण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 आयु वर्ग के लोगों में से 01 धन प्रेषण के वित्तीय लेनदेन करना पसंद करते हैं

तालिका 4. काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	1.162ए	3	.762

संभावना अनुपात	1.559	3	.669
रैखिक-दर-रैखिक एसोसिएशन	.146	1	.702
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए कार्ई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि धन प्रेषण का उपयोग और आयु स्वतंत्र नहीं हैं (कार्ई-स्क्वायर 1.162, df 3, $p > 0.05$)। इस प्रकार, धन प्रेषण जैसे वित्तीय लेन-देन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है। धन प्रेषण धन का एक हस्तांतरण है, जो अक्सर किसी विदेशी कर्मचारी द्वारा अपने मूल देश में किसी व्यक्ति को किया जाता है। इसलिए, धन प्रेषण जैसे वित्तीय लेन-देन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.17. विभिन्न आयु वर्गों में विदेशी मुद्रा के वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.57 विभिन्न आयु समूहों में विदेशी मुद्रा के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. आयु के आधार पर विदेशी मुद्रा के वित्तीय लेनदेन

			विदेशी मुद्रा		कुल
			नहीं	हाँ	
आयु	18 से 25	गिनती करना	301	16	317
		आयु के भीतर %	95.0%	5.0%	100.0%
	25 से 46	गिनती करना	340	39	379
		आयु के भीतर %	89.7%	10.3%	100.0%
	46 से 60	गिनती करना	27	1	28
		आयु के भीतर %	96.4%	3.6%	100.0%
	60 से ऊपर	गिनती करना	2	0	2
		आयु के भीतर %	100.0%	0.0%	100.0%
	कुल	गिनती करना	670	56	726
		आयु के भीतर %	92.3%	7.7%	100.0%

उपरोक्त तालिका 4.57 आयु के आधार पर किए गए विदेशी मुद्रा के वित्तीय लेनदेन को दर्शाती है। तालिका 4.57 के आंकड़ों से यह देखा जा सकता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18-25 आयु वर्ग के बीच के थे, 379 25-46 आयु वर्ग के बीच के थे, 28 46-60 आयु वर्ग के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 आयु वर्ग के बीच के लोगों में से 16 विदेशी मुद्रा के वित्तीय लेनदेन करना पसंद करते हैं जबकि 301 विदेशी मुद्रा के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 39 विदेशी मुद्रा

के वित्तीय लेनदेन करना पसंद करते हैं जबकि 340 विदेशी मुद्रा के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 आयु वर्ग के लोगों में से 01 विदेशी मुद्रा के वित्तीय लेनदेन करना पसंद करते हैं

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	7.543ए	3	.056
संभावना अनुपात	7.951	3	.047
रैखिक-दर-रैखिक एसोसिएशन	2.837	1	.092
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि फॉरेक्स का उपयोग और आयु स्वतंत्र नहीं हैं (काई-स्क्वायर 7.543, डीएफ 3, पी > 0.05)। इस प्रकार, फॉरेक्स जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है। मुद्रा (फॉरेक्स) मुद्रा बाजार को संदर्भित करता है। फॉरेक्स एक ऑफ-एक्सचेंज बाजार से ज्यादा कुछ नहीं है जिसमें दुनिया की विदेशी मुद्राओं का कारोबार होता है। यह दुनिया के सबसे बड़े और सबसे अधिक तरल बाजारों में से एक है। इसलिए, फॉरेक्स जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.18. विभिन्न आयु वर्गों की प्रतिभूतियों का वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.59 विभिन्न आयु समूहों में प्रतिभूतियों के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **विभिन्न आयु वर्गों में प्रतिभूतियों के वित्तीय लेनदेन**

		गिनती करना	300	17	317
		आयु के भीतर %	94.6%	5.4%	100.0%
आयु	18 से 25	गिनती करना	339	40	379
		आयु के भीतर %	89.4%	10.6%	100.0%
	25 से 46	गिनती करना	27	1	28
		आयु के भीतर %	96.4%	3.6%	100.0%
	46 से 60	गिनती करना	2	0	2
		आयु के भीतर %	100.0%	0.0%	100.0%
	60 से ऊपर	गिनती करना	668	58	726
		आयु के भीतर %	92.0%	8.0%	100.0%

उपरोक्त तालिका 4.61 आयु के आधार पर किए गए प्रतिभूतियों के वित्तीय लेनदेन को दर्शाती है। तालिका 4.59 के आंकड़ों से यह देखा जा सकता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18-25 आयु वर्ग के बीच के थे, 379 25-46 आयु वर्ग के बीच के थे, 28 46-60 आयु वर्ग के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 आयु वर्ग के बीच के लोगों में से 17 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद करते हैं जबकि 300 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 40 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद करते हैं जबकि 339 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 आयु वर्ग के लोगों में से 01 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद करते हैं

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	7.284ए	3	.063
संभावना अनुपात	7.695	3	.053
रैखिक-दर-रैखिक एसोसिएशन	2.581	1	.108
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि प्रतिभूतियों का उपयोग और आयु स्वतंत्र नहीं हैं (काई-स्क्वायर 7.284, df 3, $p > 0.05$)। इस प्रकार, प्रतिभूतियों जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है। प्रतिभूतियाँ किसी कंपनी या सरकार द्वारा जारी किए जाने वाले परक्राम्य वित्तीय साधन हैं जो किसी विकल्प के लिए स्वामित्व अधिकार, ऋण अधिकार या खरीद, बिक्री या विनिमय अधिकार प्रदान करते हैं। इसलिए, प्रतिभूतियों के रूप में वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर करता है।

4.19. शिक्षा क्षेत्र में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शिक्षा के स्तर के आधार पर डेटा एकत्र किया गया। नीचे दी गई तालिका 4.61 शिक्षा के क्षेत्र में किए गए NEFT/RTGS भेजने के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. शिक्षा जगत में एनईएफटी/आरटीजीएस/आईएमपीएस भेजने के वित्तीय लेनदेन

			एनईएफटी/आरटीजीएस भेजना		कुल
			नहीं	हाँ	
शिक्षा	तकएचएससी	गिनती करना	31	22	53
		शिक्षा के क्षेत्र में %	58.5%	41.5%	100.0%
	डिप्लोमा	गिनती करना	6	0	6
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	स्नातक	गिनती करना	147	130	277
		शिक्षा के क्षेत्र में %	53.1%	46.9%	100.0%
	स्नातकोत्तर	गिनती करना	131	231	362
		शिक्षा के क्षेत्र में %	36.2%	63.8%	100.0%
	पीएच.डी.	गिनती करना	12	0	12
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	चार्टर्ड एकाउंटेंट	गिनती करना	0	14	14
		शिक्षा के क्षेत्र में %	0.0%	100.0%	100.0%
	रिसर्च स्कॉलर	गिनती करना	2	0	2
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	कुल	गिनती करना	329	397	726
		शिक्षा के क्षेत्र में %	45.3%	54.7%	100.0%

उपरोक्त तालिका 4.61 से, 53 उत्तरदाता एचएससी तक शिक्षित थे, उनमें से 06 ने डिप्लोमा किया था, 277 स्नातक थे, 362 विभिन्न धाराओं में स्नातकोत्तर थे, 12 पीएचडी धारक थे और 14 चार्टर्ड एकाउंटेंट थे। जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी की थी, उनमें से 22 एनईएफटी / आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद करते हैं जबकि 31 एनईएफटी / आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे, उनमें से एनईएफटी / आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं

करते हैं। जिन उत्तरदाताओं ने स्नातक किया था, उनमें से 130 एनईएफटी / आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद करते हैं जबकि 147 एनईएफटी / आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने पीएचडी की है, वे एनईएफटी/आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने चार्टर्ड अकाउंटेंट के रूप में काम किया है, वे सभी एनईएफटी/आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद करते हैं। जिन उत्तरदाताओं ने शोध किया है, वे सभी एनईएफटी/आरटीजीएस भेजकर वित्तीय लेनदेन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	58.339ए	6	.000
संभावना अनुपात	71.322	6	.000
रैखिक-दर-रैखिक एसोसिएशन	16.876	1	.000
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज करते हैं कि NEFT/RTGS/IMPS का उपयोग और शिक्षा स्वतंत्र हैं (काई-स्क्वायर 58.339, df 6, $p < 0.05$)। इस प्रकार, NEFT/RTGS/IMPS जैसे वित्तीय लेन-देन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर करता है। NEFT/RTGS/IMPS के माध्यम से पैसे भेजने के लिए बुनियादी कंप्यूटर और हैंडहेल्ड डिवाइस ज्ञान की आवश्यकता होती है। इसलिए, NEFT/RTGS/IMPS जैसे वित्तीय लेन-देन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर करता है।

4.20. शिक्षा जगत में नकद जमा के वित्तीय लेनदेन:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शिक्षा के स्तर के आधार पर डेटा एकत्र किया गया। नीचे दी गई तालिका 4.63 शिक्षा के क्षेत्र में किए गए नकद जमा के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **शिक्षा जगत में नकद जमा के वित्तीय लेनदेन**

			नकद जमा		कुल
			नहीं	हाँ	
शिक्षा	तकएचएस सी	गिनती करना	22	31	53

		शिक्षा के क्षेत्र में %	41.5%	58.5%	100.0%
	डिप्लोमा	गिनती करना	0	6	6
		शिक्षा के क्षेत्र में %	0.0%	100.0%	100.0%
	स्नातक	गिनती करना	97	180	277
		शिक्षा के क्षेत्र में %	35.0%	65.0%	100.0%
	स्नातकोत्तर	गिनती करना	225	137	362
		शिक्षा के क्षेत्र में %	62.2%	37.8%	100.0%
	पीएच.डी.	गिनती करना	6	6	12
		शिक्षा के क्षेत्र में %	50.0%	50.0%	100.0%
	चार्टर्ड एकाउंटेंट	गिनती करना	12	2	14
		शिक्षा के क्षेत्र में %	85.7%	14.3%	100.0%
	रिसर्च स्कॉलर	गिनती करना	2	0	2
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
कुल		गिनती करना	364	362	726
		शिक्षा के क्षेत्र में %	50.1%	49.9%	100.0%

तालिका 4.63 से, सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 53 एचएससी तक शिक्षित थे, उनमें से 06 ने डिप्लोमा किया था, 277 स्नातक थे, 362 विभिन्न धाराओं में स्नातकोत्तर थे, 12 पीएचडी धारक थे और 14 चार्टर्ड एकाउंटेंट थे। जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी की थी, उनमें से 31 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं जबकि 22 नकद जमा के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे, उनमें से 06 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं। जिन उत्तरदाताओं ने स्नातक किया था, उनमें से 180 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं जबकि 97 नकद जमा के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातकोत्तर किया था, उनमें से 137 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं उत्तरदाताओं में से जो चार्टर्ड अकाउंटेंट थे, उनमें से 02 नकद जमा के वित्तीय लेनदेन करना पसंद करते हैं जबकि 12 नकद जमा के वित्तीय लेनदेन करना पसंद नहीं करते हैं। उत्तरदाताओं में से जो शोध विद्वान थे, वे नकद जमा के वित्तीय लेनदेन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	62.928ए	6	.000
संभावना अनुपात	67.410	6	.000
रैखिक-दर-रैखिक एसोसिएशन	34.616	1	.000
वैध मामलों की संख्या N	726		

ऊपर मौजूद काई-स्क्वायर परीक्षण इस शून्य परिकल्पना को खारिज करता है कि नकद जमा और शिक्षा का उपयोग स्वतंत्र हैं (काई-स्क्वायर 62.928, df 6, $p < 0.05$)। इस प्रकार, नकद जमा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर करता है। नकद जमा द्वारा पैसे भेजने के लिए कंप्यूटर और पोर्टेबल उपकरणों का बुनियादी ज्ञान होना आवश्यक है।

इसलिए, नकदी जमा जैसे वित्तीय लेनदेन का उपयोग व्यक्ति की शिक्षा के स्तर पर निर्भर करता है।

4.21. शिक्षा जगत में नकद निकासी के वित्तीय लेनदेन:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शिक्षा के स्तर के आधार पर डेटा एकत्र किया गया। नीचे दी गई तालिका 4.65 शिक्षा के क्षेत्र में किए गए नकद निकासी के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **शिक्षा जगत में नकद निकासी के वित्तीय लेनदेन**

			नकद निकासी		कुल	
			नहीं	हाँ		
शिक्षा	एचएससी तक	गिनती करना	24	29	53	
		शिक्षा के क्षेत्र में %	45.3%	54.7%	100.0%	
	डिप्लोमा	गिनती करना	6	0	6	
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%	
	स्नातक	गिनती करना	147	130	277	
		शिक्षा के क्षेत्र में %	53.1%	46.9%	100.0%	
	डाकस्नातक	गिनती करना	158	204	362	
		शिक्षा के क्षेत्र में %	43.6%	56.4%	100.0%	

	पीएच.डी.	गिनती करना	2	10	12	
		शिक्षा के क्षेत्र में %	16.7%	83.3%	100.0%	
	चार्टर्ड एकाउंटेंट	गिनती करना	2	12	14	
		शिक्षा के क्षेत्र में %	14.3%	85.7%	100.0%	
	अनुसंधान	गिनती करना	2	0	2	

	पंडित	शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
कुल		गिनती करना	341	385	726
		शिक्षा के क्षेत्र में %	47.0%	53.0%	100.0%

तालिका 4.65 के अनुसार, सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 53 एचएससी तक शिक्षित थे, उनमें से 06 ने डिप्लोमा किया था, 277 स्नातक थे, 362 विभिन्न धाराओं में स्नातकोत्तर थे, 12 पीएचडी धारक थे और 14 चार्टर्ड एकाउंटेंट थे। जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी की थी, उनमें से 29 नकद निकासी के वित्तीय लेनदेन करना पसंद करते हैं जबकि 24 नकद निकासी के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे, उनमें से 06 नकद निकासी के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातक किया था, उनमें से 130 नकद निकासी के वित्तीय लेनदेन करना पसंद करते हैं जबकि 147 नकद निकासी के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातकोत्तर किया था, उनमें से 204 नकद निकासी के वित्तीय लेनदेन करना पसंद करते हैं जिन उत्तरदाताओं ने पीएचडी की है, उनमें से 10 नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं जबकि 02 नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करते हैं। जो उत्तरदाता चार्टर्ड अकाउंटेंट थे, उनमें से 12 नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं जबकि 02 नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करते हैं। जो उत्तरदाता शोध छात्र थे, उनमें से नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	25.263ए	6	.000
संभावना अनुपात	29.546	6	.000
रैखिक-दर-रैखिक एसोसिएशन	5.694	1	.017
वैध मामलों की संख्या N	726		

ऊपर दिए गए कार्ई-स्कायर परीक्षण का डोमिनो प्रभाव इस शून्य परिकल्पना को खारिज करता है कि नकद निकासी और शिक्षा का उपयोग स्वतंत्र हैं (कार्ई-स्कायर 25.263, df 6, $p < 0.05$)। इस प्रकार, नकद निकासी जैसे वित्तीय लेनदेन का उपयोग व्यक्ति के शिक्षा स्तर पर निर्भर करता है। पैसे निकालने के लिए कंप्यूटर और पोर्टेबल डिवाइस का बुनियादी ज्ञान होना आवश्यक है। इसलिए, नकद निकासी जैसे वित्तीय लेनदेन का उपयोग व्यक्ति के शैक्षिक स्तर पर निर्भर करता है।

4.22. शिक्षा जगत में एक खाते से दूसरे खाते में धन हस्तांतरण का वित्तीय लेनदेन:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शिक्षा के स्तर के आधार पर डेटा एकत्र किया गया। नीचे दी गई तालिका 4.67 शिक्षा के क्षेत्र में एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. शिक्षा जगत में एक खाते से दूसरे खाते में धन हस्तांतरण के वित्तीय लेनदेन

			धन का स्थानांतरण एक खाते से दूसरे खाते में		कुल
			नहीं	हाँ	
शिक्षा	तकएचएससी	गिनती करना	26	27	53
		शिक्षा के क्षेत्र में %	49.1%	50.9%	100.0%
	डिप्लोमा	गिनती करना	6	0	6
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	स्नातक	गिनती करना	110	167	277
		शिक्षा के क्षेत्र में %	39.7%	60.3%	100.0%
	स्नातकोत्तर	गिनती करना	145	217	362
		शिक्षा के क्षेत्र में %	40.1%	59.9%	100.0%
	पीएच.डी.	गिनती करना	6	6	12
		शिक्षा के क्षेत्र में %	50.0%	50.0%	100.0%
	चार्टर्ड एकाउंटेंट	गिनती करना	7	7	14
		शिक्षा के क्षेत्र में %	50.0%	50.0%	100.0%

	रिसर्च स्कॉलर	गिनती करना	0	2	2
		शिक्षा के क्षेत्र में %	0.0%	100.0%	100.0%
कुल		गिनती करना	300	426	726
		शिक्षा के क्षेत्र में %	41.3%	58.7%	100.0%

तालिका 4.67 से यह देखा जा सकता है कि जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी कर ली थी, उनमें से 27 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद करते हैं जबकि 26 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने डिप्लोमा कोर्स किया था, उनमें से 06 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातक किया था, उनमें से 167 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद करते हैं जबकि 110 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातकोत्तर किया था, उनमें से 217 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद करते हैं जबकि 145 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने पीएचडी की थी, उनमें से 06 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद करते हैं जबकि 06 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जो उत्तरदाता चार्टर्ड अकाउंटेंट थे, उनमें से 07 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद करते हैं जबकि 07 फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जो उत्तरदाता शोध छात्र थे, उनमें से सभी एक खाते से दूसरे खाते में फंड ट्रांसफर के वित्तीय लेनदेन करना पसंद करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	12.580ए	6	.050
संभावना अनुपात	15.360	6	.018
रैखिक-दर-रैखिक एसोसिएशन	1.238	1	.266
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के निष्कर्ष शून्य परिकल्पना को खारिज नहीं करते हैं कि एक खाते से दूसरे खाते में धन हस्तांतरण का उपयोग और शिक्षा स्वतंत्र नहीं हैं (काई-स्क्वायर 12.580, df 6, $p > 0.05$)। किसी भी व्यक्ति द्वारा अपने शिक्षा स्तर की परवाह किए बिना

धन हस्तांतरित किया जा सकता है। इस प्रकार, एक खाते से दूसरे खाते में धन हस्तांतरण जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर नहीं करता है।

4.23. शिक्षा के क्षेत्र में धन प्रेषण का वित्तीय लेनदेन:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शिक्षा स्तर के आधार पर डेटा एकत्र किया गया। नीचे दी गई तालिका 4.69 शिक्षा के क्षेत्र में धन प्रेषण के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. शिक्षा क्षेत्र में धन प्रेषण के वित्तीय लेनदेन

			प्रेषण		कुल
			नहीं	हाँ	
शिक्षा	तकएचएससी	गिनती करना	48	5	53
		शिक्षा के क्षेत्र में %	90.6%	9.4%	100.0%
	डिप्लोमा	गिनती करना	6	0	6
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	स्नातक	गिनती करना	263	14	277
		शिक्षा के क्षेत्र में %	94.9%	5.1%	100.0%
	स्नातकोत्तर	गिनती करना	321	41	362
		शिक्षा के क्षेत्र में %	88.7%	11.3%	100.0%
	पीएच.डी.	गिनती करना	12	0	12
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	चार्टर्ड एकाउंटेंट	गिनती करना	12	2	14
		शिक्षा के क्षेत्र में %	5.7%	14.3%	100.0%
	रिसर्च स्कॉलर	गिनती करना	2	0	2
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	कुल	गिनती करना	664	62	726
		शिक्षा के क्षेत्र में %	91.5%	8.5%	100.0%

तालिका 4.69 से पता चलता है कि जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी कर ली थी, 05 धन प्रेषण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 48 धन प्रेषण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे, उनमें से 06 धन प्रेषण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातक किया था, उनमें

से 14 धन प्रेषण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 263 धन प्रेषण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातकोत्तर किया था, उनमें से 41 धन प्रेषण के वित्तीय लेनदेन करना पसंद करते हैं जबकि 321 धन प्रेषण के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने पीएचडी की थी, उनमें से सभी 12 धन प्रेषण के वित्तीय लेनदेन करना पसंद नहीं करते हैं।

तालिका 4. स्कायर परीक्षण के ग्रेड शून्य

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन कार्ई-स्कायर	10.420ए	6	.108
संभावना अनुपात	12.403	6	.054
रैखिक-दर-रैखिक एसोसिएशन	1.735	1	.188
वैध मामलों की संख्या N	726		

ऊपर दिए गए कार्ई-स्कायर परीक्षण के ग्रेड शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि धन प्रेषण और शिक्षा का उपयोग स्वतंत्र नहीं हैं (कार्ई-स्कायर 1.162, df 3, $p > 0.05$)। इस प्रकार, धन प्रेषण जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर नहीं करता है। धन प्रेषण नकदी का हस्तांतरण हो सकता है, जो अक्सर दूर के कर्मचारी द्वारा अपने मूल देश में किसी व्यक्ति को किया जाता है। इसलिए, धन प्रेषण जैसे मौद्रिक लेनदेन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर नहीं करता है।

4.24. शिक्षा के क्षेत्र में विदेशी मुद्रा का वित्तीय लेनदेन:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शिक्षा के स्तर के आधार पर डेटा एकत्र किया गया। नीचे दी गई तालिका 4.71 शिक्षा के स्तर पर विदेशी मुद्रा के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. शिक्षा जगत में विदेशी मुद्रा के वित्तीय लेनदेन

			विदेशी मुद्रा		कुल
			नहीं	हाँ	
शिक्षा	तकएचएससी	गिनती करना	51	2	53
		शिक्षा के क्षेत्र में %	96.2%	3.8%	100.0%
	डिप्लोमा	गिनती करना	6	0	6
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	स्नातक	गिनती करना	267	10	277

		शिक्षा के क्षेत्र में %	96.4%	3.6%	100.0%
	स्नातकोत्तर	गिनती करना	321	41	362
		शिक्षा के क्षेत्र में %	88.7%	11.3%	100.0%
	पीएच.डी.	गिनती करना	12	0	12
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
	चार्टर्ड एकाउंटेंट	गिनती करना	11	3	14
		शिक्षा के क्षेत्र में %	78.6%	21.4%	100.0%
	रिसर्च स्कॉलर	गिनती करना	2	0	2
		शिक्षा के क्षेत्र में %	100.0%	0.0%	100.0%
कुल		गिनती करना	670	56	726
		शिक्षा के क्षेत्र में %	92.3%	7.7%	100.0%

तालिका से यह देखा जा सकता है कि जिन उत्तरदाताओं ने एचएससी तक की शिक्षा पूरी कर ली है, उनमें से 02 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद करते हैं जबकि 51 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किया है, उनमें से 06 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातक किया है, उनमें से 10 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद करते हैं जबकि 267 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातकोत्तर किया है, उनमें से 41 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद करते हैं जबकि 321 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने पीएचडी की है, उनमें से सभी 12 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद नहीं करते हैं। जो उत्तरदाता चार्टर्ड एकाउंटेंट थे, उनमें से 03 विदेशी मुद्रा का वित्तीय लेनदेन करना पसंद करते हैं

तालिका 4. स्कायर परीक्षण का डोमिनो प्रभाव

	कीमत	डीएफ	असिम्प. सिग. (2-पक्षीय)
पियर्सन कार्ई-स्कायर	19.715ए	6	.003
संभावना अनुपात	21.115	6	.002
रैखिक-दर-रैखिक एसोसिएशन	9.653	1	.002
वैध मामलों की संख्या N	726		

ऊपर प्राप्त किए जा सकने वाले कार्ई-स्कायर परीक्षण का डोमिनो प्रभाव शून्य परिकल्पना को खारिज करता है कि विदेशी मुद्रा और शिक्षा का उपयोग स्वतंत्र हैं (कार्ई-स्कायर 19.715, डीएफ 6, पी > 0.05)। इस प्रकार, विदेशी मुद्रा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर करता है। मुद्रा (फॉरेक्स) मुद्रा बाजार को संदर्भित करता है। फॉरेक्स एक ऑफ-एक्सचेंज बाजार से ज्यादा कुछ नहीं है जिसमें दुनिया की विदेशी मुद्राओं का कारोबार होता है। यह दुनिया के सबसे बड़े और सबसे अधिक तरल बाजारों में से एक है। इसलिए, फॉरेक्स जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर नहीं करता है।

4.25. शिक्षा जगत में प्रतिभूतियों का वित्तीय लेनदेन:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शिक्षा स्तर के आधार पर डेटा एकत्र किया गया। नीचे दी गई तालिका 4.73 शिक्षा के क्षेत्र में प्रतिभूतियों के वित्तीय लेन-देन को दर्शाती है।

तालिका 4. शिक्षा जगत में प्रतिभूतियों के वित्तीय लेनदेन

			प्रतिभूति		कुल
			नहीं	हाँ	
शिक्षा	तकएचएससी	गिनती करना	51	2	53
		शिक्षा के क्षेत्र में %	96.20%	3.80%	100.00%
	डिप्लोमा	गिनती करना	6	0	6
		शिक्षा के क्षेत्र में %	100.00%	0.00%	100.00%
	स्नातक	गिनती करना	269	8	277
		शिक्षा के क्षेत्र में %	97.10%	2.90%	100.00%
	स्नातकोत्तर	गिनती करना	314	48	362
		शिक्षा के क्षेत्र में %	86.70%	13.30%	100.00%
	पीएच.डी.	गिनती करना	12	0	12
		शिक्षा के क्षेत्र में %	100.00%	0.00%	100.00%
	चार्टर्ड एकाउंटेंट	गिनती करना	14	0	14
		शिक्षा के क्षेत्र में %	100.00%	0.00%	100.00%
	रिसर्च स्कॉलर	गिनती करना	2	0	2
		शिक्षा के क्षेत्र में %	100.00%	0.00%	100.00%
कुल	गिनती करना	गिनती करना	668	58	726
	शिक्षा के क्षेत्र में %	शिक्षा के क्षेत्र में %	92.00%	8.00%	100.00%

तालिका 4.73 से पता चलता है कि जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी कर ली है, उनमें से 02 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद करते हैं जबकि 51 प्रतिभूतियों के

वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किया है, उनमें से 06 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातक किया है, उनमें से 08 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद करते हैं जबकि 269 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने स्नातकोत्तर किया है, उनमें से 48 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद करते हैं जबकि 314 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जिन उत्तरदाताओं ने पीएचडी की है, उनमें से सभी 12 प्रतिभूतियों के वित्तीय लेनदेन करना पसंद नहीं करते हैं। जो उत्तरदाता चार्टर्ड एकाउंटेंट थे उनमें से कोई भी प्रतिभूतियों का वित्तीय लेनदेन करना पसंद नहीं करता है

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	27.719ए	6	.000
संभावना अनुपात	31.574	6	.000
रैखिक-दर-रैखिक एसोसिएशन	6.951	1	.008
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को खारिज करते हैं कि प्रतिभूतियों का उपयोग और शिक्षा स्वतंत्र हैं (काई-स्क्वायर 19.715, df 6, $p > 0.05$)। इस प्रकार, प्रतिभूतियों जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के शिक्षा स्तर पर निर्भर करता है। मुद्रा (प्रतिभूतियाँ) मुद्रा बाजार को संदर्भित करती है। प्रतिभूतियाँ कुछ और नहीं बल्कि एक ऑफ-एक्सचेंज बाजार हैं जिसके दौरान ग्रह की विदेशी मुद्राओं का कारोबार होता है। यह दुनिया के सबसे महत्वपूर्ण और सबसे अधिक तरल बाजारों में से एक है। इसलिए, प्रतिभूतियों जैसे मौद्रिक लेनदेन का उपयोग किसी निजी व्यक्ति के शिक्षा स्तर पर निर्भर नहीं करता है।

4.26. विभिन्न लिंगों के ग्राहकों के विवरण जैसे मोबाइल नंबर, पता आदि को अद्यतन करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.75 में लिंग के आधार पर ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि अपडेट करने के गैर-वित्तीय लेन-देन दिखाए गए हैं।

तालिका 4. **लिंग के आधार पर ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को अद्यतन करने के गैर-वित्तीय लेनदेन**

			ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि अपडेट करना		कुल	
			नहीं	हाँ		
	पुरुष	गिनती करना	164	268	432	
लिंग		लिंग के भीतर %	38	62	100	
	महिला	गिनती करना	111	183	294	
		लिंग के भीतर %	38	62	100	
कुल		गिनती करना	275	451	726	

तालिका 4.75 से पता चलता है कि 432 उत्तरदाता पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 268 पुरुष मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 164 पुरुष ऑनलाइन मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 183 महिलाएँ मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करती हैं। जबकि 111 महिलाएँ ऑनलाइन मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करती हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)
पियर्सन काई-स्क्वायर	.003ए	1	1		
निरंतरता सुधार	0	1	1		
संभावना अनुपात	0	1	1		
फिशर का सटीक परीक्षण				1	0.5
रैखिक-दर-रैखिक एसोसिएशन	0	1	1		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने के गैर-वित्तीय लेनदेन का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 0.003, डीएफ 1, $P > 0.05$)। इस प्रकार,

मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण ऑनलाइन अपडेट करने के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.27. विभिन्न लिंगों के खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.77 लिंग के आधार पर खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. लिंग के आधार पर खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन

			खाता खोलना और खाता बंद करना		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	273	159	432
लिंग		लिंग के भीतर %	63.2%	36.8%	100.0%
	महिला	गिनती करना	199	95	294
		लिंग के भीतर %	67.7%	32.3%	100.0%
कुल		गिनती करना	472	254	726
		लिंग के भीतर %	65.0%	35.0%	100.0%

तालिका 4.77 से पता चलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 159 पुरुष खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन करना पसंद करते हैं जबकि 273 पुरुष खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 95 महिलाएँ खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन करना पसंद करती हैं जबकि 199 महिलाएँ खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करती हैं।

तालिका 4. काई-स्क्वायर परीक्षण

			असि. सि. ग. (2-	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)	
	कीमत	डीएफ				

			पक्षी य)			
पियर्सन कार्ई-स्कायर	1.552ए	1	.21 3			
निरंतरता सुधार	1.361	1	.24 3			
संभावना अनुपात	1.559	1	.21 2			
फिशर का सटीक परीक्षण				.235	.122	
रैखिक-दर-रैखिक एसोसिएशन	1.550	1	.21 3			
वैध मामलों की संख्या N	726					

ऊपर प्रस्तुत किए गए कार्ई-स्कायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन का उपयोग और लिंग स्वतंत्र नहीं हैं (कार्ई-स्कायर 1.552, df 1, $p > 0.05$)। इस प्रकार, ऑनलाइन खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.28. विभिन्न लिंगों में शेष राशि की जांच के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.79 लिंग के आधार पर शेष राशि की जांच के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. लिंग के आधार पर शेष राशि की जांच के गैर-वित्तीय लेनदेन

			तुला राशि जाँच		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	123	309	432
लिंग		लिंग के भीतर %	28.5%	71.5%	100.0%
	महिला	गिनती करना	96	198	294
		लिंग के भीतर %	32.7%	67.3%	100.0%
कुल		गिनती करना	219	507	726
		लिंग के भीतर %	30.2%	69.8%	100.0%

तालिका 4.79 से पता चलता है कि सर्वेक्षण में 726 उत्तरदाताओं को शामिल किया गया, जिनमें 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 309 पुरुष बैलेंस इंकायरी के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 123 पुरुष बैलेंस इंकायरी के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 198 महिलाएँ बैलेंस इंकायरी के गैर-वित्तीय लेनदेन करना पसंद करती हैं जबकि 96 महिलाएँ बैलेंस इंकायरी के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करती हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प. सिग.	सटीक हस्ताक्षर.	सटीक हस्ताक्षर.
			(दो तरफा)	(दो तरफा)	(एक तरफा)
पियर्सन काई-स्क्वायर	1.452ए	1	.228		
निरंतरता सुधार	1.260	1	.262		
संभावना अनुपात	1.445	1	.229		
फिशर का सटीक परीक्षण				.249	.131
रैखिक-दर-रैखिक एसोसिएशन	1.450	1	.229		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि बैलेंस पूछताछ के गैर-वित्तीय लेनदेन का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 1.452, df 1, $p > 0.05$)। इस प्रकार, ऑनलाइन बैलेंस पूछताछ के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.29. विभिन्न लिंगों के बीच खाता विवरण मुद्रित करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.81 लिंग के आधार पर खाता विवरण मुद्रित करने के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **लिंग के आधार पर खाता विवरण मुद्रित करने के गैर-वित्तीय लेन-देन**

			खाता विवरण प्रिंट करना		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	284	148	432
लिंग		लिंग के भीतर %	65.7%	34.3%	100.0%

	महिला	गिनती करना	186	108	294
		लिंग के भीतर %	63.3%	36.7%	100.0%
कुल		गिनती करना	470	256	726
		लिंग के भीतर %	64.7%	35.3%	100.0%

ऊपर दी गई तालिका 4.81 से यह देखा जा सकता है कि सर्वेक्षण में शामिल कुल 726 आरोपियों में से 432 पुरुष थे जबकि 294 महिलाएं थीं। इन 432 पुरुषों में से 148 पुरुष खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 284 पुरुष ऑनलाइन खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 108 महिलाएं खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करती हैं जबकि 186 महिलाएं ऑनलाइन खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करती हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)	सटीक हस्ताक्षर.(दो तरफा)	सटीक हस्ताक्षर.(दो तरफा)
पियर्सन काई-स्क्वायर	.470ए	1	.493		
निरंतरता सुधार	.367	1	.544		
संभावना अनुपात	.469	1	.494		
फिशर का सटीक परीक्षण				.527	.272
रैखिक-दर-रैखिक एसोसिएशन	.469	1	.493		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि खाता विवरण प्रिंट करने के गैर-वित्तीय लेनदेन का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 0.470, df 1, $p > 0.05$)। इस प्रकार, खाता विवरण ऑनलाइन प्रिंट करने के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.30. विभिन्न लिंगों के बीच चेक बुक/पासबुक जारी करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.83 लिंग के आधार पर चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. विभिन्न लिंगों के बीच चेक बुक/पासबुक जारी करने के गैर-वित्तीय लेनदेन

			चेक बुक/पास बुक जारी करना		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	304	128	432
लिंग		लिंग के भीतर %	70.4%	29.6%	100.0%
	महिला	गिनती करना	191	103	294
		लिंग के भीतर %	65.0%	35.0%	100.0%
कुल		गिनती करना	495	231	726
		लिंग के भीतर %	68.2%	31.8%	100.0%

तालिका 4.83 से प्राप्त आंकड़ों से यह देखा जा सकता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएं थीं। इन 432 पुरुषों में से 128 पुरुष चेक बुक/पास बुक जारी करने का गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 304 पुरुष चेक बुक/पास बुक जारी करने का गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं। इसी प्रकार, इन 294 महिलाओं में से 103 महिलाएं चेक बुक/पास बुक जारी करने का गैर-वित्तीय लेनदेन करना पसंद करती हैं जबकि 191 महिलाएं चेक बुक/पास बुक जारी करने का गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करती हैं। एक साथ एकीकृत करने पर 231 उत्तरदाता चेक बुक/पास बुक जारी करने का गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 495 उत्तरदाता चेक बुक/पास बुक जारी करने का गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं।

तालिका 4. कार्ड-स्कायर परीक्षण

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)
पियर्सन कार्ड-स्कायर	2.355ए	1	.125		
निरंतरता सुधार	2.113	1	.146		
संभावना अनुपात	2.344	1	.126		
फिशर का सटीक परीक्षण				.144	.073
रैखिक-दर-रैखिक एसोसिएशन	2.352	1	.125		

वैध मामलों की संख्या N	726				
------------------------	-----	--	--	--	--

ऊपर प्रस्तुत किए गए कार्ड-स्कायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन का उपयोग और लिंग स्वतंत्र नहीं हैं (कार्ड-स्कायर 2.355, df 1, $p > 0.05$)। इस प्रकार, चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन का उपयोग ऑनलाइन किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.31. विभिन्न लिंगों के बीच केवाईसी अद्यतन के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.85 लिंग के आधार पर केवाईसी अपडेट के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. लिंग के आधार पर केवाईसी अपडेट

क्रमांक	लिंग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	पुरुष	240	192	432	55.6%	44.4%
2	महिला	167	127	294	56.8%	43.2%
	कुल	407	319	726	56.1%	43.9%

तालिका 4.85 ओवरहेड दर्शाती है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 192 पुरुष KYC अपडेट के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 240 पुरुष KYC अपडेट के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 127 महिलाएँ KYC अपडेट के गैर-वित्तीय लेनदेन करना पसंद करती हैं जबकि 167 महिलाएँ KYC अपडेट के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करती हैं। एक साथ एकीकृत करने पर 319 उत्तरदाता KYC अपडेट के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 407 उत्तरदाता KYC अपडेट के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

			असिम्ट. सिग (दो तरफा)	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)
पियर्सन काई-स्क्वायर	.110ए	1	.740		
निरंतरता सुधार	.066	1	.798		
संभावना अनुपात	.111	1	.740		
फिशर का सटीक परीक्षण				.761	.399
रैखिक-दर-रैखिक एसोसिएशन	.110	1	.740		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि केवाईसी अपडेट के गैर-वित्तीय लेनदेन का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्क्वायर 0.110, डीएफ 1, पी > 0.05)। इस प्रकार, ऑनलाइन केवाईसी अपडेट के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.32. आयु के आधार पर ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को अद्यतन करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए अलग-अलग आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.87 में लिंग के आधार पर ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को अपडेट करने के गैर-वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. **लिंग के आधार पर ग्राहक विवरण**

क्रमांक	आयु वर्ग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	18 से 25 वर्ष	102	215	317	32.2%	67.8%
2	25 से 46 वर्ष	169	210	379	44.6%	55.4%
3	46 से 60 वर्ष	4	24	28	14.3%	85.7%
4	60 वर्ष से ऊपर	0	2	2	0.0%	100.0%
	कुल	275	451	726	37.9%	62.1%

सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18 से 25 वर्ष की आयु के थे, 379 25 से 46 वर्ष की आयु के थे, 28 46-60 वर्ष की आयु के थे तथा 2 60 वर्ष से अधिक आयु के थे। 18 से 25 वर्ष की आयु के लोगों में से 215 लोग मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 102 लोग मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 वर्ष की आयु के लोगों में से 210 लोग मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 169 लोग मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 वर्ष की आयु के लोगों में से 24 लोग मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 04 लोग मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। एक साथ एकीकृत करने पर 451 उत्तरदाता ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 275 उत्तरदाता ग्राहक विवरण जैसे मोबाइल नंबर, पता आदि को ऑनलाइन अपडेट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	19.480 ^a	3	.000
संभावना अनुपात	21.152	3	.000
रैखिक-दर-रैखिक एसोसिएशन	1.744	1	.187
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज करते हैं कि मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण अपडेट करने के गैर-वित्तीय लेनदेन का उपयोग और आयु स्वतंत्र हैं (काई-स्क्वायर 19.480, df 3, $p < 0.05$)। इस प्रकार, मोबाइल नंबर, पता आदि जैसे ग्राहक विवरण ऑनलाइन अपडेट करने के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर करता है।

4.33. विभिन्न आयु वर्ग में खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए अलग-अलग आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.89 में आयु के आधार पर खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. आयु के आधार पर खाता खोलने और खाता बंद करने के गैर-वित्तीय लेन-देन

			खाता खोलना और खाता बंद करना		कुल
			नहीं	हाँ	
	18 से 25	गिनती करना	181	136	317
		आयु के भीतर %	57.1%	42.9%	100.0%
	25 से 46	गिनती करना	272	107	379
आयु		आयु के भीतर %	71.8%	28.2%	100.0%
	46 से 60	गिनती करना	18	10	28
		आयु के भीतर %	64.3%	35.7%	100.0%
	60 से ऊपर	गिनती करना	1	1	2
		आयु के भीतर %	50.0%	50.0%	100.0%
कुल		गिनती करना	472	254	726
		आयु के भीतर %	65.0%	35.0%	100.0%

तालिका 4.89 में, सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 317 18 से 25 आयु वर्ग के बीच के थे, 379 25 से 46 आयु वर्ग के बीच के थे, 28 46-60 आयु वर्ग के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 आयु वर्ग के बीच के लोगों में से 136 खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 181 खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 आयु वर्ग के लोगों में से 107 खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 272 खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 60 वर्ष से अधिक आयु वर्ग के 01 लोग खाता खोलने और खाता बंद करने जैसे गैर-वित्तीय लेन-देन करना पसंद करते हैं, जबकि 01 लोग खाता खोलने और खाता बंद करने जैसे गैर-वित्तीय लेन-देन करना पसंद नहीं करते हैं। एक साथ मिलाने पर 254 उत्तरदाता खाता खोलने और खाता बंद करने जैसे गैर-वित्तीय लेन-देन करना पसंद करते हैं, जबकि 472 उत्तरदाता खाता खोलने और खाता बंद करने जैसे गैर-वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	16.539ए	3	.001
संभावना अनुपात	16.541	3	.001
रैखिक-दर-रैखिक एसोसिएशन	10.742	1	.001
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज करते हैं कि खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन का उपयोग और आयु स्वतंत्र हैं (काई-स्क्वायर 16.539, df 3, $p < 0.05$)। इस प्रकार, ऑनलाइन खाता खोलने और खाता बंद करने के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर करता है।

4.34. विभिन्न आयु वर्गों में शेष राशि की जांच के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.91 आयु के अनुसार बैलेंस इंकायरी के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **आयु के अनुसार बैलेंस इंकायरी के गैर-वित्तीय**

			तुला राशि जाँच		कुल
			नहीं	हाँ	
	18 से 25	गिनती करना	82	235	317
		आयु के भीतर %	25.9%	74.1%	100.0%
	25 से 46	गिनती करना	128	251	379
आयु		आयु के भीतर %	33.8%	66.2%	100.0%
	46 से 60	गिनती करना	8	20	28
		आयु के भीतर %	28.6%	71.4%	100.0%
	60 से ऊपर	गिनती करना	1	1	2
		आयु के भीतर %	50.0%	50.0%	100.0%
कुल		गिनती करना	219	507	726
		आयु के भीतर %	30.2%	69.8%	100.0%

तालिका 4.91 से यह निष्कर्ष निकलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18 से 25 वर्ष की आयु के बीच के थे, 379 25 से 46 वर्ष की आयु के बीच के थे, 28 46-60 वर्ष की आयु के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 वर्ष की आयु के बीच के लोगों में से 235 बैलेंस पूछताछ के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 82 बैलेंस

पूछताछ के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 वर्ष की आयु के लोगों में से 251 बैलेंस पूछताछ के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 128 बैलेंस पूछताछ के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 वर्ष की आयु के लोगों में से 20 बैलेंस पूछताछ के गैर-वित्तीय लेनदेन करना पसंद करते हैं 60 वर्ष से अधिक आयु वर्ग के 01 लोग बैलेंस इंकायरी के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 01 लोग बैलेंस इंकायरी के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। एक साथ मिलाने पर 507 उत्तरदाता बैलेंस इंकायरी के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 219 उत्तरदाता बैलेंस इंकायरी के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	5.529ए	3	.137
संभावना अनुपात	5.531	3	.137
रैखिक-दर-रैखिक एसोसिएशन	3.838	1	.050
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण का अंतिम उत्पाद शून्य परिकल्पना को अस्वीकार नहीं करता है कि बैलेंस पूछताछ के गैर-वित्तीय लेनदेन का उपयोग और आयु स्वतंत्र हैं (काई-स्क्वायर 5.529, df 3, $p > 0.05$)। इस प्रकार, ऑनलाइन बैलेंस पूछताछ के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.35 विभिन्न आयु वर्गों में खाता विवरण मुद्रित करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए अलग-अलग आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.93 में आयु के आधार पर खाता विवरण मुद्रित करने के गैर-वित्तीय लेन-देन को दर्शाया गया है।

तालिका 4. **आयु के आधार पर खाता विवरण मुद्रित करने के गैर-वित्तीय लेन-देन**

			खाता विवरण प्रिंट करना		कुल
			नहीं	हाँ	
		गिनती करना	201	116	317
	18 से 25	आयु के भीतर %	63.40%	36.60%	100.00%
		गिनती करना	247	132	379
आयु	25 से 46	आयु के भीतर %	65.20%	34.80%	100.00%

		गिनती करना	21	7	28
	46 से 60	आयु के भीतर %	75.00%	25.00%	100.00%
	60 से ऊपर	गिनती करना	1	1	2
		आयु के भीतर %	50.00%	50.00%	100.00%
		गिनती करना	470	256	726
	कुल	आयु के भीतर %	64.70%	35.30%	100.00%

तालिका 4.93 दर्शाती है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18 से 25 वर्ष की आयु के बीच के थे, 379 25 से 46 वर्ष की आयु के बीच के थे, 28 46-60 वर्ष की आयु के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 वर्ष की आयु के बीच के लोगों में से 116 खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 201 खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 वर्ष की आयु के लोगों में से 132 खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 247 खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 वर्ष की आयु के लोगों में से 07 खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं 60 वर्ष से अधिक आयु वर्ग के 01 लोग खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 01 लोग खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। एक साथ एकीकृत करने पर 256 उत्तरदाताओं ने खाता विवरण प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद किया, जबकि 470 उत्तरदाताओं ने खाता विवरण ऑनलाइन प्रिंट करने जैसे गैर-वित्तीय लेनदेन करना पसंद नहीं किया।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	1.759ए	3	0.624
संभावना अनुपात	1.823	3	0.61
रैखिक-दर-रैखिक एसोसिएशन	0.768	1	0.381
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि खाता विवरण प्रिंट करने के गैर-वित्तीय लेनदेन का उपयोग और आयु स्वतंत्र हैं (काई-स्क्वायर 1.759, df 3, $p > 0.05$)। इस प्रकार, खाता विवरण ऑनलाइन प्रिंट करने के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.36. विभिन्न आयु वर्ग के चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए विभिन्न आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.95 आयु के अनुसार चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. आयु के अनुसार चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेन-देन

			चेक बुक/पास बुक जारी करना		कुल
			नहीं	हाँ	
	18 से 25	गिनती करना	207	110	317
		आयु के भीतर %	65.3%	34.7%	100.0%
	25 से 46	गिनती करना	266	113	379
आयु		आयु के भीतर %	70.2%	29.8%	100.0%
	46 से 60	गिनती करना	20	8	28
		आयु के भीतर %	71.4%	28.6%	100.0%
	60 से ऊपर	गिनती करना	2	0	2
		आयु के भीतर %	100.0%	0.0%	100.0%
	कुल	गिनती करना	495	231	726
		आयु के भीतर %	68.2%	31.8%	100.0%

तालिका 4.95 से पता चलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18 से 25 वर्ष की आयु के बीच के थे, 379 25 से 46 वर्ष की आयु के बीच के थे, 28 46-60 वर्ष की आयु के बीच के थे और 2 60 वर्ष से अधिक आयु के थे। 18 से 25 वर्ष की आयु के बीच के लोगों में से 110 चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 207 चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 वर्ष की आयु के लोगों में से 113 चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 266 चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 वर्ष की आयु के लोगों में से 08 चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 20 चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 60 वर्ष से अधिक आयु के लोगों में से कोई भी चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद नहीं करता है, जबकि 02 चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। एक साथ एकीकृत करने पर 231 उत्तरदाता चेक

बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 495 उत्तरदाता चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	2.984ए	3	.394
संभावना अनुपात	3.575	3	.311
रैखिक-दर-रैखिक एसोसिएशन	2.446	1	.118
वैध मामलों की संख्या N	726		

ऊपर दिए गए काई-स्क्वायर परीक्षण का डोमिनो प्रभाव इस शून्य परिकल्पना को खारिज नहीं करता है कि चेक बुक/पास बुक जारी करने के गैर-वित्तीय लेनदेन का उपयोग और आयु स्वतंत्र हैं (काई-स्क्वायर 2.984, df 3, $p > 0.05$)। इस प्रकार, चेक बुक और पास बुक जारी करने के गैर-वित्तीय लेनदेन का उपयोग ऑनलाइन व्यक्ति की आयु पर निर्भर नहीं करता है।

4.37. विभिन्न आयु वर्गों में केवाईसी अद्यतन के गैर-वित्तीय लेनदेन:

सर्वेक्षण के लिए अलग-अलग आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.97 आयु के अनुसार केवाईसी अपडेट के गैर-वित्तीय लेन-देन को दर्शाती है।

तालिका 4. **आयु के अनुसार केवाईसी अपडेट के गैर-वित्तीय लेन-देन**

			केवाईसी अपडेट		कुल
			नहीं	हाँ	
	18 से 25	गिनती करना	194	123	317
		आयु के भीतर %	61.2%	38.8%	100.0%
आयु	25 से 46	गिनती करना	198	181	379
		आयु के भीतर %	52.2%	47.8%	100.0%
	46 से 60	गिनती करना	14	14	28
		आयु के भीतर %	50.0%	50.0%	100.0%
	60 से ऊपर	गिनती करना	1	1	2
		आयु के भीतर %	50.0%	50.0%	100.0%
	कुल	गिनती करना	407	319	726
		आयु के भीतर %	56.1%	43.9%	100.0%

तालिका 4.97 से यह देखा जा सकता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 317 18 से 25 वर्ष की आयु के बीच के थे, 379 25 से 46 वर्ष की आयु के बीच के थे, 28 46-60 वर्ष की

आयु के बीच के थे और कुछ 60 वर्ष से अधिक आयु के थे। 18 से 25 वर्ष की आयु के बीच के लोगों में से 123 केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 194 केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 25 से 46 वर्ष की आयु के लोगों में से 181 केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद करते हैं जबकि 198 केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। 46 से 60 वर्ष की आयु के लोगों में से 14 केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद करते हैं 60 वर्ष से अधिक आयु वर्ग के 01 लोग केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 01 लोग केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद नहीं करते हैं। एक साथ एकीकृत करने पर 319 उत्तरदाता केवाईसी अपडेट के गैर-वित्तीय लेनदेन करना पसंद करते हैं, जबकि 407 उत्तरदाता केवाईसी अपडेट के गैर-वित्तीय लेनदेन ऑनलाइन करना पसंद नहीं करते हैं।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	6.088ए	3	.107
संभावना अनुपात	6.108	3	.106
रैखिक-दर-रैखिक एसोसिएशन	5.586	1	.018
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि केवाईसी अपडेट के गैर-वित्तीय लेनदेन का उपयोग और आयु स्वतंत्र हैं (काई-स्क्वायर 6.088, डीएफ 3, पी > 0.05)। इस प्रकार, ऑनलाइन केवाईसी अपडेट के गैर-वित्तीय लेनदेन का उपयोग किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.38. ऑनलाइन लेनदेन में विभिन्न लिंगों के बीच ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया। नीचे दी गई तालिका 4.99 लिंग के आधार पर ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. **लिंग के आधार पर ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन**

			ऑनलाइन धोखाधड़ी और चार्जबैक		
			नहीं	हाँ	कुल
	पुरुष	गिनती करना	233	199	432

लिंग		लिंग के भीतर %	54%	46%	100
	महिला	गिनती करना	159	135	294
		लिंग के भीतर %	54%	46%	100
कुल		गिनती करना	392	334	726
		लिंग के भीतर %	54%	46%	100.0%

तालिका 4.99 से पता चलता है कि 432 पुरुषों में से 199 पुरुषों को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 233 पुरुषों को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली। इसी तरह, 294 महिलाओं में से 135 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 159 महिलाओं को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली। एकीकृत करने के बाद, 334 उत्तरदाताओं को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 392 उत्तरदाताओं को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली।

तालिका 4. **काई-स्कायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)	सटीक हस्ताक्षर.(दो तरफा)	सटीक हस्ताक्षर.(दो तरफा)
पियर्सन काई-स्कायर	.002ए	1	1		
निरंतरता सुधार	0	1	1		
संभावना अनुपात	0	1	1		
फिशर का सटीक परीक्षण				1	0.5
रैखिक-दर-रैखिक एसोसिएशन	0	1	1		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत काई-स्कायर परीक्षण के उपकरण इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि ऑनलाइन धोखाधड़ी, चार्जबैक और लिंग की चुनौतियां स्वतंत्र हैं (काई-स्कायर 0.002, df 1, $p > 0.05$) इसलिए, ऑनलाइन धोखाधड़ी और चार्जबैक द्वारा उत्पन्न चुनौतियां किसी व्यक्ति के लिंग पर निर्भर नहीं करती हैं।

4.39. ऑनलाइन लेनदेन में डेटा सुरक्षा के रूप में विभिन्न लिंगों के समक्ष आने वाली चुनौतियाँ:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया। नीचे दी गई तालिका 4.101 लिंग के आधार पर डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. लिंग के आधार पर डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति

		डेटा सुरक्षा		कुल	
			नहीं	हाँ	
	पुरुष	गिनती करना	181	251	432
लिंग		लिंग के भीतर %	41.9%	58.1%	100.0%
	महिला	गिनती करना	134	160	294
		लिंग के भीतर %	45.6%	54.4%	100.0%
कुल		गिनती करना	315	411	726
		लिंग के भीतर %	43.4%	56.6%	100.0%

तालिका 4.101 के अनुसार, 432 पुरुषों में से 251 पुरुषों को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 181 पुरुषों को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। इसी तरह, 294 महिलाओं में से 160 को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 134 महिलाओं को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। एकीकृत करने के बाद, 441 उत्तरदाताओं को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 315 उत्तरदाताओं को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)	सटीक सिग. (दो तरफा)	सटीक सिग. (दो तरफा)
पियर्सन काई-स्क्वायर	.965ए	1	.326		
निरंतरता सुधार	.821	1	.365		
संभावना अनुपात	.964	1	.326		
फिशर का सटीक परीक्षण				.360	.182
रैखिक-दर-रैखिक एसोसिएशन	.963	1	.326		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत कार्ई-स्कायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि डेटा सुरक्षा और लिंग की चुनौतियां स्वतंत्र हैं (कार्ई-स्कायर 0.965, df 1, $p > 0.05$) इसलिए, डेटा सुरक्षा द्वारा उत्पन्न चुनौतियां किसी व्यक्ति के लिंग पर निर्भर नहीं करती हैं।

4.40. अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में विभिन्न लिंगों के समक्ष आने वाली चुनौतियाँ

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया। नीचे दी गई तालिका 4.103 लिंग के आधार पर अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4.103 लिंग के आधार पर अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन

			अंतर्राष्ट्रीय ऑनलाइन भुगतान		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	377	55	432
लिंग		लिंग के भीतर %	87.3%	12.7%	100.0%
	महिला	गिनती करना	262	32	294
		लिंग के भीतर %	89.1%	10.9%	100.0%
कुल		गिनती करना	639	87	726
		लिंग के भीतर %	88.0%	12.0%	100.0%

तालिका 4.103 से पता चलता है कि 432 पुरुषों में से 55 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 377 पुरुषों को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। इसी तरह, 294 महिलाओं में से 32 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 262 महिलाओं को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। एकीकृत करने के बाद, 87 उत्तरदाताओं को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 639 उत्तरदाताओं को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई।

तालिका 4.104 कार्ड-स्कायर परीक्षण

			असि म्प. सिग.	सटीक हस्ता क्षर.	सटीक हस्ताक्षर.	
	कीमत	डीएफ	(दो तरफा)	(दो तरफा)	(एक तरफा)	
पियर्सन कार्ड-स्कायर	.566ए	1	.452			
निरंतरता सुधार	.404	1	.525			
संभावना अनुपात	.571	1	.450			
फिशर का सटीक परीक्षण				.486	.264	
रैखिक-दर-रैखिक एसोसिएशन	.565	1	.452			
वैध मामलों की संख्या N	726					

ऊपर प्रस्तुत कार्ड-स्कायर मूल्यांकन इस शून्य परिकल्पना को अस्वीकार नहीं करता है कि अंतर्राष्ट्रीय ऑनलाइन भुगतान और लिंग की चुनौतियाँ स्वतंत्र हैं (कार्ड-स्कायर 0.566, df 1, $p > 0.05$) इसलिए, अंतर्राष्ट्रीय ऑनलाइन भुगतान द्वारा उत्पन्न चुनौतियाँ किसी व्यक्ति के लिंग पर निर्भर नहीं करती हैं।

4.41. ऑनलाइन लेनदेन में भुगतान गेटवे चुनने में लिंग के आधार पर आने वाली चुनौतियाँ:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया। नीचे दी गई तालिका 4.105 लिंग के आधार पर ऑनलाइन लेनदेन में भुगतान गेटवे चुनने में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. लिंग के आधार पर ऑनलाइन लेनदेन में भुगतान गेटवे चुनने में आने वाली चुनौति

			भुगतान गेटवे चुनना		कुल
			नहीं	हाँ	
	पुरुष	गिनती करना	328	104	432
लिंग		लिंग के भीतर %	75.9%	24.1%	100.0%
	महिला	गिनती करना	227	67	294
		लिंग के भीतर %	77.2%	22.8%	100.0%
कुल		गिनती करना	555	171	726
		लिंग के भीतर %	76.4%	23.6%	100.0%

तालिका 4.105 से यह देखा जा सकता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष और 294 महिलाएं थीं। इन 432 पुरुषों में से 104 पुरुषों को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में चुनौतियों का सामना करना पड़ा, जबकि 328 पुरुषों को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में कोई चुनौती नहीं आई। इसी तरह, 294 महिलाओं में से 67 को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में चुनौतियों का सामना करना पड़ा, जबकि 227 महिलाओं को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में कोई चुनौती नहीं आई। एकीकृत करने के बाद, 171 उत्तरदाताओं को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में चुनौतियों का सामना करना पड़ा, जबकि 555 उत्तरदाताओं को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में कोई चुनौती नहीं आई।

तालिका 4. कार्ड-स्कायर परीक्षण

	कीमत	डीएफ	असिम्प. सिग.(दो तरफा)	सटीक हस्ताक्षर.(दो तरफा)	सटीक सिग. (1- पक्षीय)
पियर्सन कार्ड-स्कायर	.160ए	1	.689		
निरंतरता सुधार	.097	1	.755		
संभावना अनुपात	.161	1	.688		
फिशर का सटीक परीक्षण				.722	.379
रैखिक-दर-रैखिक एसोसिएशन	.160	1	.689		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत कार्ड-स्कायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि भुगतान गेटवे चुनने की चुनौतियां और लिंग स्वतंत्र हैं (कार्ड-स्कायर 0.160, df 1, $p > 0.05$) इसलिए, भुगतान गेटवे चुनने में आने वाली चुनौतियां किसी व्यक्ति के लिंग पर निर्भर नहीं करती हैं।

4.42. विभिन्न लिंगों के बीच बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.107 लिंग के आधार पर बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. लिंग के आधार पर बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति

क्रमांक	लिंग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	पुरुष	400	32	432	92.6%	7.4%
2	महिला	270	24	294	91.8%	8.2%
	कुल	670	56	726	92.3%	7.7%

तालिका 4.107 से आगे पता चलता है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 432 पुरुष और 294 महिलाएं थीं। इन 432 पुरुषों में से 32 पुरुषों को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 400 पुरुषों को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। इसी तरह, 294 महिलाओं में से 24 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 270 महिलाओं को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। एकीकृत करने के बाद, 56 उत्तरदाताओं को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 670 उत्तरदाताओं को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई।

4.43 सभी लिंगों के लोगों के सामने डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया। नीचे दी गई तालिका 4.108 लिंग के आधार पर डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. लिंग के आधार पर डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति

क्रमांक	लिंग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
---------	------	---------------	--------------	-----	----------	---------

1	पुरुष	220	212	432	50.9%	49.1%
2	महिला	151	143	294	51.4%	48.6%
	कुल	371	355	726	51.1%	48.9%

तालिका 4.108 से पता चलता है कि 432 पुरुषों में से 212 पुरुषों को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 220 पुरुषों को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली। इसी तरह, 294 महिलाओं में से 143 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 151 महिलाओं को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली। एकीकृत करने के बाद, 355 उत्तरदाताओं को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 371 उत्तरदाताओं को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली।

4.44 ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.109 ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को विभिन्न आयु समूहों में दर्शाती है।

तालिका 4. ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति

क्रमांक	आयु वर्ग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	18 से 25 वर्ष	163	154	317	51.4%	48.6%
2	25 से 46 वर्ष	216	163	379	57.0%	43.0%
3	46 से 60 वर्ष	13	15	28	46.4%	53.6%
4	60 वर्ष से ऊपर	0	2	2	0.0%	100.0%
	कुल	392	334	726	54.0%	46.0%

तालिका 4.109 से, 317 उत्तरदाता 18 से 25 वर्ष की आयु वर्ग में थे, 379 25 से 46 वर्ष की आयु वर्ग में थे, 28 46-60 आयु वर्ग में थे और 02 60 वर्ष से अधिक आयु के थे। 18-25 आयु वर्ग के लोगों में से 154 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 163 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली। 25 से 46 आयु वर्ग के लोगों में से 163 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 216 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया। 60 वर्ष से अधिक आयु वर्ग के 02 लोगों को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा है। एक साथ एकीकृत करने पर 334 उत्तरदाताओं को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 392 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	5.210 ^ए	3	.157
संभावना अनुपात	5.969	3	.113
रैखिक-दर-रैखिक एसोसिएशन	.252	1	.616
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के प्रभाव इस शून्य परिकल्पना को खारिज नहीं करते हैं कि ऑनलाइन धोखाधड़ी, चार्जबैक और आयु की चुनौतियां स्वतंत्र हैं (काई-स्क्वायर 5.210, df 3, $p > 0.05$) इसलिए, ऑनलाइन धोखाधड़ी और चार्जबैक द्वारा उत्पन्न चुनौतियां किसी व्यक्ति की आयु पर निर्भर नहीं करती हैं।

4.45. ऑनलाइन लेनदेन में डेटा सुरक्षा के रूप में विभिन्न युगों में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.111 में विभिन्न आयु समूहों के लोगों द्वारा ऑनलाइन लेनदेन में डेटा सुरक्षा के रूप में आने वाली चुनौतियों को दर्शाया गया है।

तालिका 4. विभिन्न आयु समूहों के लोगों द्वारा ऑनलाइन लेनदेन में डेटा सुरक्षा के रूप में आने वाली चुनौति

क्रमांक	आयु वर्ग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	18 से 25 वर्ष	126	191	317	39.7%	60.3%
2	25 से 46 वर्ष	176	203	379	46.4%	53.6%
3	46 से 60 वर्ष	12	16	28	42.9%	57.1%
4	60 वर्ष से ऊपर	1	1	2	50.0%	50.0%
	कुल	315	411	726	43.4%	56.6%

तालिका 4.111 से, 18-25 आयु वर्ग के उन उत्तरदाताओं में से 191 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 126 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया। 25 से 46 आयु वर्ग के लोगों में से 203 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 176 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया। 46 से 60 आयु वर्ग के लोगों में से 16 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 12 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया। 60 से ऊपर के आयु वर्ग के लोगों में से 01 ने ऑनलाइन लेनदेन में चुनौतियों का सामना किया है, जबकि 01 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	3.184ए	3	.364
संभावना अनुपात	3.190	3	.363
रैखिक-दर-रैखिक एसोसिएशन	2.291	1	.130
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत कार्ई-स्क्रायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि डेटा सुरक्षा और आयु की चुनौतियाँ स्वतंत्र हैं (कार्ई-स्क्रायर 3.184, df 3, $p > 0.05$) इसलिए, डेटा सुरक्षा द्वारा उत्पन्न चुनौतियाँ किसी व्यक्ति की आयु पर निर्भर नहीं करती हैं।

4.46. विभिन्न आयु वर्गों में अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.113 विभिन्न आयु समूहों के लोगों द्वारा अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. विभिन्न आयु समूहों के लोगों द्वारा अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति

क्रमांक	आयु वर्ग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	18 से 25 वर्ष	272	45	317	85.8%	14.2%
2	25 से 46 वर्ष	343	36	379	90.5%	9.5%
3	46 से 60 वर्ष	23	5	28	82.1%	17.9%
4	60 वर्ष से ऊपर	1	1	2	50.0%	50.0%
	कुल	639	87	726	88.0%	12.0%

तालिका 4.113 से पता चलता है कि 18-25 आयु वर्ग के 45 लोगों को अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 272 लोगों को अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 25 से 46 आयु वर्ग के 36 लोगों को अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 343 लोगों को अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 46 से 60 आयु वर्ग के लोगों में से 05 ने अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 23 ने अंतरराष्ट्रीय ऑनलाइन

भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं झेली। 60 से अधिक आयु वर्ग के लोगों में से 01 ने ऑनलाइन लेनदेन में चुनौतियों का सामना किया है, जबकि 01 ने अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं झेली। एक साथ एकीकृत करने पर 87 उत्तरदाताओं को अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 639 को अंतरराष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं झेलनी पड़ी।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग.(2-पक्षीय)
पियर्सन काई-स्क्वायर	7.346ए	3	.062
संभावना अनुपात	6.304	3	.098
रैखिक-दर-रैखिक एसोसिएशन	.581	1	.446
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि अंतरराष्ट्रीय ऑनलाइन भुगतान की चुनौतियाँ और आयु स्वतंत्र हैं (काई-स्क्वायर 7.346, df 3, $p > 0.05$) इसलिए, अंतरराष्ट्रीय ऑनलाइन भुगतान द्वारा उत्पन्न चुनौतियाँ किसी व्यक्ति की आयु पर निर्भर नहीं करती हैं।

4.47. ऑनलाइन लेनदेन में भुगतान गेटवे चुनने में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.115 में ऑनलाइन लेनदेन में विभिन्न आयु समूहों के लिए भुगतान गेटवे चुनने में आने वाली चुनौतियों को दर्शाया गया है।

तालिका 4. ऑनलाइन लेनदेन में विभिन्न आयु समूहों के लिए भुगतान गेटवे चुनने में आने वाली चुनौति

क्रमांक	आयु वर्ग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	18 से 25 वर्ष	242	75	317	76.3%	23.7%
2	25 से 46 वर्ष	289	90	379	76.3%	23.7%

3	46 से 60 वर्ष	23	5	28	82.1%	17.9%
4	60 वर्ष से ऊपर	1	1	2	50.0%	50.0%
	कुल	555	171	726	76.4%	23.6%

तालिका 4.115 से, 18-25 आयु वर्ग के 75 व्यक्तियों को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 242 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 25 से 46 आयु वर्ग के 90 लोगों को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 289 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 46 से 60 आयु वर्ग के 05 लोगों को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 23 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 60 से अधिक आयु वर्ग के 01 लोगों को ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 01 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। एक साथ एकीकृत करने पर 171 उत्तरदाताओं को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 555 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	1.291ए	3	.731
संभावना अनुपात	1.203	3	.752
रैखिक-दर-रैखिक एसोसिएशन	.017	1	.895
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि भुगतान गेटवे चुनने की चुनौतियां और आयु स्वतंत्र हैं (काई-स्क्वायर 1.291, df 3, $p > 0.05$) इसलिए, भुगतान गेटवे चुनने में आने वाली चुनौतियां किसी व्यक्ति की आयु पर निर्भर नहीं करती हैं।

4.48. विभिन्न आयु वर्गों में बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.117 विभिन्न आयु समूहों के लोगों द्वारा बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. विभिन्न आयु समूहों के लोगों द्वारा बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौति

क्रमांक	आयु वर्ग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	18 से 25 वर्ष	291	26	317	91.8%	8.2%
2	25 से 46 वर्ष	354	25	379	93.4%	6.6%
3	46 से 60 वर्ष	24	4	28	85.7%	14.3%
4	60 वर्ष से ऊपर	1	1	2	50.0%	50.0%
	कुल	670	56	726	92.3%	7.7%

तालिका 4.117 से पता चलता है कि 18-25 आयु वर्ग के 26 लोगों को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 291 लोगों को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 25 से 46 आयु वर्ग के लोगों में से 26 लोगों को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 291 लोगों को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई।

25 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 354 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 46 से 60 आयु वर्ग के लोगों में से 04 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 24 को बहुमुद्रा भुगतान

स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 60 से ऊपर के आयु वर्ग के लोगों में से 01 को ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा है, जबकि 01 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। एक साथ एकीकृत करने पर 56 उत्तरदाताओं को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा

तालिका 4. काई-स्क्वायर परीक्षण

	कीमत	डीएफ	असिम्ट. सिग.(2-पक्षीय)
पियर्सन काई-स्क्वायर	7.494ए	3	.058
संभावना अनुपात	4.697	3	.195
रैखिक-दर-रैखिक एसोसिएशन	.229	1	.632
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि बहुमुद्रा भुगतान स्वीकार करने की चुनौतियाँ और आयु स्वतंत्र हैं (काई-स्क्वायर 7.494, df 3, $p > 0.05$) इसलिए, बहुमुद्रा भुगतान स्वीकार करने से उत्पन्न चुनौतियाँ किसी व्यक्ति की आयु पर निर्भर नहीं करती हैं।

4.49. डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में विभिन्न आयु वर्गों में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.119 विभिन्न आयु समूहों में डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियों को दर्शाती है।

तालिका 4. विभिन्न आयु समूहों में डिजिटल भुगतान विफलता रूप में ऑनलाइन लेनदेन में आने वाली चुनौति

क्रमांक	आयु वर्ग	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	18 से 25 वर्ष	192	125	317	60.60%	39.40%
2	25 से 46 वर्ष	167	212	379	44.10%	55.90%
3	46 से 60 वर्ष	11	17	28	39.30%	60.70%

4	60 वर्ष से ऊपर	1	1	2	50.00%	50.00%
	कुल	371	355	726	51.10%	48.90%

तालिका 4.119 से, 18-25 आयु वर्ग के व्यक्तियों में से 125 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 192 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 25 से 46 आयु वर्ग के लोगों में से 212 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 167 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 46 से 60 आयु वर्ग के लोगों में से 17 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 11 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। 60 से अधिक आयु वर्ग के लोगों में से 01 को ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा है, जबकि 01 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग.(2-पक्षीय)
पियर्सन काई-स्क्वायर	20.447ए	3	.000
संभावना अनुपात	20.567	3	.000
रैखिक-दर-रैखिक एसोसिएशन	18.445	1	.000
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत किए गए काई-स्क्वायर परीक्षण का डोमिनो प्रभाव शून्य परिकल्पना को खारिज करता है कि डिजिटल भुगतान विफलता और उम्र की चुनौतियाँ स्वतंत्र हैं (काई-स्क्वायर 20.447, df 3, $p < 0.05$)। इसलिए, डिजिटल भुगतान विफलता से उत्पन्न चुनौतियाँ व्यक्ति की उम्र पर निर्भर करती हैं।

4.50. शिक्षा जगत में ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शैक्षिक स्तर पर डेटा एकत्र किया गया था। निम्न तालिका 4.121 शिक्षा के क्षेत्र में ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियों को दर्शाती है।

तालिका 4. शिक्षा के क्षेत्र में ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियाँ

क्रमांक	शिक्षा स्तर	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	एचएससी तक	30	23	53	56.6%	43.4%
2	डिप्लोमा	3	3	6	50.0%	50.0%
3	स्नातक	138	139	277	49.8%	50.2%
4	स्नातकोत्तर (PG)	203	159	362	56.1%	43.9%
5	पीएच.डी.	9	3	12	75.0%	25.0%
6	चार्टर्ड लेखाकार	7	7	14	50.0%	50.0%
7	अनुसंधान/अन्य	2	0	2	100.0%	0.0%
	कुल	392	334	726	54.0%	46.0%

तालिका 4.121 से, जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी की थी, उनमें से 23 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 30 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे, उनमें से 03 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 03 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती

नहीं मिली। जो उत्तरदाता स्नातक थे, उनमें से 139 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 138 को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं मिली। उत्तरदाताओं में से जो पीएचडी थे, 03 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 09 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया। उत्तरदाताओं में से जो चार्टर्ड अकाउंटेंट थे, 07 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 07 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया। उत्तरदाताओं में जो रिसर्च स्कॉलर थे, 02 ने ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में किसी चुनौती का सामना नहीं किया। एक साथ एकीकृत करने पर 334 उत्तरदाताओं को ऑनलाइन धोखाधड़ी और चार्जबैक के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 392

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	6.685ए	6	.351
संभावना अनुपात	7.566	6	.272
रैखिक-दर-रैखिक एसोसिएशन	.911	1	.340
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि ऑनलाइन धोखाधड़ी और चार्जबैक की चुनौतियां और शिक्षा स्वतंत्र हैं (काई-स्क्वायर 6.685, df 6, $p > 0.05$) इसलिए, ऑनलाइन धोखाधड़ी और चार्जबैक द्वारा उत्पन्न चुनौतियां किसी व्यक्ति की शिक्षा पर निर्भर नहीं करती हैं।

4.51. शिक्षा जगत में डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए 726 उत्तरदाताओं से उनके शैक्षिक स्तर के आधार पर डेटा एकत्र किया गया। निम्न तालिका 4.123 शिक्षा के क्षेत्र में डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियों को दर्शाती है।

तालिका 4. शिक्षा के क्षेत्र में डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति

क्रमांक	शिक्षा स्तर	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	एचएससी तक	24	29	53	45.3%	54.7%
2	डिप्लोमा	0	6	6	0.0%	100.0%
3	स्नातक	105	172	277	37.9%	62.1%
4	स्नातकोत्तर (PG)	172	190	362	47.5%	52.5%
5	पीएच.डी.	4	8	12	33.3%	66.7%
6	चार्टर्ड लेखाकार	8	6	14	57.1%	42.9%
7	अनुसंधान/अन्य	2	0	2	100.0%	0.0%
	कुल	315	411	726	43.4%	56.6%

तालिका 4.123 से यह देखा जा सकता है कि, एचएससी तक की शिक्षा पूरी करने वाले उत्तरदाताओं में से 29 को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 24 को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किया था उनमें से 06 को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि उनमें से किसी को भी डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। स्नातक उत्तरदाताओं में से 172 को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 105 को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। स्नातकोत्तर उत्तरदाताओं में से 190 को डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा उत्तरदाताओं में से जो चार्टर्ड अकाउंटेंट थे, उनमें से 06 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 08 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में किसी भी चुनौती का सामना नहीं किया। उत्तरदाताओं में से जो रिसर्च स्कॉलर थे, उनमें से 02 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में किसी भी चुनौती का सामना नहीं किया। एक साथ एकीकृत करने पर 411 उत्तरदाताओं ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया,

जबकि 315 ने डेटा सुरक्षा के रूप में ऑनलाइन लेनदेन में किसी भी चुनौती का सामना नहीं किया।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग.(2-पक्षीय)
पियर्सन काई-स्क्वायर	14.755ए	6	.022
संभावना अनुपात	17.740	6	.007
रैखिक-दर-रैखिक एसोसिएशन	3.477	1	.062
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि डेटा सुरक्षा और शिक्षा की चुनौतियाँ स्वतंत्र हैं (काई-स्क्वायर 14.755, df 6, $p > 0.05$) इसलिए, डेटा सुरक्षा द्वारा उत्पन्न चुनौतियाँ किसी व्यक्ति की शिक्षा पर निर्भर नहीं करती हैं।

4.52 शिक्षा के क्षेत्र में अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शैक्षिक स्तर के आधार पर डेटा एकत्र किया गया। निम्न तालिका 4.125 शिक्षा के क्षेत्र में अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियों को दर्शाती है।

तालिका 4. शिक्षा के क्षेत्र में अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति

क्रमांक	शिक्षा स्तर	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	एचएससी तक	47	6	53	88.7%	11.3%
2	डिप्लोमा	6	0	6	100.0%	0.0%
3	स्नातक	236	41	277	85.2%	14.8%
4	स्नातकोत्तर (PG)	325	37	362	89.8%	10.2%
5	पीएच.डी.	9	3	12	75.0%	25.0%
6	चार्टर्ड लेखाकार	14	0	14	100.0%	0.0%
7	अनुसंधान/अन्य	2	0	2	100.0%	0.0%
	कुल	639	87	726	88.0%	12.0%

तालिका 4.125 से यह समझा जा सकता है कि, जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किया था, उनमें से 06 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती

नहीं आई। उत्तरदाताओं में से जो स्नातक थे, उनमें से 41 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 236 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो स्नातकोत्तर थे, उनमें से 37 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 325 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो पीएचडी थे, उनमें से 03 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 09 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो चार्टर्ड अकाउंटेंट थे, उनमें से 14 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में जो रिसर्च स्कॉलर थे, उनमें से 02 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। एक साथ एकीकृत करने पर 87 उत्तरदाताओं को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 639 को अंतर्राष्ट्रीय ऑनलाइन भुगतान के रूप में ऑनलाइन लेनदेन में कोई चुनौती का सामना नहीं करना पड़ा।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग.(2-पक्षीय)
पियर्सन काई-स्क्वायर	8.097ए	6	.231
संभावना अनुपात	10.244	6	.115
रैखिक-दर-रैखिक एसोसिएशन	.904	1	.342
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि अंतर्राष्ट्रीय ऑनलाइन भुगतान और शिक्षा की चुनौतियाँ स्वतंत्र हैं (काई-स्क्वायर 8.097, df 6, $p > 0.05$) इसलिए, अंतर्राष्ट्रीय ऑनलाइन भुगतान द्वारा उत्पन्न चुनौतियाँ किसी व्यक्ति की शिक्षा पर निर्भर नहीं करती हैं।

4.53. शिक्षा जगत में भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शैक्षिक स्तर पर डेटा एकत्र किया गया था। निम्न तालिका 4.127 शिक्षा के क्षेत्र में भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियों को दर्शाती है।

तालिका 4. शिक्षा के क्षेत्र में भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति

क्रमांक	शिक्षा स्तर	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	एचएससी तक	42	11	53	79.2%	20.8%
2	डिप्लोमा	6	0	6	100.0%	0.0%
3	स्नातक	212	65	277	76.5%	23.5%
4	स्नातकोत्तर (PG)	273	89	362	75.4%	24.6%
5	पीएच.डी.	11	1	12	91.7%	8.3%
6	चार्टर्ड लेखाकार	9	5	14	64.3%	35.7%
7	अनुसंधान/अन्य	2	0	2	100.0%	0.0%
	कुल	555	171	726	76.4%	23.6%

तालिका 4.127 से, जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किया था, उनमें से 06 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो स्नातक थे, उनमें से 65 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 212 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो स्नातकोत्तर थे, उनमें से 89 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 273 को भुगतान गेटवे चुनने के

रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो पीएचडी थे, उनमें से 01 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 11 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो चार्टर्ड अकाउंटेंट थे, उनमें से 05 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 09 को भुगतान गेटवे चुनने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। शोधार्थियों में से 02 को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में किसी तरह की चुनौती का सामना नहीं करना पड़ा। जब एक साथ मिलाया गया तो 171 उत्तरदाताओं को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में किसी तरह की चुनौती का सामना करना पड़ा, जबकि 555 को ऑनलाइन लेनदेन में पेमेंट गेटवे चुनने में किसी तरह की चुनौती का सामना नहीं करना पड़ा।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2- पक्षीय)
पियर्सन काई-स्क्वायर	5.604ए	6	.469
संभावना अनुपात	7.709	6	.260
रैखिक-दर-रैखिक एसोसिएशन	.511	1	.475
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम, इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि भुगतान गेटवे चुनने की चुनौतियां और शिक्षा स्वतंत्र हैं (काई-स्क्वायर 5.604, df 6, $p > 0.05$) इसलिए, भुगतान गेटवे चुनने में उत्पन्न चुनौतियां किसी व्यक्ति की शिक्षा पर निर्भर नहीं करती हैं।

4.54 शिक्षा जगत में बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शैक्षिक स्तर पर डेटा एकत्र किया गया था। निम्न तालिका 4.129 शिक्षा के क्षेत्र में बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियों को दर्शाती है।

तालिका 4. शिक्षा के क्षेत्र में बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति

क्रमांक	शिक्षा स्तर	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	एचएससी तक	49	4	53	92.5%	7.5%
2	डिप्लोमा	6	0	6	100.0%	0.0%
3	स्नातक	255	22	277	92.1%	7.9%
4	स्नातकोत्तर (PG)	334	28	362	92.3%	7.7%
5	पीएच.डी.	12	0	12	100.0%	0.0%
6	चार्टर्ड लेखाकार	12	2	14	85.7%	14.3%
7	अनुसंधान/अन्य	2	0	2	100.0%	0.0%
	कुल	670	56	726	92.3%	7.7%

तालिका 4.129 से यह अनुमान लगाया जा सकता है कि जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी की है, उनमें से 04 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 49 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे, उनमें से 06 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। जो उत्तरदाता स्नातक थे, उनमें से 22 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 255 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। जो उत्तरदाता स्नातकोत्तर थे, उनमें से 28 को बहुमुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा उत्तरदाताओं में से जो चार्टर्ड अकाउंटेंट थे, उनमें से 12 को बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। उत्तरदाताओं में से जो रिसर्च स्कॉलर थे, उनमें से 02 को बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। एक साथ एकीकृत करने पर 56 उत्तरदाताओं को बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 670 को बहु-मुद्रा भुगतान स्वीकार करने के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई।

तालिका 4. कार्ड-स्कायर परीक्षण

	कीमत	डीएफ	असिम्ट. सिग.(2-पक्षीय)
पियर्सन कार्ड-स्कायर	2.544ए	6	.864
संभावना अनुपात	3.925	6	.687
रैखिक-दर-रैखिक एसोसिएशन	.022	1	.881

वैध मामलों की संख्या N	726		
------------------------	-----	--	--

जैसा कि ऊपर प्रस्तुत किया गया है, कार्ई-स्क्रायर परीक्षण इस शून्य परिकल्पना को अस्वीकार नहीं करता है कि बहुमुद्रा भुगतान स्वीकार करने की चुनौतियां और शिक्षा स्वतंत्र हैं (कार्ई-स्क्रायर 2.544, df 6, $p > 0.05$) इसलिए, बहुमुद्रा भुगतान स्वीकार करने से उत्पन्न चुनौतियां किसी व्यक्ति की शिक्षा पर निर्भर नहीं करती हैं।

4.55 शिक्षा जगत में डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में आने वाली चुनौतियाँ:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शैक्षिक स्तर के आधार पर डेटा एकत्र किया गया। निम्न तालिका 4.131 शिक्षा के क्षेत्र में डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौतियों को दर्शाती है।

तालिका 4. शिक्षा के क्षेत्र में डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन के सामने आने वाली चुनौति

क्रमांक	शिक्षा स्तर	नहीं (संख्या)	हाँ (संख्या)	कुल	नहीं (%)	हाँ (%)
1	एचएससी तक	31	22	53	58.5%	41.5%
2	डिप्लोमा	6	0	6	100.0%	0.0%
3	स्नातक	154	123	277	55.6%	44.4%
4	स्नातकोत्तर (PG)	167	195	362	46.1%	53.9%
5	पीएच.डी.	7	5	12	58.3%	41.7%
6	चार्टर्ड लेखाकार	6	8	14	42.9%	57.1%
7	अनुसंधान/अन्य	0	2	2	0.0%	100.0%
	कुल	371	355	726	51.1%	48.9%

तालिका 4.131 के ठीक ऊपर स्थिति यह है कि, एचएससी तक अपनी शिक्षा पूरी करने वाले उत्तरदाताओं में से 22 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 31 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे उनमें से 06 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। जो उत्तरदाता स्नातक थे उनमें से 123 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा, जबकि 154 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में कोई चुनौती नहीं आई। जो उत्तरदाता स्नातकोत्तर थे उनमें से 195 को डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना करना पड़ा उत्तरदाताओं में से जो चार्टर्ड अकाउंटेंट थे, उनमें से 08 ने डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 06 ने डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में किसी भी चुनौती का सामना नहीं किया। उत्तरदाताओं में से जो शोध विद्वान थे, उनमें से 02 ने डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया। एक साथ एकीकृत करने पर 355 उत्तरदाताओं ने डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में चुनौतियों का सामना किया, जबकि 371 ने डिजिटल भुगतान विफलता के रूप में ऑनलाइन लेनदेन में किसी भी चुनौती का सामना नहीं किया।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	15.437ए	6	.017
संभावना अनुपात	18.540	6	.005
रैखिक-दर-रैखिक एसोसिएशन	7.446	1	.006
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत काई-स्क्वायर परीक्षण के परिणाम इस शून्य परिकल्पना को खारिज नहीं करते हैं कि डिजिटल भुगतान विफलता और शिक्षा की चुनौतियां स्वतंत्र हैं (काई-स्क्वायर 15.437, df 6, $p > 0.05$) इसलिए, डिजिटल भुगतान विफलता से उत्पन्न चुनौतियां किसी व्यक्ति की शिक्षा पर निर्भर नहीं करती हैं।

4.56. लिंग के आधार पर ऑनलाइन सुरक्षा का महत्व:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.133 लिंग के आधार पर ऑनलाइन सुरक्षा के महत्व को दर्शाती है।

तालिका 4. लिंग के आधार पर ऑनलाइन सुरक्षा के महत्व

			क्या आपको लगता है कि ऑनलाइन सुरक्षा महत्वपूर्ण है?			कुल
			हाँ	कुछ हद तक महत्वपूर्ण ।	नहीं	
लिंग	पुरुष	गिनती करना	395	29	8	432
		लिंग के भीतर %	91.4%	6.7%	1.9%	100.0 %
	महिला	गिनती करना	285	7	2	294
		लिंग के भीतर %	96.9%	2.4%	0.7%	100.0 %
कुल		गिनती करना	680	36	10	726
		लिंग के भीतर %	93.7%	5.0%	1.4%	100.0 %

तालिका 4.133 से 432 पुरुषों में से 08 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 29 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 395 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। 294 महिलाओं में से 02 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 07 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 285 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। एकीकृत करने के बाद, 10 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 36 उत्तरदाताओं

ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 680 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	8.930ए	2	.012
संभावना अनुपात	9.775	2	.008
रैखिक-दर-रैखिक एसोसिएशन	7.884	1	.005
वैध मामलों की संख्या N	726		

जैसा कि ऊपर बताया गया है, काई-स्क्वायर परीक्षण का डोमिनो प्रभाव शून्य परिकल्पना को खारिज नहीं करता है कि ऑनलाइन सुरक्षा और लिंग का महत्व स्वतंत्र हैं (काई-स्क्वायर 8.930, $df\ 2, p > 0.05$) इसलिए, ऑनलाइन सुरक्षा का महत्व किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

4.57. आयु के आधार पर ऑनलाइन सुरक्षा का महत्व:

सर्वेक्षण के लिए, विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। निम्न तालिका 4.135 विभिन्न आयु समूहों में ऑनलाइन सुरक्षा के महत्व को दर्शाती है।

तालिका 4. **विभिन्न आयु समूहों में ऑनलाइन सुरक्षा के महत्व**

			उत्तरदाताओं की भावना कि ऑनलाइन सुरक्षा महत्वपूर्ण है			कुल
			हाँ	कुछ हद तक महत्वपूर्ण	नहीं	
	18 से 25	गिनती करना	289	22	6	317
		आयु के भीतर %	91.2%	6.9%	1.9%	100.0%
	25 से 46	गिनती करना	363	14	2	379
		आयु के भीतर %	95.8%	3.7%	0.5%	100.0%
आयु	46 से 60	गिनती करना	26	0	2	28
		आयु के भीतर %	92.9%	0.0%	7.1%	100.0%

	60 से ऊपर	गिनती करना	2	0	0	2
		आयु के भीतर %	100.0%	0.0%	0.0%	100.0%
	कुल	गिनती करना	680	36	10	726
		आयु के भीतर %	93.7%	5.0%	1.4%	100.0%

तालिका 4.135 के ठीक आगे, कुल 726 उत्तरदाताओं को सर्वेक्षण में शामिल किया गया था, 317 18 से 25 वर्ष की आयु वर्ग के थे, 379 25 से 46 वर्ष की आयु वर्ग के थे, 28 46-60 आयु वर्ग के थे और 02 60 वर्ष से अधिक आयु के थे। 18-25 आयु वर्ग के लोगों में से, 06 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 22 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 289 उत्तरदाताओं को लगा कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। 25 से 46 आयु वर्ग के लोगों में से, 02 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 14 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 363 उत्तरदाताओं को लगा कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। 46 से 60 आयु वर्ग के लोगों में से, 02 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, किसी भी उत्तरदाता ने महसूस नहीं किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है 60 वर्ष से अधिक आयु वर्ग के 02 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। एक साथ एकीकृत करने पर, 10 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 36 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 680 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	15.005ए	6	.020
संभावना अनुपात	13.510	6	.036
रैखिक-दर-रैखिक एसोसिएशन	2.696	1	.101
वैध मामलों की संख्या N	726		

ऊपर प्रस्तुत कार्ई-स्क्रायर परीक्षण के परिणाम इस शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि ऑनलाइन सुरक्षा और आयु का महत्व स्वतंत्र हैं (कार्ई-स्क्रायर 15.005, df 2, $p > 0.05$) इसलिए, ऑनलाइन सुरक्षा का महत्व किसी व्यक्ति की आयु पर निर्भर नहीं करता है।

4.58 शिक्षा में ऑनलाइन सुरक्षा का महत्व:

सर्वेक्षण के लिए, 726 उत्तरदाताओं से उनके शैक्षिक स्तर के आधार पर डेटा एकत्र किया गया। निम्न तालिका 4.137 शिक्षा के क्षेत्र में ऑनलाइन सुरक्षा के महत्व को दर्शाती है।

तालिका 4. शिक्षा के क्षेत्र में ऑनलाइन सुरक्षा के महत्व

			शिक्षा के माध्यम से ऑनलाइन सुरक्षा का महत्व			
			हाँ	कुछ हद तक महत्वपूर्ण.	नहीं	कुल
शिक्षा	एचएससी तक	गिनती करना	47	4	2	53
		शिक्षा के क्षेत्र में %	88.7%	7.5%	3.8%	100.0%
	डिप्लोमा	गिनती करना	2	4	0	6
		शिक्षा के क्षेत्र में %	33.3%	66.7%	0.0%	100.0%
	स्नातक	गिनती करना	253	16	8	277
		शिक्षा के क्षेत्र में %	91.3%	5.8%	2.9%	100.0%
	स्नातकोत्तर	गिनती करना	350	12	0	362
		शिक्षा के क्षेत्र में %	96.7%	3.3%	0.0%	100.0%
	पीएचडी	गिनती करना	12	0	0	12
		शिक्षा के क्षेत्र में %	100.0%	0.0%	0.0%	100.0%
	चार्टर्ड एकाउंटेंट	गिनती करना	14	0	0	14
		शिक्षा के क्षेत्र में %	100.0%	0.0%	0.0%	100.0%
	रिसर्च स्कॉलर	गिनती करना	2	0	0	2
		शिक्षा के क्षेत्र में %	100.0%	0.0%	0.0%	100.0%

		शिक्षा के क्षेत्र में %	100.0%	0.0%	0.0%	100.0%
कुल	गिनती करना		680	36	10	726
	शिक्षा के क्षेत्र में %		93.7%	5.0%	1.4%	100.0%

तालिका 4.137 से, जिन उत्तरदाताओं ने एचएससी तक अपनी शिक्षा पूरी की थी, 02 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 04 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 47 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। जिन उत्तरदाताओं ने डिप्लोमा पाठ्यक्रम किए थे, उनमें से 04 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 02 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। उत्तरदाताओं में से जो स्नातक थे, 08 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 16 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 253 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है। उत्तरदाताओं में से जो स्नातकोत्तर थे, 12 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है जबकि 350 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है एक साथ एकीकृत करने पर, 10 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा महत्वपूर्ण नहीं है, 36 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा कुछ हद तक महत्वपूर्ण है, जबकि 680 उत्तरदाताओं ने महसूस किया कि ऑनलाइन सुरक्षा वास्तव में महत्वपूर्ण है।

तालिका 4. **काई-स्क्वायर परीक्षण**

	कीमत	डीएफ	असिम्प्ट. सिग. (2-पक्षीय)
पियर्सन काई-स्क्वायर	65.884 ^a	12	.000
संभावना अनुपात	39.123	12	.000
रैखिक-दर-रैखिक एसोसिएशन	17.164	1	.000
वैध मामलों की संख्या N	726		

उपरोक्त काई-स्क्वायर परीक्षण का अंतिम परिणाम इस शून्य परिकल्पना को खारिज करता है कि ऑनलाइन सुरक्षा और शिक्षा का महत्व स्वतंत्र हैं (काई-स्क्वायर 65.884, df 12, $p < 0.05$)। इसलिए, ऑनलाइन सुरक्षा का महत्व व्यक्ति की शिक्षा पर निर्भर करता है।

4.59. लिंग के आधार पर डेटा सुरक्षा पर हमला:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.139 डेटा सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) से जुड़े जोखिम कारक को दर्शाती है, जिसके लिए उत्तरदाता जिम्मेदार हैं (जैसे परिवार के सदस्य)।

तालिका 4. डेटा सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) से जुड़े जोखिम कारक

	लिंग	मैलवेयर	फ़िशिंग	डेटा लीक	डॉक्सिंग
	अर्थ	3.10	3.20	3.28	3.23
पुरुष	एन	432	432	432	432
	मानक व्यतिक्रम	1.388	1.308	1.407	1.300
	अर्थ	3.32	3.45	3.52	3.55
महिला	एन	294	294	294	294
	मानक व्यतिक्रम	1.304	1.215	1.374	1.254
	अर्थ	3.19	3.30	3.38	3.36
कुल	एन	726	726	726	726
	मानक व्यतिक्रम	1.358	1.276	1.398	1.290

ऊपर दी गई तालिका में पुरुष और महिला उत्तरदाताओं द्वारा अनुभव किए गए मैलवेयर, फ़िशिंग, डेटा लीक और डॉक्सिंग के विशेष संदर्भ के साथ डेटा सुरक्षा जोखिम के बारे में जानकारी से पता चलता है कि सभी प्रकार के जोखिम में महिला उत्तरदाताओं ने अपने पुरुष समकक्षों की तुलना में इसे अधिक जोखिम भरा माना, जैसा कि उच्च औसत मूल्य द्वारा दर्शाया गया है। इस प्रकार, डेटा से यह स्पष्ट है कि महिलाओं द्वारा अनुभव किए जाने वाले सुरक्षा जोखिम पुरुषों की तुलना में अधिक हैं। पुरुष और महिला के बीच सुरक्षा जोखिम के प्रति धारणा में महत्वपूर्ण परिवर्तन को समझने के लिए आगे का विश्लेषण किया गया है।

तालिका 4. संगति के माप

	ईटा	एटा स्केर्ड
मैलवेयर * लिंग	.081	.007
फ़िशिंग * लिंग	.094	.009
डेटा लीक * लिंग	.085	.007
डॉक्सिंग * लिंग	.121	.015

पुरुष और महिला के बीच जोखिम धारणा में महत्वपूर्ण अंतर की जांच करने के लिए आयोजित एनोवा परीक्षण के परिणाम बताते हैं कि विचाराधीन सभी चार प्रकार के जोखिम यानी मैलवेयर,

फ़िशिंग, डेटा लीक और डॉक्सिंग (पी < 0.05) में पुरुष और महिला के बीच महत्वपूर्ण अंतर है। इस प्रकार, हम निष्कर्ष निकालते हैं कि पुरुषों की तुलना में महिलाओं की जोखिम धारणा अधिक है।

4.60. सभी आयु वर्गों में डेटा सुरक्षा पर हमला:

सर्वेक्षण के लिए, सभी आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। निम्न तालिका 4.141 उत्तरदाताओं के लिए जिम्मेदार लोगों (उदाहरण के लिए, परिवार के सदस्यों) के लिए डेटा सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) में शामिल जोखिम कारक को दर्शाती है।

तालिका 4. उत्तरदाताओं के लिए जिम्मेदार लोगों (उदाहरण के लिए, परिवार के सदस्यों) के लिए डेटा सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) में शामिल जोखिम कारक

	आयु	मैलवेयर	फ़िशिंग	डेटा लीक	डॉक्सिंग
	अर्थ	2.93	3.19	3.17	3.26
18 से 25	एन	317	317	317	317
	मानक व्यतिक्रम	1.368	1.328	1.414	1.298
	अर्थ	3.37	3.36	3.53	3.42
25 से 46	एन	379	379	379	379
	मानक व्यतिक्रम	1.320	1.229	1.365	1.281
	अर्थ	3.79	3.86	3.86	3.79
46 से 60	एन	28	28	28	28
	मानक व्यतिक्रम	1.228	1.145	1.325	1.228
	अर्थ	2.00	2.00	2.00	2.00
60 से ऊपर	एन	2	2	2	2
	मानक व्यतिक्रम	.000	.000	.000	.000
	अर्थ	3.19	3.30	3.38	3.36
कुल	एन	726	726	726	726
	मानक व्यतिक्रम	1.358	1.276	1.398	1.290

ऊपर दी गई तालिका में प्रस्तुत विभिन्न आयु समूहों के उत्तरदाताओं द्वारा अनुभव किए गए मैलवेयर, फ़िशिंग, डेटा लीक और डॉक्सिंग के विशेष संदर्भ के साथ डेटा सुरक्षा जोखिम के बारे में जानकारी से पता चलता है कि सभी प्रकार के जोखिमों में 46-60 आयु वर्ग के उत्तरदाताओं ने इसे अपने अन्य समकक्षों की तुलना में अधिक जोखिम भरा माना, जैसा कि उच्च औसत मूल्य द्वारा इंगित किया गया है। इसलिए, डेटा से यह स्पष्ट है कि 46-60 आयु वर्ग द्वारा अनुभव किए गए सुरक्षा जोखिम 18-25, 25-46 और 60 से ऊपर के आयु वर्ग की तुलना में अधिक हैं। सभी

आयु के उत्तरदाताओं के बीच सुरक्षा जोखिम के प्रति धारणा में महत्वपूर्ण अंतर को समझने के लिए आगे का विश्लेषण किया गया है।

तालिका 4. संगति के माप

	ईटा	एटा स्केर्ड
मैलवेयर * आयु	.188	.035
फ़िशिंग * आयु	.120	.014
डेटा लीक * आयु	.153	.023
डॉक्सिंग * आयु	.105	.011

विभिन्न आयु वर्ग के उत्तरदाताओं के बीच जोखिम धारणा में महत्वपूर्ण अंतर की जांच करने के लिए आयोजित एनोवा परीक्षण के परिणाम दर्शाते हैं कि विचाराधीन सभी चार प्रकार के जोखिम अर्थात् मैलवेयर, फ़िशिंग, डेटा लीक और डॉक्सिंग (पी > 0.05) में विभिन्न आयु वर्ग के उत्तरदाताओं के बीच कोई महत्वपूर्ण अंतर नहीं है। इस प्रकार, हम निष्कर्ष निकालते हैं कि सभी उत्तरदाताओं में, 18-25, 46-60 और 60 से ऊपर आयु वर्ग की तुलना में 46 से 60 आयु वर्ग सबसे अधिक है।

4.61. शिक्षा जगत में डेटा सुरक्षा पर हमला:

सर्वेक्षण के लिए शिक्षा जगत के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.143 डेटा सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) से जुड़े जोखिम कारक को दर्शाती है, जिसके लिए उत्तरदाता जिम्मेदार हैं (जैसे परिवार के सदस्य)।

तालिका 4. सुरक्षा हमलों (मैलवेयर, फ़िशिंग, डेटा लीक, डॉक्सिंग) से जुड़े जोखिम कारक

शिक्षा	मैलवेयर	फ़िशिंग	डेटा लीक	डॉक्सिंग
अर्थ	3.26	3.34	3.68	3.23
एचएससी तक	एन	53	53	53
मानक व्यतिक्रम	1.546	1.427	1.37	1.436
अर्थ	4.33	5	5	5
डिप्लोमा	एन	6	6	6
मानक व्यतिक्रम	0.516	0	0	0
अर्थ	2.86	3.08	3.09	3.18
स्नातक	एन	277	277	277
मानक व्यतिक्रम	1.347	1.311	1.414	1.29
अर्थ	3.4	3.42	3.54	3.5
स्नातकोत्तर	एन	362	362	362
मानक व्यतिक्रम	1.297	1.21	1.358	1.253

	अर्थ	2.5	3	2.5	2.67
पीएच.डी.	एन	12	12	12	12
	मानक व्यतिक्रम	1.446	1.206	1.446	1.435
	अर्थ	4	4	4	3.57
चार्टर्ड एकाउंटेंट	एन	14	14	14	14
	मानक व्यतिक्रम	0.961	0.961	0.961	0.938
	अर्थ	3	3	3	3
रिसर्च स्कॉलर	एन	2	2	2	2
	मानक व्यतिक्रम	0	0	0	0
	अर्थ	3.19	3.3	3.38	3.36
कुल	एन	726	726	726	726
	मानक व्यतिक्रम	1.358	1.276	1.398	1.29

ऊपर दी गई तालिका में विभिन्न शैक्षिक पृष्ठभूमि के उत्तरदाताओं द्वारा मैलवेयर, फ़िशिंग, डेटा लीक और डॉक्सिंग के विशेष संदर्भ के साथ डेटा सुरक्षा जोखिम के बारे में जानकारी से पता चलता है कि सभी प्रकार के जोखिम में उत्तरदाताओं ने इसे अपने अन्य समकक्षों की तुलना में अधिक जोखिम भरा माना, जैसा कि उच्च औसत मूल्य से संकेत मिलता है। इसलिए, डेटा से यह स्पष्ट है कि एचएससी तक की शिक्षा पूरी करने वाले उत्तरदाताओं द्वारा महसूस किए गए सुरक्षा जोखिम उन उत्तरदाताओं की तुलना में अधिक हैं जिन्होंने स्नातक, डिप्लोमा पाठ्यक्रम, स्नातकोत्तर, चार्टर्ड अकाउंटेंसी, पीएचडी या रिसर्च स्कॉलर हैं। शिक्षा भर के उत्तरदाताओं के बीच सुरक्षा जोखिम के प्रति धारणा में महत्वपूर्ण अंतर को समझने के लिए आगे का विश्लेषण किया गया है।

तालिका 4. संगति के माप

	ईटा	एटा स्केर्ड
मैलवेयर * शिक्षा	0.227	0.052
फ़िशिंग * शिक्षा	0.194	0.037
डेटा लीक * शिक्षा	0.217	0.047
डॉक्सिंग * शिक्षा	0.182	0.033

शिक्षा के विभिन्न क्षेत्रों में उत्तरदाताओं के बीच जोखिम धारणा में महत्वपूर्ण अंतर की जांच करने के लिए आयोजित एनोवा परीक्षण के परिणाम दर्शाते हैं कि विचाराधीन सभी चार प्रकार के जोखिम अर्थात मैलवेयर, फ़िशिंग, डेटा लीक और डॉक्सिंग ($p < 0.05$) में शिक्षा के विभिन्न क्षेत्रों में उत्तरदाताओं के बीच महत्वपूर्ण अंतर है। इस प्रकार, हम निष्कर्ष निकालते हैं कि सभी

उत्तरदाताओं में, एचएससी तक की शिक्षा पूरी करने वाले उत्तरदाताओं के बीच सुरक्षा जोखिम के प्रति धारणा में अंतर उन उत्तरदाताओं की तुलना में अधिक था जिन्होंने स्नातक, डिप्लोमा पाठ्यक्रम, स्नातकोत्तर, चार्टर्ड अकाउंटेंसी, पीएचडी या शोध विद्वान हैं।

4.62. मैलवेयर/लिंग-भेदभावपूर्ण गतिविधियों के विरुद्ध डेटा सुरक्षा:

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 4.145 लिंग के आधार पर मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा को दर्शाती है।

तालिका 4. मैलवेयर/लिंग-भेदभावपूर्ण गतिविधियों के विरुद्ध डेटा सुरक्षा

लिंग		रैंसमवेयर	बिना सूचना के डिवाइस कैमरा / वेबकैम पर निगरानी रखी जा रही है	सरकारी हस्तक्षेप	आपके द्वारा देखी जाने वाली वेबसाइटों के साथ स्थान ऑकड़े साझा किए जा रहे हैं
पुरुष	अर्थ	3.1296	3.2986	3.1921	3.2986
	एन	432	432	432	432
	मानक व्यतिक्रम	1.48679	1.43900	1.41999	1.49281
महिला	अर्थ	3.2449	3.4218	3.2653	3.4558
	एन	294	294	294	294
	मानक व्यतिक्रम	1.54165	1.47990	1.48635	1.53561
कुल	अर्थ	3.1763	3.3485	3.2218	3.3623
	एन	726	726	726	726
	मानक व्यतिक्रम	1.50925	1.45594	1.44666	1.51121

मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा से संबंधित जानकारी, विशेष रूप से रैंसमवेयर के संबंध में, डिवाइस के कैमरा/वेबकैम के माध्यम से जांच की जा रही है, उत्तरदाताओं की जागरूकता से वंचित, सरकारी हस्तक्षेप और वेबसाइट की जानकारी उत्तरदाताओं द्वारा देखी जा रही वेबसाइटों के साथ साझा की जा रही है, जैसा कि पुरुष और महिला उत्तरदाताओं द्वारा माना जाता है, जैसा कि ऊपर दी गई तालिका में दिखाया गया है कि कुल मिलाकर काफी मैलवेयर/गतिविधियां पाई गईं, महिला उत्तरदाताओं ने इसे अपने पुरुष समकक्षों की तुलना में डेटा सुरक्षा जोखिम के बारे में अधिक चिंतित माना, जैसा कि उच्च माध्य द्वारा इंगित किया गया है। इस प्रकार, जानकारी से यह स्पष्ट है कि महिलाओं द्वारा महसूस किए जाने वाले सूचना सुरक्षा

जोखिम पुरुषों की तुलना में अधिक हैं। पुरुष और महिला के बीच सुरक्षा जोखिम चिंताओं में कई अंतरों को जानने के लिए आगे का विश्लेषण किया गया।

4.63. मैलवेयर/विभिन्न आयु वर्गों की गतिविधियों के विरुद्ध डेटा सुरक्षा:

सर्वेक्षण के लिए विभिन्न आयु वर्ग के 726 उत्तरदाताओं से डेटा एकत्र किया गया। नीचे दी गई तालिका 4.146 विभिन्न आयु वर्ग के लोगों के बीच मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा को दर्शाती है।

तालिका 4. विभिन्न आयु वर्ग के लोगों के बीच मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा

आयु		मैलवेयर	मेरी डिवाइस के कैमरे / वेबकैम के माध्यम से मेरी जानकारी के बिना देखा जाना	सरकारी हस्तक्षेप	आपके द्वारा देखी जाने वाली वेबसाइटों के साथ स्थान की जानकारी साझा की जा रही है
18 से 25	अर्थ	2.9590	3.2208	3.0820	3.2208
	एन	317	317	317	317
	मानक व्यतिक्रम	1.48885	1.48040	1.42076	1.60945
25 से 46	अर्थ	3.3456	3.4248	3.3034	3.4459
	एन	379	379	379	379
	मानक व्यतिक्रम	1.51685	1.45715	1.48547	1.44534
46 से 60	अर्थ	3.4286	3.8571	3.7857	3.9286
	एन	28	28	28	28
	मानक व्यतिक्रम	1.37244	.93152	.95674	.97861
60 से ऊपर	अर्थ	2.0000	2.0000	2.0000	2.0000
	एन	2	2	2	2
	मानक व्यतिक्रम	.00000	.00000	.00000	.00000

कुल	अर्थ	3.1763	3.3485	3.2218	3.3623
	एन	726	726	726	726
	मानक व्यतिक्रम	1.50925	1.45594	1.44666	1.51121

रैनसमवेयर के विशेष संदर्भ में मैलवेयर/गतिविधियों के खिलाफ संबंधित डेटा सुरक्षा के बारे में जानकारी, उत्तरदाताओं की जानकारी के बिना उपकरणों के कैमरा/वेबकैम के माध्यम से देखी जा रही है, सरकारी हस्तक्षेप और उत्तरदाताओं द्वारा देखी जाने वाली वेबसाइटों के साथ स्थान की जानकारी साझा की जा रही है, जैसा कि विभिन्न आयु समूहों के उत्तरदाताओं द्वारा ऊपर दी गई तालिका में प्रस्तुत किया गया है, यह दर्शाता है कि सभी प्रकार के मैलवेयर/गतिविधियों में 46-60 आयु वर्ग के उत्तरदाताओं ने इसे अपने अन्य समकक्षों की तुलना में डेटा सुरक्षा जोखिम के बारे में अधिक चिंतित माना, जैसा कि उच्च औसत मूल्य द्वारा इंगित किया गया है। इसलिए, डेटा से यह स्पष्ट है कि 46-60 आयु वर्ग द्वारा डेटा सुरक्षा जोखिम की चिंता 18-25, 25-46 और 60 से ऊपर के आयु वर्ग की तुलना में अधिक है।

4.64. शिक्षा जगत में मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा:

सर्वेक्षण के लिए शिक्षा जगत के 726 उत्तरदाताओं से डेटा एकत्र किया गया। नीचे दी गई तालिका 4.147 शिक्षा जगत में मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा को दर्शाती है।

तालिका 4. शिक्षा जगत में मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा से संबंधित

शिक्षा		रैनसमवेयर	मेरी डिवाइस के कैमरे / वेबकैम के माध्यम से मेरी जानकारी के बिना देखा जाना	सरकारी हस्तक्षेप	आपके द्वारा देखी जाने वाली वेबसाइटों के साथ स्थान की जानकारी साझा की जा रही है
एचएससी तक	अर्थ	2.7736	3.1509	3.0377	3.0755
	एन	53	53	53	53
	मानक व्यतिक्रम	1.43636	1.62192	1.30033	1.74145
डिप्लोमा	अर्थ	4	4.3333	4.6667	5
	एन	6	6	6	6
	मानक व्यतिक्रम	1.54919	1.0328	0.5164	0
स्नातक	अर्थ	3	3.2238	3.0542	3.1805
	एन	277	277	277	277

	मानक व्यतिक्रम	1.52039	1.46223	1.42466	1.57537
स्नातकोत्तर	अर्थ	3.337	3.4392	3.3315	3.489
	एन	362	362	362	362
	मानक व्यतिक्रम	1.49504	1.4251	1.46257	1.40484
पीएच.डी.	अर्थ	2.8333	2.8333	3	3.1667
	एन	12	12	12	12
	मानक व्यतिक्रम	1.64225	1.64225	1.80907	1.74946
चार्टर्ड एकाउंटेंट	अर्थ	3.8571	4	3.7143	4
	एन	14	14	14	14
	मानक व्यतिक्रम	1.16732	0.96077	1.32599	1.24035
	अर्थ	4	5	5	5
रिसर्च स्कॉलर	एन	2	2	2	2
कुल	मानक व्यतिक्रम	0	0	0	0
	अर्थ	3.1763	3.3485	3.2218	3.3623
	एन	726	726	726	726
	मानक				
	विचलन	1.50925	1.45594	1.44666	1.51121

रैनसमवेयर के विशेष संदर्भ में मैलवेयर/गतिविधियों के खिलाफ संबंधित डेटा सुरक्षा के बारे में जानकारी, उत्तरदाताओं की जानकारी के बिना उपकरणों के कैमरा/वेबकैम के माध्यम से देखी जा रही है, सरकारी हस्तक्षेप और उत्तरदाताओं द्वारा देखी जाने वाली वेबसाइटों के साथ स्थान की जानकारी साझा की जा रही है जैसा कि विभिन्न शैक्षिक पृष्ठभूमि के उत्तरदाताओं द्वारा ऊपर दी गई तालिका में प्रस्तुत किया गया है, यह दर्शाता है कि सभी प्रकार के मैलवेयर/गतिविधियों में, जो उत्तरदाता शोध विद्वान थे, वे अपने अन्य समकक्षों की तुलना में डेटा सुरक्षा जोखिम के बारे में अधिक चिंतित थे, जैसा कि उच्च औसत मूल्य द्वारा इंगित किया गया है। इसलिए, यह डेटा से स्पष्ट है कि उत्तरदाताओं द्वारा डेटा सुरक्षा जोखिम की चिंता, जो शोध विद्वान थे, एचएससी तक अपनी शिक्षा पूरी करने वाले उत्तरदाताओं की तुलना में अधिक थे, जिन्होंने स्नातक, डिप्लोमा पाठ्यक्रम, स्नातकोत्तर, चार्टर्ड अकाउंटेंसी और पीएचडी की थी।

तालिका 4. संगति के माप

	ईटा	एटा स्केर्ड
रैनसमवेयर * शिक्षा	.155	.024
मेरी जानकारी के बिना मेरे डिवाइस के कैमरे/वेबकैम के माध्यम से देखा जाना * शिक्षा	.139	.019
सरकारी हस्तक्षेप * शिक्षा	.156	.024
आपके द्वारा देखी जाने वाली वेबसाइटों के साथ स्थान की जानकारी साझा की जा रही है * शिक्षा	.168	.028

शिक्षा के विभिन्न क्षेत्रों में उत्तरदाताओं के बीच मैलवेयर/गतिविधियों के विरुद्ध डेटा सुरक्षा में महत्वपूर्ण अंतर की जाँच करने के लिए आयोजित ANOVA परीक्षण के परिणाम दर्शाते हैं कि शिक्षा के विभिन्न क्षेत्रों में उत्तरदाताओं के बीच कोई महत्वपूर्ण अंतर नहीं है ($p > 0.05$)। इस प्रकार, हम निष्कर्ष निकालते हैं कि सभी उत्तरदाताओं में, शोधार्थी उत्तरदाताओं के बीच सुरक्षा जोखिम के प्रति चिंताएँ उन उत्तरदाताओं की तुलना में अधिक थीं, जिन्होंने HSC तक अपनी शिक्षा पूरी की थी, जिन्होंने स्नातक, डिप्लोमा पाठ्यक्रम, स्नातकोत्तर, चार्टर्ड अकाउंटेंसी और पीएचडी की थी।

अध्याय 5 निष्कर्ष

इस अंतिम अध्याय में पूरे शोध के प्रमुख निष्कर्षों को संक्षेप में प्रस्तुत किया गया है। इसमें यह बताया गया है कि भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा खतरे लगातार बढ़ रहे हैं और इनके प्रभाव व्यापक हैं। साथ ही, साइबर सुरक्षा को मजबूत करने के लिए आवश्यक उपायों, नीतिगत सुझावों और भविष्य के शोध की संभावनाओं पर भी प्रकाश डाला गया है। यह अध्याय शोध के समग्र निष्कर्ष और उसकी उपयोगिता को स्पष्ट करता है।

हमारा समाज एक साइबर-भौतिक समाज बन रहा है जो हमारे दैनिक जीवन के सभी पहलुओं में सूचना और संचार प्रौद्योगिकी (ICT) पर आधारित है, जिससे IT सुरक्षा की आवश्यकता मौलिक हो गई है। साइबर सुरक्षा की अमूर्त प्रकृति, सामाजिक-तकनीकी निर्भरता, साइबर सुरक्षा के खिलाफ लड़ाई का अस्पष्ट प्रभाव और विवादास्पद प्रकृति इसे उपयोगकर्ताओं के लिए एक उत्तेजक क्षेत्र बनाती है। साइबर सुरक्षा को अलग-अलग तरीकों से तैयार किया जा सकता है, जिसका लोगों पर अलग-अलग प्रभाव पड़ता है। साइबर सुरक्षा एक जटिल और बहुआयामी क्षेत्र है जिसका कोई स्पष्ट नायक या अपराधी नहीं है। साइबर सुरक्षा को तैयार करने में असमर्थता ने उचित कार्रवाई करना और पर्याप्त नीतियाँ विकसित करना असंभव बना दिया है। हालाँकि, साइबर युद्ध पहले से ही चल रहे हैं और नागरिकों और सरकारों को बेहतर तरीके से तैयार रहने की आवश्यकता है। भविष्य में साइबर सुरक्षा खतरों का पता लगाना अधिक कठिन होगा, जिससे संवेदनशील डेटा और सिस्टम की सुरक्षा करना अधिक कठिन हो जाएगा। किसी कंपनी की सुरक्षा के लिए प्रत्येक कर्मचारी के समर्थन की आवश्यकता होगी। अधिकतम प्रभावशीलता के लिए अनुकूलित चल रहे सुरक्षा जागरूकता कार्यक्रम के साथ, एक संगठन सभी कर्मियों द्वारा समर्थित साइबर सुरक्षा संस्कृति बना सकता है। जबकि कई उपयोगकर्ता ऑनलाइन वित्तीय और गैर-वित्तीय लेनदेन का उपयोग करते हैं, वे साइबर सुरक्षा नियमों से अनजान हैं। ऑनलाइन वित्तीय या गैर-वित्तीय लेनदेन करते समय उन्हें कई जोखिमों और चुनौतियों का सामना करना पड़ता है। उन्हें नहीं पता था कि ऑनलाइन वित्तीय और गैर-वित्तीय लेनदेन में कई सुरक्षा उपाय हैं

नीचे सूकाईबद्ध बिंदुओं में नए मुद्दे शामिल हैं जो सभी कर्मचारियों को प्रभावित कर सकते हैं, साथ ही चल रही चुनौतियाँ भी शामिल हैं जिन पर निरंतर ध्यान देने और शायद एक नए दृष्टिकोण की आवश्यकता है, क्योंकि वे अभी भी संगठनों के लिए समस्या बने हुए हैं।

- अधिक परिष्कृत फ़िशिंग हमलों और सामाजिक इंजीनियरिंग योजनाओं के लिए तैयारी। अनुशंसा: फ़िशिंग सिमुलेशन के साथ पता लगाएं कि कौन से उपयोगकर्ता फ़िशिंग हमलों और सामाजिक इंजीनियरिंग योजनाओं के अधीन हैं।
- उपयोगकर्ता नाम और पासवर्ड के लिए सर्वोत्तम प्रथाओं पर कर्मचारियों को शिक्षित करें। अनुशंसा: पासवर्ड और प्रमाणीकरण प्रशिक्षण और शिक्षा के लिए नए और अधिक प्रभावी दृष्टिकोण बनाने के लिए सुरक्षा जागरूकता क्षेत्र में भागीदारों के साथ काम करने पर विचार करें।
- GDPR (जनरल डेटा प्रोटेक्शन रेगुलेशन) के समान विनियमों के विस्तार की तैयारी। अनुशंसा: कर्मचारियों को व्यक्तिगत जानकारी की सुरक्षा के सर्वोत्तम तरीकों के बारे में शिक्षित करें।
- रैनसमवेयर की मूल बातें सिखाएँ। अनुशंसा: रैनसमवेयर जागरूकता कार्यक्रम बनाकर अपने संगठन की सुरक्षा करें।
- कर्मचारियों को सुरक्षा घटनाओं की सफलतापूर्वक रिपोर्ट करने के लिए प्रशिक्षित करें। अनुशंसा: उपयोगकर्ताओं की पहचान करें और वास्तविक समय में निगरानी करें कि क्या वे फ़िशिंग घोटाले की रिपोर्ट करते हैं।
- सुरक्षा पेशेवरों की कमी को दूर करें। अनुशंसा: फ़िशिंग या सुरक्षा जागरूकता को एक प्रबंधित सेवा के रूप में देखें

अध्ययन की सीमाएं:

- वर्तमान अध्ययन प्राथमिक आंकड़ों को प्राथमिकता देता है; इस शोध के विषयों में जनसंख्या के बड़े समूह के लिए बहुआयामी विशेषताएं शामिल हैं।
- चयनित क्षेत्र मुंबई, महाराष्ट्र, भारत में बांद्रा और कुर्ला क्षेत्र हैं। यह समय की कमी और कुछ मौद्रिक कारणों के कारण है।
- प्रश्नावली तैयार की गई है और उसी के आधार पर शोध किया गया है। प्रश्नावली में कुछ कारकों को शामिल नहीं किया गया है और नमूने यादृच्छिक आधार पर चुने गए हैं।

भावी अनुसंधान की संभावनाएँ:

अध्ययन से पता चलता है कि मात्रात्मक तरीकों का उद्देश्य साइबर सुरक्षा के बारे में जागरूकता पैदा करना है जिसके लिए भविष्य में उपयोग के लिए कुछ नियमों और विनियमों का पालन किया जाना चाहिए। व्यक्ति को हमेशा नियमों और विनियमों का पालन करना चाहिए। इस अध्ययन में

चुने गए वित्तीय और गैर-वित्तीय तरीके मुंबई क्षेत्र से संबंधित हैं। यह शोध अध्ययन आम लोगों को इंटरनेट सुरक्षा में मदद करेगा।

अनुशंसाएँ:

ऑनलाइन वित्तीय और गैर-वित्तीय लेनदेन करते समय सुरक्षा बनाए रखने के लिए यहां कुछ सुझाव दिए गए हैं।

- उन्नत एंटी-मैलवेयर प्रोग्राम का उपयोग करें: यह आपके कंप्यूटर और आपके द्वारा उपयोग किए जा रहे अन्य डिजिटल उपकरणों पर वर्गीकृत और अवर्गीकृत दोनों तरह के हमलों से सुरक्षा प्रदान करेगा। पुष्टि करें कि आपका एंटीमैलवेयर प्रोग्राम अपडेट है या इसका ऑटो अपडेट विकल्प "चालू" है। पुष्टि करें कि एंटीवायरस प्रोग्राम स्वचालित अपडेट के डेटाबेस में शामिल होने से पहले ही नए बनाए गए और उत्परिवर्तित मैलवेयर खतरों का पता लगाने की स्थिति में है।
- अपने डेस्कटॉप/लैपटॉप/मोबाइल में सुरक्षा कमज़ोरियों पर नज़र रखें: कई मैलवेयर प्रोग्राम ऑपरेटिंग सिस्टम और वेब ब्राउज़र में सुरक्षा कमज़ोरियों को नियंत्रित करने और आपके वित्तीय डेटा को चुराने के लिए डिज़ाइन किए गए हैं। आप सिस्टम मैकेनिक सुरक्षा ऑप्टिमाइज़र चलाएँगे, जो ऑनलाइन ब्राउज़र और OS दोनों में ऐसी कमज़ोरियों का पता लगा सकता है और उन्हें ठीक कर सकता है। अपने ब्राउज़र और OS को हमेशा नवीनतम रखें।
- सुनिश्चित करें कि आप सुरक्षित कनेक्शन का उपयोग कर रहे हैं: जब आप सुरक्षित कनेक्शन का उपयोग कर रहे होते हैं तो URL <https://> से शुरू होता है, लेकिन अन्य सभी मामलों में यह <http://> से शुरू होता है। इसलिए, सुनिश्चित करें कि आप [https](https://) का उपयोग कर रहे हैं।
- केवल प्रतिष्ठित वेबसाइटों से ही लेन-देन करें: जब तक आप इसके बारे में न जानते हों, तब तक किसी भी वेबसाइट पर सीधे भुगतान न करें। PayTabs जैसे भुगतान प्रोसेसर में उपयोग किए जाने वाले उन्नत सुरक्षा उपाय आपकी वित्तीय जानकारी को गलत हाथों में जाने से रोकेंगे। PayTabs का उपयोग करना संदिग्ध वेबसाइटों और ऑनलाइन बदमाशों से सुरक्षित रहने का सबसे अच्छा तरीका है। Paytas द्वारा नियोजित उन्नत सुरक्षा उपाय यह सुनिश्चित करेंगे कि आपकी गोपनीय वित्तीय जानकारी सुरक्षित है और इसके लीक होने की कोई संभावना नहीं है।
- ऑनलाइन शॉपिंग के लिए मास्टर कार्ड का उपयोग करें: सभी ऑनलाइन शॉपर्स के लिए सावधानी बरतने की बात है। सुनिश्चित करें कि आप ऑनलाइन शॉपिंग क्रेडिट कार्ड का उपयोग

करके कर रहे हैं न कि ओपन-एंड क्रेडिट का। ओपन-एंड क्रेडिट का उपयोग करना बेहद जोखिम भरा है क्योंकि यह आपके चेकिंग अकाउंट से जुड़ा होता है। खर्च सीमा के साथ, क्रेडिट कार्ड का दुरुपयोग ओपन-एंड क्रेडिट की तरह नहीं किया जा सकता है। ओपन-एंड क्रेडिट से निकाले गए पैसे को वापस पाने की तुलना में मास्टरकार्ड पर धोखाधड़ी के आरोपों पर विवाद करना बहुत आसान है। इन दिनों, एक बार इस्तेमाल होने वाले क्रेडिट कार्ड भी प्रचलन में हैं। ये कार्ड खास तौर पर ऑनलाइन शॉपिंग के लिए डिज़ाइन किए गए हैं।

- सार्वजनिक कंप्यूटर का उपयोग न करें: ऑनलाइन लेनदेन के दौरान सुरक्षा का ध्यान रखने के लिए, सुनिश्चित करें कि आप अपना खुद का कंप्यूटर या मोबाइल डिवाइस इस्तेमाल कर रहे हैं। सार्वजनिक पुस्तकालयों या इंटरनेट कैफ़े में स्थापित कंप्यूटर का उपयोग न करें, क्योंकि इन कंप्यूटरों के हार्डवेयर या सॉफ़्टवेयर में बदलाव करके आसानी से छेड़छाड़ की जा सकती है।

- एक मजबूत और परिष्कृत पासवर्ड सेट करें: सामान्य पासवर्ड या ऐसे पासवर्ड का उपयोग न करें जिसका आसानी से अनुमान लगाया जा सके। अल्फ़ान्यूमेरिक और विशेष वर्णों के मिश्रण का उपयोग करें और सुनिश्चित करें कि पासवर्ड की लंबाई 6 अंकों से अधिक हो।

- फ़िशिंग साइट्स से सावधान रहें: फ़िशिंग साइट्स लगभग असली साइट्स जैसी ही होती हैं। नकली लिंक आपको फ़िशिंग साइट्स के संपर्क में ले जाते हैं। URL (वेब एड्रेस) को गलत टाइप करने से भी आप फ़िशिंग साइट पर पहुँच सकते हैं। भुगतान करते समय ऐसा करने से पहले URL की जाँच करें। इस तरह की फ़िशिंग साइट्स आपकी संवेदनशील जानकारी जैसे मास्टरकार्ड विवरण, पासवर्ड आदि प्राप्त करती हैं। अगर आपको लगता है कि लिंक संदिग्ध है, तो उसे कॉपी करके दूसरे टैब में पेस्ट करें, यह फ़िशिंग साइट्स को देखने के तरीकों में से एक है।

- अपने खुद के पर्सनल कंप्यूटर का इस्तेमाल करें दूसरों के कंप्यूटर या स्मार्टफोन का इस्तेमाल करने से बचें: आपके द्वारा दर्ज की गई सारी जानकारी, आपके द्वारा सर्फ की गई साइट्स (यूआरएल), यूज़रनेम, पासवर्ड जैसी जानकारी ब्राउज़र की कुकीज़ में संग्रहीत होती है। ऐसे कारणों से सार्वजनिक मशीनों या दूसरों के कंप्यूटर का इस्तेमाल करने से बचें। हमेशा उन साइट्स से लॉगआउट करें जहाँ आप अपनी लॉगिन जानकारी और अन्य टिप्स दर्ज करते हैं। साइट्स को बंद न करें।

- गोपनीय जानकारी मांगने वाले फ़िशिंग ईमेल को न खोलें या क्लिक न करें: हमें एक दिन में बहुत ज़्यादा मेल मिलते हैं। हमारा मेल बॉक्स संदेशों से भरा हुआ है। बैंकों, थर्ड पार्टी वेबसाइट

या किसी अनजान व्यक्ति से आने वाले मार्केटिंग मेल या प्रमोशनल मेल को खोलने से बचना बेहतर है। मेल में दिए गए किसी भी लिंक पर क्लिक न करें। साथ ही, ऑफ़र, लॉटरी पुरस्कार, पुरस्कार जीतने आदि के लालच में आकर मेल पर मांगी गई कोई भी जानकारी साझा न करें। वे स्पैम होंगे। हैकर्स भी लगभग आपकी तरह ही फ़िशिंग ईमेल आईडी बनाते हैं। अगर आपके ईमेल से छेड़छाड़ की गई है जिसमें चेकिंग अकाउंट नंबर में भुगतान लेनदेन के बारे में उल्लेख किया गया है, तो यह लगभग ग्राहक के खाते की तरह लग सकता है जो आपसे खाते में भुगतान स्थानांतरित करने के लिए कह रहा है। कृपया ऐसा कोई भी लेनदेन करने से पहले पुष्टि करें। मैंने बहुत से मासूम लोगों को ऐसी फ़िशिंग वेबसाइट और ईमेल में फंसते हुए देखा है।

- ऑनलाइन लेनदेन करते समय सार्वजनिक वाई-फाई का उपयोग न करें: हमेशा सुरक्षित रहें, अपने वाई-फाई पासवर्ड को सुरक्षित रखें। ऑनलाइन लेनदेन करते समय सार्वजनिक या अन्य वाई-फाई का उपयोग न करें, ऐसा करना असुरक्षित है।
- नवीनतम सुरक्षा सॉफ़्टवेयर स्थापित करें: अपनी मशीन पर आधुनिक सुरक्षा सॉफ़्टवेयर स्थापित करें। सप्ताह में एक बार अपनी मशीन को स्कैन करना सुनिश्चित करें और समय-समय पर अपने एंटीवायरस को अपडेट करते रहें। जब आप किसी साइट पर जाते हैं या नेट से कुछ डाउनलोड करते हैं तो आपकी जानकारी के बिना कुछ हानिकारक सॉफ़्टवेयर आपकी मशीन पर डाउनलोड हो सकते हैं। अपने फ़ायरवॉल को हमेशा चालू रखें। एंटीवायरस अपडेट करने के अलावा अपने ओएस और ब्राउज़र को अपडेट रखना भी अनुशंसित है ताकि सुरक्षा सुविधाओं को अपडेट रखा जा सके।
- कठिन और अलग-अलग पासवर्ड का इस्तेमाल करें: हम आमतौर पर अलग-अलग साइट्स के लिए एक ही पासवर्ड का इस्तेमाल करते हैं ताकि उसे याद रखना आसान हो जाए। लेकिन अगर हैकर्स को आपका पासवर्ड पता चल जाता है तो उनके लिए आपकी किसी भी बैंकिंग साइट, ई-कॉमर्स साइट, ईमेल अकाउंट और दूसरे महत्वपूर्ण अकाउंट में सेंध लगाना आसान हो जाता है। साथ ही, अल्फाबेट, कैरेक्टर और स्पेशल कैरेक्टर के कॉम्बिनेशन वाले कठिन पासवर्ड का इस्तेमाल करें। अपने और अपने प्रियजनों के पूरे नाम, जन्मदिन को पासवर्ड के तौर पर इस्तेमाल करने से बचें क्योंकि हम सोशल साइट्स पर यह जानकारी शेयर करते हैं और हैकर्स के लिए आपका पासवर्ड अनुमान लगाना आसान हो जाता है।
- अपने भौतिक कीबोर्ड के बजाय वर्चुअल कीबोर्ड का उपयोग करें: यदि आपकी मशीन मैलवेयर से संक्रमित है तो आपके कीबोर्ड के साथ छेड़छाड़ होने की संभावना है? ऐसे मामलों में मैलवेयर प्रोग्राम जैसे कि "स्पाईवेयर" जो कीबोर्ड पर टाइप करते समय कुंजियों का पता लगाते

हैं और आपका पासवर्ड हैक कर सकते हैं। जबकि वर्चुअल कीबोर्ड सुरक्षा उद्देश्य के लिए डिज़ाइन किए गए हैं जो ऑनलाइन लेनदेन करते समय सुरक्षित और संरक्षित हैं।

- लेन-देन के दौरान OTP का उपयोग करें: जब आप क्रेडिट या ओपन-एंड क्रेडिट का उपयोग करके भुगतान करते हैं, तो बैंक सुरक्षित पिन (व्यक्तिगत पहचान संख्या) या OTP (वन-टाइम पासवर्ड) के लिए अनुरोध करते हैं। हमेशा पिन के बजाय OTP चुनें यह एक सुरक्षित विकल्प है क्योंकि जब भी बैंक द्वारा एक नया छह अंकों का नंबर जनरेट किया जाता है और आपका पंजीकृत मोबाइल नंबर भेजा जाता है।
- प्रतिष्ठित व्यापारियों से खरीदें: हमेशा प्रतिष्ठित साइटों और ई-कॉमर्स प्लेटफ़ॉर्म से खरीदारी करें। बड़ी कंपनियाँ साइट की सुरक्षा और भुगतान गेटवे पर समझौता नहीं करेंगी। छोटे विक्रेता सुरक्षा पर ज़्यादा खर्च नहीं कर सकते हैं, इससे आपकी महत्वपूर्ण जानकारी जैसे क्रेडिट/ओपन-एंड क्रेडिट विवरण, बैंक विवरण, उपयोगकर्ता नाम, पासवर्ड आदि के साथ समझौता हो सकता है।
- टेलीफोन या ईमेल पर किसी से भी गोपनीय जानकारी साझा न करें: बैंक और अन्य वित्तीय सेवा कंपनी से धोखेबाज़ों द्वारा की जाने वाली फ़र्जी कॉल आपके विवरण के लिए वास्तविक साबित हो सकती हैं। CVV जैसी जानकारी कभी भी साझा न करें
- , समाप्ति तिथियाँ, उपयोगकर्ता नाम, टेलीफोन या ईमेल पर पासवर्ड। कोई भी कंपनी या बैंक ऐसी जानकारी नहीं मांगता। वे सत्यापन के उद्देश्य से कार्ड नंबर, आरंभ तिथि, DOB जैसी जानकारी मांगेंगे।

संदर्भ

1. “कॉसमॉस बैंक का सर्वर हैक, 2 दिन में 94 करोड़ रुपये उड़ाए गए,” लाइव मिनट, 2018।
2. “साइबर सुरक्षा: खतरे, कारण, चुनौतियाँ, कार्यप्रणाली और औद्योगिक अनुप्रयोगों के लिए अत्याधुनिक समाधान,” स्कूल ऑफ इलेक्ट्रिकल इंजीनियरिंग और कंप्यूटर साइंस (एसईईसीएस) नेशनल यूनिवर्सिटी ऑफ साइंसेज एंड टेक्नोलॉजी, इस्लामाबाद, पाकिस्तान, 2019।
3. अंतर्राष्ट्रीय मुद्रा कोष (आईएमएफ), 2020, एक ऐसा संकट जैसा कोई और नहीं, एक अनिश्चित रिकवरी, देखा गया, <https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEO-अपडेट-जून-2020>।
4. अकेलो, बर्नार्ड. (2023). संगठनात्मक सूचना सुरक्षा खतरे: स्थिति और चुनौतियाँ. वर्ल्ड जर्नल ऑफ़ एडवांस्ड इंजीनियरिंग टेक्नोलॉजी एंड साइंसेज. 11. 148–162. 10.30574/wjaets.2024.11.1.0152.
5. अतुल, पीएचडी, बामरारा और सिंह, गजेंद्र और भट्ट, ममता। (2013)। भारत में साइबर हमले और बचाव रणनीतियाँ: बैंकिंग क्षेत्र का एक अनुभवजन्य मूल्यांकन। साइबर अपराध विज्ञान का अंतर्राष्ट्रीय जर्नल। 7. 49-61। 10.2139/ssrn.2488413।
6. अन्वेषा चक्रवर्ती (2024), “भारतीय बैंकिंग क्षेत्र में साइबर सुरक्षा खतरे और निवारक उपाय के रूप में एआई का कार्यान्वयन,” www.ijcspub.org © 2024 ijcspub | खंड 14, अंक 4 दिसंबर 2024 | आईएसएसएन: 2250-1770
7. अफ़ज़ल, मोहम्मद और अहमद, नसीम और अंसारी, शमीम. (2024). भारत में ई-बैंकिंग उपयोगकर्ताओं के उपयोग के इरादे पर साइबर धोखाधड़ी और साइबर सुरक्षा जागरूकता का प्रभाव. 10.1201/9781003542506-25.
8. अल-दोसारी, के., फ़ेतैस, एन., और कुकुकवर, एम. (2022)। बैंकिंग उद्योग के लिए आर्टिफिशियल इंटेलिजेंस और साइबर डिफेंस सिस्टम: एआई अनुप्रयोगों और चुनौतियों का एक गुणात्मक अध्ययन। साइबरनेटिक्स और सिस्टम, 55(2), 302–330।
9. अल-दोसारी, के., फ़ेतैस, एन., और कुकुकवर, एम. (2022)। बैंकिंग उद्योग के लिए आर्टिफिशियल इंटेलिजेंस और साइबर डिफेंस सिस्टम: एआई अनुप्रयोगों और चुनौतियों का एक गुणात्मक अध्ययन। साइबरनेटिक्स और सिस्टम, 55(2), 302–330। <https://doi.org/10.1080/01969722.2022.2112539>

10. अलबेनजसिम, एस., दरगाही, टी., तकरुरी, एच., और अल-जैदी, आर. (2023)। फिनटेक साइबर सुरक्षा चुनौतियां और विनियम: बहरीन केस स्टडी। जर्नल ऑफ कंप्यूटर इंफॉर्मेशन सिस्टम, 1-17।
11. अलसैफ़, उमर और शहाथा, अमर. (2024). साइबर सुरक्षा खतरों के लिए दृष्टिकोण और कठिनाइयों का एक व्यापक विश्लेषण- लेख समीक्षा. मुस्तनसिरिया जर्नल ऑफ़ प्योर एंड एप्लाइड साइंसेज. 2. 126-139. 10.47831/mjpas. v2i4.164.
12. अहमद, अदी और मौलाना, रियान और यासिर, मुहम्मद। (2024)। डिजिटल परिवर्तन के युग में साइबर सुरक्षा चुनौतियाँ सूचना प्रणालियों का एक व्यापक विश्लेषण। जर्नल इंफॉर्मेटिक, एजुकेशन एंड मैनेजमेंट (जेआईईएम)। 6. 7-11. 10.61992/jiem. v6i1.57.
13. आई. मुगारी, एस. गोना, एम. मौगा, और आर. चियाम्बिरो, "साइबर अपराध - जिम्बाब्वे में वित्तीय सेवा क्षेत्र के लिए उभरता खतरा," मेडिटेरे. जे. सोक. साइंस., खंड 7, संख्या 3, पृष्ठ 135-143, 2016,
14. आर. राघवन और एल. पार्थिवन, "बैंक के वित्त पर साइबर अपराध का प्रभाव," अंतर्राष्ट्रीय जे. करेंट रिसर्च एकेडमिस्टिक रिव्यू, खंड 2, संख्या 2, पृष्ठ 173-178, 2014,
15. आरबीआई, "रिज़र्व बैंक के खाते," 2019. [ऑनलाइन]. उपलब्ध: <https://m.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1267>.
16. इकबाल, साद और नवाज, दानिश। (2024)। साइबर सुरक्षा में उभरते रुझान और भविष्य की चुनौतियाँ: एक व्यापक समीक्षा।
17. इब्राहिम, अब्दुल्ला. (2025). वित्तीय क्षेत्र में साइबर सुरक्षा खतरे: रुझान और शमन रणनीतियाँ. 10.5281/zenodo.15387211.
18. ए. लक्ष्मणन, "साइबर अपराध और इसकी रोकथाम तंत्र पर साहित्य समीक्षा," फरवरी, पृ. 1-5, 2019,
19. ए. सरवडे, एन; भल्ला, "साइबर सुरक्षा में उभरते रुझान और चुनौतियाँ _ रिज़र्व बैंक सूचना प्रौद्योगिकी प्राइवेट लिमिटेड (रीबिट)।" 2018,
20. एंटोनी बाउवेरेट, "वित्तीय क्षेत्र के लिए साइबर जोखिम: मात्रात्मक मूल्यांकन के लिए एक रूपरेखा," विक्रम हक्सर द्वारा वितरण के लिए अधिकृत।, आईएमएफ वर्किंग पेपर रणनीति, नीति और समीक्षा विभाग, 27 मई, 2019।

21. एज़े, वैल और उग्वू, चिनयेरे और उग्वुआनी, इफियानी। (2023)। साइबर सुरक्षा खतरों का एक अध्ययन, विभिन्न क्षेत्रों में चुनौतियाँ और इसके संभावित समाधान: एक समीक्षा। 9. 13-24।
22. एम. मनीषा, जेएम पी, और एनकेएम, "ऑनलाइन बैंकिंग और साइबर हमलों में उन्नत अनुसंधान का अंतर्राष्ट्रीय जर्नल: वर्तमान परिदृश्य," अंतर्राष्ट्रीय जर्नल ऑफ एडवांस्ड रिसर्च, कम्प्यूटिंग, विज्ञान, सॉफ्टवेयर इंजीनियरिंग, खंड 5, संख्या 12, पृष्ठ 743-749, 2015,
23. एल. अली, एफ. अली, पी. सुरेन्द्रन, और बी. थॉमस, "ई-बैंकिंग सेवाओं में ग्राहक के व्यवहार पर साइबर खतरों का प्रभाव," अंतर्राष्ट्रीय जर्नल ई-शिक्षा, ई-बिजनेस, ई-प्रबंधन ई-लर्निंग, खंड 7, संख्या 1, पृष्ठ 70-78, 2017,
24. एस. तंवर, टी. पॉल, के. सिंह, एम. जोशी और ए. राणा, "भारत में साइबर खतरों का वर्गीकरण और प्रभाव: एक समीक्षा," 2020 8वां अंतर्राष्ट्रीय सम्मेलन विश्वसनीयता, इन्फोकॉम प्रौद्योगिकी और अनुकूलन (रुझान और भविष्य की दिशाएं) (आईसीआरआईटीओ), नोएडा, भारत, 2020, पृष्ठ 129-135,
25. ओ. कोलेस्निकोव, "कॉसमॉस बैंक स्विफ्ट / एटीएम यूएस \$ 13. 5 हमले का पता लगाना सुरक्षा का उपयोग करना," 2018।
26. ओनुमादु, पी.; अब्रोशन, एच. भुगतान लेनदेन में निकट-क्षेत्र संचार (एनएफसी) साइबर खतरे और शमन समाधान: एक समीक्षा। सेंसर 2024, 24, 7423. <https://doi.org/10.3390/s24237423>
27. कांत, डॉ. (2024). भारतीय बैंकों के सामने साइबर सुरक्षा के मुद्दों पर एक व्यवस्थित अध्ययन। 10.58532/nbennurch42.
28. कोवासेविक, एना और राडेनकोविक, सोंजा और निकोलिक, ड्रैगाना। (2024)। बैंकिंग क्षेत्र में कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा: अवसर और जोखिम। 10.48550/arxiv.2412.04495.
29. कौसर, शबाना और सिंध, जमशोरो और अली, पाकिस्तान और रजा लघारी, अली और जमशोरो, सिंध और पाकिस्तान, सिंध और इफ्तिखार, एरम और कौसर, शबाना। (2023)। साइबर सुरक्षा चुनौतियों और समाधानों का विश्लेषण। जर्नल ऑफ पॉजिटिव स्कूल साइकोलॉजी। 7. 163-171।

30. क्लैपर, डी. सिंगर, एस. अंसार, और जे. हेस, “असली डेमिरगुक-कुंट ग्लोबल फ़ाइनडेक्स डेटाबेस वित्तीय समावेशन और फ़िनटेक क्रांति 2017 को मापता है।” 2017,
31. ख्यात, जूनी और बोरसे, योगेश. (2025). भारतीय बैंकिंग और वित्तीय क्षेत्रों के लिए सुरक्षा चुनौतियाँ कैप्टन डॉ. योगेश सुभाषचंद्र बोरसे सहायक प्रोफेसर, रक्षा और सामरिक अध्ययन विभाग, मूलजी जैथा कॉलेज, जलगांव, महाराष्ट्र. जूनी ख्यात जर्नल. 13. 75-84.
32. गाडे, निखिता रेड्डी और रेड्डी, युगांडर (2014)। नवीनतम तकनीकों पर साइबर सुरक्षा चुनौतियों और इसके उभरते रुझानों का एक अध्ययन।
33. गोनी, अशरफ़ुल और जहाँगीर, मोहम्मद उमर और रॉय चौधरी, राजर्षि। (2024)। साइबर सुरक्षा पर एक अध्ययन: वर्तमान खतरों का विश्लेषण, जटिलताओं को समझना और रोकथाम रणनीतियों को लागू करना। इंटरनेशनल जर्नल ऑफ़ रिसर्च एंड साइंटिफिक इनोवेशन। X. 507-522. 10.51244/IJRSI.2023.1012039।
34. गोम्स, लिंड्रे और देशमुख, अभिनव और अनुते, नीलेश। (2022)। साइबर सुरक्षा और इंटरनेट बैंकिंग: मुद्दे और निवारक उपाय। जर्नल ऑफ़ इन्फॉर्मेशन टेक्नोलॉजी एंड साइंसेज। 8. 31-42. 10.46610/जोर्दे। 2022.v08i02.005।
35. गोराई, संजय और बेरा, सुमित और कुमार, महेश्वर। (2025)। भारत में साइबर सुरक्षा के मुद्दे और चुनौतियाँ। कंप्यूटर विज्ञान, इंजीनियरिंग और सूचना प्रौद्योगिकी में वैज्ञानिक अनुसंधान के अंतर्राष्ट्रीय जर्नल। 11. 159-166। 10.32628/CSEIT251112।
36. गोविंदराज, योगानंदम. (2024). भारत के बैंकिंग और वित्तीय क्षेत्र में समकालीन साइबर अपराध अर्थव्यवस्था: आर्थिक विकास और ग्राहक संबंधों के लिए खतरे, रणनीति और निहितार्थ - एक आकलन. 08. 632-647.
37. चड्ढा, प्रियंका और बनर्जी, सोनाली और उप्पल, अर्हिता और राणा, कनिका। (2024)। बैंकिंग में साइबर सुरक्षा के सार को उजागर करना: वित्तीय अखंडता को बनाए रखना और विश्वास का निर्माण करना। बैंकिंग, जोखिम और बीमा का अंतर्राष्ट्रीय जर्नल। 12. 17-29. 10.21863/ijbri/2024.12.sp.iss.003।
38. चेक प्वाइंट सॉफ्टवेयर टेक्नोलॉजीज लिमिटेड, “चेक प्वाइंट रिसर्च: क्षेत्रवार साइबर हमले की श्रेणियाँ H1 2020।”
39. जुआन कार्लोस क्रिसेंटो, जेरेमी प्रीनियो, “बैंकों के साइबर-सुरक्षा ढांचे को बढ़ाने के लिए नियामक दृष्टिकोण” वित्तीय स्थिरता संस्थान, एसबीएन 978-92-9259-080-2: अगस्त 2017।

40. जुयाल, तेजस और थपलियाल, सिद्धांत और गर्ग, नेहा और सिंह, दर्शन। (2023)। भारत में साइबर सुरक्षा और इसकी चुनौतियों पर एक अध्ययन। 10.1007/978-981-99-3761-5_15.
41. ज़ेबारी, दिलोवन और असद, रेनास। (2022)। साइबर सुरक्षा खतरे, भेद्यता, चुनौतियाँ और प्रस्तावित समाधान। एप्लाइड कंप्यूटिंग जर्नल। 227-244। 10.52098/acj.202260।
42. जैन, सात्विक और सिन्हा, शिवांगी (2024)। इंटरनेशनल जर्नल ऑफ एडवांस्ड लीगल रिसर्च साइबर सिक्योरिटी थ्रेट इन डिजिटल बैंकिंग सेक्टर।
43. जोएल चिगाडा। रूजेको मैडज़िंगा, "कोविड-19 के दौरान साइबर हमले और खतरे: एक व्यवस्थित साहित्य समीक्षा, साउथ अफ्रीकन जर्नल ऑफ इंफॉर्मेशन मैनेज
44. डी. स्टियावान, एमवाई इदरीस, एएच अब्दुल्ला, एफ. अलजाबेर, और आर. बुडियार्टो, "साइबर हमले की पैठ परीक्षण और भेद्यता विश्लेषण," अंतर्राष्ट्रीय जर्नल ऑफ ऑनलाइन इंजीनियरिंग, खंड 13, संख्या 1, पृष्ठ 125-132, 2017,
45. डी.वी. सारस्वत, "साइबर सुरक्षा," 2003. doi: 10.1016/j.techsoc.2003.09.022. एस. गोयल, "साइबर अपराध: भारतीय बैंकिंग क्षेत्र के लिए बढ़ता खतरा," तीसरा अंतर्राष्ट्रीय सम्मेलन, हाल ही में नवाचार विज्ञान प्रौद्योगिकी प्रबंधन पर्यावरण, खंड 2016, पृष्ठ 13-20, 2016,
46. डेलॉन, एल. (2024) वाणिज्यिक बैंकिंग संस्थानों में जोखिम प्रबंधन: भारत में वाणिज्यिक बैंकों के लिए साइबर सुरक्षा चुनौतियों की जांच: गुयाना के बैंकिंग क्षेत्र के लिए सिफारिशें। जर्नल ऑफ फाइनेंशियल रिस्क मैनेजमेंट, 13, 549-575।
डोई:10.4236/jfrm.2024.133026.
47. डॉ. सविता एस. पाटिल (2025), "भारतीय बैंकिंग क्षेत्र में साइबर सुरक्षा व्यवधान अवसर और चुनौतियां," © 2025 जेटिर मार्च 2025, खंड 12, अंक 3 www.jetir.org (issn-2349-5162)
48. तनवीर फातिमा नाइक बुख्त, मुहम्मद अहसन रज़ा, जवाद हुसैन अवान, रिज़वान अहमद4, "पाकिस्तान के बैंकों और उनके समाधानों पर लक्षित साइबर हमलों का विश्लेषण," आईजेसीएसएनएस इंटरनेशनल जर्नल ऑफ़ कंप्यूटर साइंस एंड नेटवर्क सिक्योरिटी, वॉल्यूम.20 नंबर 2, फ़रवरी 2020।
49. तारिक शहाब (2021), "भारतीय बैंकिंग क्षेत्र में साइबर सुरक्षा चुनौतियां," इंटरनेशनल जर्नल इन मैनेजमेंट एंड सोशल साइंस वॉल्यूम 09 अंक 11, नवंबर 2021 आईएसएसएन:

2321-1784 प्रभाव कारक: 7.088 जर्नल होमपेज: <http://ijmr.net.in>, ईमेल: irjmss@gmail.com

50. दास, सुलग्रा और गांगुली, देवराज. (2024). अपनी संपत्तियों की सुरक्षा: बैंकिंग उद्योगों में साइबर सुरक्षा उपायों का प्रभावी उपयोग. 10.1007/978-981-97-1249-6_12.
51. नाहिद जोवेदा, एमडी तारेक खान² और अभिजीत पाठक "साइबर लॉन्ड्रिंग: बांग्लादेश में बैंकिंग उद्योगों के लिए खतरा: प्रभावी कानूनी ढांचे और वित्तीय जानकारी की साइबर सुरक्षा की तलाश में," इंटरनेशनल जर्नल ऑफ इकोनॉमिक्स एंड फाइनेंस; खंड 11, संख्या 10; 2019
52. परिता कौशिक भाई घाघड़ा (2024), "भारतीय बैंकिंग प्रणाली पर फिनटेक के प्रभावों पर एक अध्ययन," इंजीनियरिंग प्रौद्योगिकी और विज्ञान में आधुनिकीकरण के अंतर्राष्ट्रीय शोध जर्नल (सहकर्मी-समीक्षित, खुली पहुंच, पूरी तरह से रेफरी अंतरराष्ट्रीय जर्नल) वॉल्यूम: 06 / अंक: 04 / अप्रैल -2024 प्रभाव कारक- 7.868 www.irjmets.com
53. पेट्टु-क्रिस्टियन, नेग्रेया। (2023)। उच्च प्रभाव वाली साइबर सुरक्षा घटनाओं का व्यापक विश्लेषण: केस स्टडीज़ और निहितार्थ। 10.13140/RG.2.2.17461.65763।
54. पेट्रोव, के.; निकोलोव, ए.; मिहैलोव, ए. ग्रे कास्ट आयरन (en-gj1-250) के साथ सिलिका सैंड मोल्ड में गुरुत्वाकर्षण भरने का अनुकरण। इंजी. प्रोक. 2025, 100, 1. <https://doi.org/10.3390/engproc2025100001>
55. पॉल, सुभ्रा और घोष, दीपायन और नजमुल आलम, मोहम्मद। (2024)। वित्तीय किले मजबूत करना: भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा के लिए एक व्यापक मार्गदर्शिका।
56. प्रभाकर, एस. भारत में डिजिटल बैंकिंग के रुझान, अवसर और चुनौतियाँ: एक समीक्षा।
57. फराजी, एमआर, शिकदर, एफ., हसन, एमएच, इस्लाम, एमएम, और अक्तर, यूके (2024)। साइबर सुरक्षा (सीएस) में कृत्रिम बुद्धिमत्ता की भूमिका की जांच: वित्तीय लेनदेन में संभावित समाधानों को रोकने के लिए एक व्यवस्थित समीक्षा। इंटरनेशनल जर्नल, 5(10), 4766-4782।
58. फिशर, ई.ए. (2015). साइबर सुरक्षा मुद्दे और चुनौतियाँ: संक्षेप में।
59. फैमिलोनी, एनबीटी, और शोएटन, एनपीओ (2024)। वित्तीय क्षेत्र में साइबर सुरक्षा: यूएसए और नाइजीरिया का तुलनात्मक विश्लेषण। कंप्यूटर साइंस और आईटी रिसर्च जर्नल, 5(4), 850–877

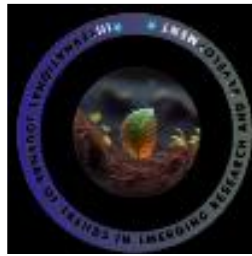
60. बामरारा, ए., सिंह, जी., और भट्ट, एम. (2013)। भारत में साइबर हमले और बचाव रणनीतियाँ: बैंकिंग क्षेत्र का एक अनुभवजन्य मूल्यांकन। एसएसआरएन इलेक्ट्रॉनिक जर्नल <https://doi.org/10.2139/ssrn.2488413>
61. बात्सम, डब्ल्यू. और डिक्सन, डी., 2020, 'कोविड-19 किस तरह साइबर गरीबी अंतर को दूर करने की तत्काल आवश्यकता को दर्शाता है', विश्व आर्थिक मंच साइबर सुरक्षा, 09 मई 2020 को देखा गया,
62. बी. स्टैंडर्ड, "बैंक साइबर खतरों के प्रति सबसे अधिक संवेदनशील हैं_ सरकारी अधिकारी_ बिजनेस स्टैंडर्ड न्यूज़।" बिजनेस स्टैंडर्ड लिमिटेड, मुंबई, पृ. 2-10, 2019,
63. बोरगावे, सचिन और कलकर, पराग और शाह, भूपाली। (2022)। ऑनलाइन बैंकिंग और ऑनलाइन लेनदेन में साइबर सुरक्षा मुद्दों की समीक्षा। न्यूरोकांटोलॉजी। 20. 405-418। 10.14704/nq.2022.20.6. nq88037।
64. भट्टाचार्य, सौरभ. (2024)। भारतीय बैंकिंग उद्योग में साइबर सुरक्षा बढ़ाना। संवाद. 28. 1-6. 10.53739/संवाद/2024/v28/173776.
65. भारद्वाज, शशांक. (2023). साइबर अपराध: भारतीय बैंकिंग क्षेत्र के लिए एक निरंतर खतरा. 10.48001/978-81-966500-9-4_19.
66. भुजंगाराव नायडू, पैचा। (2024)। ऑनलाइन बैंकिंग और लेनदेन को प्रभावित करने वाले साइबर सुरक्षा मुद्दों पर एक अध्ययन। शिक्षा में उन्नत अनुसंधान और नवीन विचारों का अंतर्राष्ट्रीय जर्नल। 9. 2023।
67. मधुमिता, एस. और वैष्णवी, सुश्री. (2025)। साइबर सुरक्षा का उपयोग करते हुए बैंकिंग सुरक्षा प्रणाली। कंप्यूटर विज्ञान, इंजीनियरिंग और सूचना प्रौद्योगिकी में वैज्ञानिक अनुसंधान का अंतर्राष्ट्रीय जर्नल। 11. 1184-1190. 10.32628/cseit25112451.
68. मलिक, एम.एस., और इस्लाम, यू. (2019)। साइबर अपराध: पाकिस्तान के बैंकिंग क्षेत्र के लिए एक उभरता खतरा। जर्नल ऑफ फाइनेंशियल क्राइम, 26(1), 50-60।
69. महतो, सुशील और साह, रंजीत और सपकोटा, सुशील। (2024)। साइबर सुरक्षा चुनौतियाँ और खतरे: डिजिटल दुनिया में जोखिम। विज्ञान, संचार और प्रौद्योगिकी में उन्नत अनुसंधान के अंतर्राष्ट्रीय जर्नल। 651-655। 10.48175/IJARSCT-22497।
70. माझी, डॉ. (2022). भारत में बैंकिंग क्षेत्र में साइबर अपराध: एक महत्वपूर्ण विश्लेषण. 10.55662/book.2022ccrs.001.

71. मानसी सुतार (2022), “कोविड-19 महामारी के दौरान बैंकिंग क्षेत्र में साइबर सुरक्षा खतरे की समीक्षा,” विज्ञान, संचार और प्रौद्योगिकी में उन्नत अनुसंधान के अंतर्राष्ट्रीय जर्नल (आईजेआरएससीटी) खंड 2, अंक 2, जून 2022
72. मुंधे, ई. (2024). भारतीय बैंकिंग क्षेत्र में डिजिटल परिवर्तन: अवसर और चुनौतियाँ। विभिन्न विषयों में ज्ञान का विकास-समकालीन रुझान और अग्रगामी नवाचार, 103.
73. मूंदड़ा, आदर्श. (2024). भारत में बैंकिंग संस्थानों पर साइबर हमलों का प्रभाव: सुरक्षा तंत्र और निवारक उपायों का एक अध्ययन. शालैक्स इंटरनेशनल जर्नल ऑफ मैनेजमेंट. 11. 142-148. 10.34293/management.v11i1-mar.8070.
74. मूंदड़ा, आदर्श। “भारत में बैंकिंग संस्थानों पर साइबर हमलों का प्रभाव: सुरक्षा तंत्र और निवारक उपायों का एक अध्ययन।” शालैक्स इंटरनेशनल जर्नल ऑफ मैनेजमेंट, खंड 11, संख्या S1, 2024, पृष्ठ 142-48।
75. मोहपात्रा, “भारतीय बैंकों में प्रभावी परिचालन जोखिम प्रबंधन साइबर सुरक्षा भेद्यता,” साइबरसिक्योरिटी फ्रेमवर्क बैंक, 2016,
76. रज्जाक, अब्दुल और हूर, अली और अहमद, हाफिज और मसूद, मुदस्सर। (2013)। साइबर सुरक्षा: खतरे, कारण, चुनौतियाँ, कार्यप्रणाली और औद्योगिक अनुप्रयोगों के लिए अत्याधुनिक समाधान। स्वायत्त विकेंद्रीकृत प्रणालियों पर IEEE 7वीं अंतर्राष्ट्रीय संगोष्ठी (ISADS'2013) की कार्यवाही: 6-8 मार्च, 2013। 1-6। 10.1109/ISADS.2013.6513420।
77. राधिका केजी (2024), “भारतीय बैंकिंग क्षेत्र में कृत्रिम बुद्धिमत्ता: एक अवलोकन,” एमएसएनआईएम प्रबंधन समीक्षा खंड 2 (2) द्वि-वार्षिक पत्रिका जुलाई – दिसंबर 2024
78. राय, डॉ. (2023). भारत में वित्तीय प्रौद्योगिकी और साइबर सुरक्षा पर एक अध्ययन। इंजीनियरिंग और प्रबंधन का अंतर्राष्ट्रीय वैज्ञानिक जर्नल। 02. 10.55041/isjem00350.
79. राव, हर्षिता. (2019). बैंकिंग क्षेत्र में साइबर अपराध. इंटरनेशनल जर्नल ऑफ रिसर्च - ग्रंथालय. 7. 148-161. 10.29121/ग्रंथालय. v7.i1.2019.1043.
80. रूपरेलिया, करिश्मा. (2023). भारतीय बैंकिंग क्षेत्र में साइबर बीमा का बढ़ता महत्व.
81. रेहान, अबू. (2024). डिजिटल युग में साइबर सुरक्षा: खतरों का आकलन और बचाव को मजबूत करना. 10.13140/RG.2.2.31480.25607.

82. लेस्माना, डेस्टा और अफिफुद्दीन, मोचम्मद और एड्रियान्टो, अगुस। (2023)। डिजिटल आर्थिक परिवर्तन में चुनौतियाँ और साइबर सुरक्षा खतरे। इंटरनेशनल जर्नल ऑफ़ ह्यूमैनिटीज़ एजुकेशन एंड सोशल साइंसेज (IJHESS)। 2. 10.55227/ijhess. v2i6.515.
83. शंकर, सहाना और गुडाडिन्नी, समर्थ और मोहता, रोनिता। (2024)। बैंकिंग उद्योग में साइबर खतरों का एक व्यापक अध्ययन। 10.4018/979-8-3693-0839-4.ch011।
84. शर्मा, सागर और चौहान, मोनाली और भारद्वाज, ऐश्वर्या। (2024)। भारत के बैंकिंग क्षेत्र में साइबर अपराध और साइबर सुरक्षा परिदृश्य का विश्लेषण। शोधकोश: दृश्य और प्रदर्शन कला की पत्रिका। 5. 10.29121/शोधकोश। v5.i1.2024.2747।
85. शुक्र, फातिना और शुक्र, सिनान। (2023)। IoT आधारित साइबर सुरक्षा खतरों का व्यापक विश्लेषण। जर्नल ऑफ़ एप्लाइड आर्टिफिशियल इंटेलिजेंस। 4. 12-21. 10.48185/jaai. v4i2.920.
86. शेखर, एनसी, और कुमार, एम. (2023)। डिजिटल बैंकिंग क्षेत्र में साइबर सुरक्षा का अवलोकन। ईस्ट एशियन जर्नल ऑफ़ मल्टीडिसिप्लिनरी रिसर्च, 2(1), 43–52।
87. शेखर, चंद्रा और कुमार, मनोजकुमार। (2023)। डिजिटल बैंकिंग क्षेत्र में साइबर सुरक्षा का अवलोकन। ईस्ट एशियन जर्नल ऑफ़ मल्टीडिसिप्लिनरी रिसर्च। 2. 43-52. 10.55927/eajmr. v2i1.1671.
88. शेहाब, रमी और अबरार, शोएब और अलमायाह, मोहम्मद और अलखदौर, तैसीर और बेलाल, महमूद और अलवादी, बेलाल और अलरावद, महमूद। (2024)। बैंकिंग और वित्तीय सेवाओं पर साइबर सुरक्षा जोखिमों और खतरों का आकलन। जर्नल ऑफ़ इंटरनेट सर्विसेज एंड इंफॉर्मेशन सिस्टिमोरिटी। 14. 167-190। 10.58346/jisis। 2024.i3.010।
89. शैरगोजरी, आदिल अहमद और डार, शौकत (2022)। उभरती साइबर सुरक्षा भारत की चिंता और खतरे। इंटरनेशनल जर्नल ऑफ़ इन्फॉर्मेशन टेक्नोलॉजी एंड कंप्यूटर इंजीनियरिंग। 17-26। 10.55529/ijitc.24.17.26।
90. श्री दिगपाल सिंह एच. राठौर और श्री कर्ण मारवाहा, “बैंकिंग क्षेत्र में साइबर अपराध - कानून मंत्र,” खंड 2, संख्या 7, 2014,
91. श्रीमती शशिकला के.जी., श्री रमेश ए.पी. (2025), “भारतीय बैंकिंग क्षेत्र में साइबर सुरक्षा खतरों पर एक विश्लेषणात्मक अध्ययन,” इंटरनेशनल जर्नल ऑफ़ रिसर्च पब्लिकेशन एंड रिव्यूज़, खंड (6), अंक (6), जून (2025), पृष्ठ – 6516-6520

92. सर्द एस, अल्लमीमी सा, अलकाय्यल ना, अलशहरी ई, अलबाद दा। व्यवसायों के लकाईलेपन के लिए डिजिटल परिवर्तन और साइबर सुरक्षा चुनौतियाँ: मुद्दे और सिफारिशें। सेंसर (बेसल)। 2023 जुलाई 25;23(15):6666। Doi: 10.3390/s23156666। पीएमआईडी: 37571451; पीएमसीआईडी: पीएमसी10422504।
93. सलमान, हसन और अलसाजरी, अब्दुलअज़ीज़। (2023)। साइबर सुरक्षा खतरों का विकास और प्रभावी सुरक्षा के लिए रणनीतियाँ। एक समीक्षा। SHIFRA। 2023. 1-13. 10.70470/SHIFRA/2023/009।
94. सालिह, अजार और अब्दुलरज्जाक, मैवान। (2023)। साइबर सुरक्षा: साइबर हमलों का पता लगाने के लिए प्रदर्शन विश्लेषण और चुनौतियाँ। इंडोनेशियाई जर्नल ऑफ इलेक्ट्रिकल इंजीनियरिंग और कंप्यूटर साइंस। 31. 1763. 10.11591/ijeecs. v31.i3. pp1763-1775.
95. सिंह, एन.; बुय्या, आर.; किम, एच. क्लाउड-आधारित इंटरनेट ऑफ थिंग्स को सुरक्षित करना: चुनौतियाँ और निवारण। सेंसर 2025, 25, 79. <https://doi.org/10.3390/s25010079>
96. सिंह, डॉ. और द्विवेदी, नीलांशु. (2024). भारत में साइबर सुरक्षा खतरों के हालिया रुझान. 2582-5208. 10.56726/irjmets61652.
97. सिंह, डॉ. और पांडे, निष्ठा. (2024). भारत में साइबर सुरक्षा खतरों की वर्तमान स्थिति. 2582-5208. 10.56726/irjmets61628.
98. सिंह, प्रभात. (2023). भारत में वित्तीय संस्थानों में साइबर सुरक्षा: एक महत्वपूर्ण विश्लेषण.
99. सिंह, हरजसदीप और खत्री, अंजना और कौर, अर्पिंदर। (2023)। नवीनतम तकनीकों पर साइबर सुरक्षा चुनौतियों और इसके उभरते रुझानों का एक अध्ययन। इंजीनियरिंग प्रौद्योगिकी और विज्ञान में आधुनिकीकरण का अंतर्राष्ट्रीय अनुसंधान जर्नल। 5. 1085-1090। 10.56726/IRJMETs47270।
100. सी.पी., कृष्णा. (2024). भारत में डिजिटल बैंकिंग में साइबर सुरक्षा खतरों पर एक अध्ययन: एक विश्लेषणात्मक परिप्रेक्ष्य. शोधकोश: जर्नल ऑफ विजुअल एंड परफॉर्मिंग आर्ट्स. 5. 10.29121/शोधकोश. V5.i1.2024.4924.
101. सुगन्या, सुश्री के. (2022). साइबर सुरक्षा: खतरे और चुनौतियाँ।

102. सुमन आचार्य, सुजाता जोशी, “भारत में बैंकिंग संस्थानों पर साइबर हमलों का प्रभाव: सुरक्षा तंत्र और निवारक उपायों का एक अध्ययन,” पलार्च जर्नल ऑफ आर्कियोलॉजी ऑफ इजिप्ट/इजिप्टोलॉजी 17(6)। आईएसएसएन 1567-214, मई 2020।
103. सेले, एन.एन., और केंडा, एस. (2024)। क्या साइबर सुरक्षा के खतरे और जोखिम डिजिटल बैंकिंग को अपनाने पर प्रभाव डालते हैं? एक व्यवस्थित साहित्य समीक्षा। जर्नल ऑफ फाइनेंशियल क्राइम।
104. सेले, एन.एन., और केंडा, एस. (2024)। क्या साइबर सुरक्षा के खतरे और जोखिम डिजिटल बैंकिंग को अपनाने पर प्रभाव डालते हैं? एक व्यवस्थित साहित्य समीक्षा। जर्नल ऑफ फाइनेंशियल क्राइम।
105. सेले, एन.एन. और केंडा, एस. (2025), "क्या साइबर सुरक्षा खतरों और जोखिमों का डिजिटल बैंकिंग को अपनाने पर प्रभाव पड़ता है? एक व्यवस्थित साहित्य समीक्षा", *वित्तीय अपराध पत्रिका*, खंड 32 संख्या 1, पृ. 31-48.
106. स्टैनिकजई, अब्दुल करीब और शाह, मुनम। (2021)। बैंकिंग प्रणालियों में साइबर सुरक्षा खतरों का मूल्यांकन। 1-4. 10.1109/ssci50451.2021.9659862।
107. हुमायूं, ममूना और नियाज़ी, महमूद और झांझी, नूर और अलशायब, मोहम्मद और महमूद, सज्जाद। (2020)। साइबर सुरक्षा खतरे और कमजोरियाँ: एक व्यवस्थित मानचित्रण अध्ययन। अरेबियन जर्नल फॉर साइंस एंड इंजीनियरिंग। 45. 10.1007/s13369-019-04319-2।
108. हे वार्ड, अलीयू ए, इवांस एम, लुओ सी. कोविड-19 की जलवायु में स्वास्थ्य सेवा साइबर सुरक्षा चुनौतियाँ और समाधान: स्कोपिंग समीक्षा। जे मेड इंटरनेट रेस। 2021 अप्रैल 20;23(4): ई21747. डीओआई: 10.2196/21747. त्रुटि: जे मेड इंटरनेट रेस। 2021 अप्रैल 28;23(4): ई29877. डीओआई: 10.2196/29877. पीएमआईडी: 33764885; पीएमसीआईडी: पीएमसी8059789.
109. हैक: यूनिन बैंक से चोरी हुए 171 मिलियन डॉलर कैसे बरामद किए गए,” 2017.
110. हैरिस, हक्सले और जैस्मीन, न्यूरेटी (2025)। डिजिटल बैंकिंग में साइबर सुरक्षा जोखिम: खतरे और शमन रणनीतियाँ।



ISSN: 2584-282X



INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Publication Certificate



This is to certify that

Authored by

Dr. Aiman Fatma

In the recognition of the paper titled "ग्राहकों और बैंक कर्मचारियों के बीच साइबर सुरक्षा जागरूकता के स्तर का विश्लेषण करना" has been published in Volume 3 Issue 4 Page Number: 219-224 journal "International Journal of Trends in Emerging Research and Development"



Certificate Number: IJTERD: 4-1-49

Authorized By:

Publisher: Mr. Vipin



Publisher: Vipin

Address: Z-372, Prem Nager, Kirari Suleman Nagar, North West Delhi, Delhi-110086, Delhi-110086, India

Phone Number: 7053938407

Email: editor.ijterdjournal@gmail.com

Website: <https://researchtrendsjournal.com>





ISSN: 2584-282X



INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Publication Certificate



This is to certify that

Authored by

Dr. Subhasish Basu

In the recognition of the paper titled "ग्राहकों और बैंक कर्मचारियों के बीच साइबर सुरक्षा जागरूकता के स्तर का विश्लेषण करना" has been published in Volume 3 Issue 4 Page Number: 219-224 journal "International Journal of Trends in Emerging Research and Development"



Certificate Number: IJTERD: 4-1-49

Authorized By:

Publisher: Mr. Vipin



Publisher: Vipin

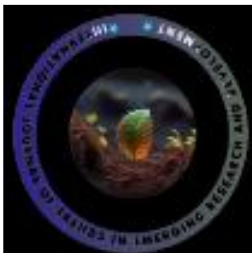
Address: Z-372, Prem Nager, Kirari Suleman Nagar, North West Delhi, Delhi-110086, Delhi-110086, India

Phone Number: 7053938407

Email: editor.ijterdjournal@gmail.com

Website: <https://researchtrendsjournal.com>





ISSN: 2584-282X



INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Publication Certificate



This is to certify that

Authored by

Rakesh Kumar Rai

In the recognition of the paper titled "ग्राहकों और बैंक कर्मचारियों के बीच साइबर सुरक्षा जागरूकता के स्तर का विश्लेषण करना" has been published in Volume 3 Issue 4 Page Number: 219-224 journal "International Journal of Trends in Emerging Research and Development"

Certificate Number: IJTERD: 4-1-49

Authorized By:

Publisher: Mr. Vipin



Publisher: Vipin

Address: Z-372, Prem Nager, Kirari Suleman Nagar, North West Delhi, Delhi-110086, Delhi-110086, India

Phone Number: 7053938407

Email: editor.ijterdjournal@gmail.com

Website: <https://researchtrendsjournal.com>





INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 4; 2025; Page No. 219-224

Received: 14-04-2025

Accepted: 27-06-2025

Published: 29-07-2025

ग्राहकों और बैंक कर्मचारियों के बीच साइबर सुरक्षा जागरूकता के स्तर का विश्लेषण करना

¹Rakesh Kumar Rai, ²Dr. Subhasish Basu and ³Dr. Aiman Fatma

¹Research Scholar, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

²Supervisor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

³Associate Professor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

DOI: <https://doi.org/10.5281/zenodo.18699881>

Corresponding Author: Rakesh Kumar Rai

सारांश

साइबर-हमले लगातार विकसित हो रहे हैं और लगातार बढ़ रहे हैं तथा व्यापक हो रहे हैं। हमलावर अपनी रणनीति और तकनीकों में सुरक्षा टीमों की तुलना में तेज़ी से सुधार कर रहे हैं तथा उनके तरीके हर साल अधिक परिष्कृत होते जा रहे हैं। इसलिए, यह शोध समीक्षाओं, लेखों, साक्षात्कारों और केस स्टडी के माध्यम से वर्तमान साइबर सुरक्षा योजनाओं और अवधारणाओं का अध्ययन करने के लिए किया गया है। इसका उद्देश्य उपयोगकर्ताओं के बीच साइबर सुरक्षा और इसके नियमों के बारे में जागरूकता पैदा करना है। इसने यह मूल्यांकन करने का प्रयास किया है कि कितने लोग ऑनलाइन लेनदेन करते समय वास्तव में साइबर सुरक्षा नियमों का उपयोग कर रहे हैं।

मूलशब्द: साइबर सुरक्षा, ऑनलाइन बैंकिंग, ऑनलाइन, बैंकिंग, जागरूकता।

प्रस्तावना

वैश्विक वित्तीय परिदृश्य में चुनौतियों की एक निरंतर विकसित श्रृंखला सामने आ रही है, जिसमें परिचालन संबंधी कमियाँ, बाजार में अस्थिरता, भू-राजनीतिक अनिश्चितताएँ, साइबर सुरक्षा खतरे और विनियामक अनुपालन और ऋण स्तरों पर आशंकाएँ शामिल हैं। इन जोखिमों में वित्तीय संकटों को ट्रिगर करने, बाजार में व्यवधान पैदा करने और वैश्विक आर्थिक विकास को प्रभावित करने की अलग-अलग डिग्री की क्षमता होती है। वित्तीय संस्थानों, नियामकों और बाजार के खिलाड़ियों को इस बदलते माहौल में सतर्क और अनुकूलनशील रहना चाहिए। इन खतरों को संबोधित करने और कम करने के लिए, सक्षम जोखिम प्रबंधन, नियामक निरीक्षण, तकनीकी नवाचार और अंतर्राष्ट्रीय सहयोग महत्वपूर्ण घटक हैं।

वर्तमान में, साइबर सुरक्षा सभी संगठनों के लिए एक बढ़ती चुनौती है। पिछले वर्ष में, यह स्पष्ट हो गया है कि बैंकिंग क्षेत्र में इसके बुनियादी ढांचे और साइबर सुरक्षा उपायों में कई कमियाँ थीं। डिजिटल परिवर्तन ने बैंकिंग उद्योग को मौलिक रूप से बदल

दिया है, जिसके परिणामस्वरूप दक्षता में वृद्धि हुई है, पहुँच में विस्तार हुआ है और ग्राहकों के लिए बेहतर अनुभव हुआ है। फिर भी, इस तेज़ डिजिटलीकरण ने साइबर खतरों को भी बढ़ा दिया है, जिससे वित्तीय संगठनों के लिए साइबर सुरक्षा एक सर्वोपरि मुद्दा बन गई है। वर्तमान में, बैंकों को मैलवेयर हमलों, फ़िशिंग, पहचान की चोरी, रैनसमवेयर, अवैध डेटा उल्लंघनों और साइबर अपराध के तेज़ी से उन्नत प्रकारों सहित कई खतरों का सामना करना पड़ता है।

इन पारंपरिक जोखिमों के अलावा, ऑनलाइन बैंकिंग से जुड़े कई उभरते खतरे तत्काल ध्यान देने की मांग करते हैं। उदाहरण के लिए, मोबाइल बैंकिंग एप्लिकेशन का व्यापक रूप से अपनाया जाना, उपयोगकर्ताओं को कम से कम सुरक्षा उपायों के साथ काम करने पर बढ़ी हुई कमज़ोरियों के प्रति उजागर करता है, जिससे अनधिकृत पहुँच और धोखाधड़ी का जोखिम काफी बढ़ जाता है। इसके अलावा, जैसे-जैसे बैंक अपने आंतरिक बचाव को मज़बूत करते हैं, साइबर अपराधी तीसरे पक्ष के नेटवर्क और साझा बैंकिंग सिस्टम को तेज़ी से निशाना बना रहे हैं, जिनमें अक्सर मज़बूत

सुरक्षा उपायों की कमी होती है, जिससे हमलों के लिए आसान प्रवेश बिंदु बन जाते हैं।

तेज़ी से बढ़ता क्रिप्टोकॉरेसी बाज़ार इन चुनौतियों को और भी जटिल बनाता है; इस क्षेत्र में नवजात विनियामक ढाँचा और तकनीकी नवाचार की तेज़ गति साइबर हमलों के लिए अवसर पैदा करती है जो सुरक्षा खामियों का फ़ायदा उठाते हैं। ये बहुआयामी जोखिम अभिनव साइबर सुरक्षा रणनीतियों की तत्काल आवश्यकता को उजागर करते हैं जो गतिशील खतरे के परिदृश्य के अनुकूल हो सकते हैं और डिजिटल बैंकिंग पारिस्थितिकी तंत्र की सुरक्षा कर सकते हैं।

साहित्य की समीक्षा

सिंह, प्रभात. (2023) ^[11] हम एक समकालीन, डिजिटल और वैश्वीकृत दुनिया में रहते हैं। जहाँ दक्षता और सुविधा प्रबल है, हालाँकि यह आसानी एक कीमत पर आती है। ई-बैंकिंग कई लाभ प्रदान करती है; फिर भी, यह चुनौतियों या मुद्दों से रहित नहीं है। ऐसा ही एक मुद्दा बैंकिंग उद्योग के अंदर साइबर सुरक्षा बनाए रखना है। यह अध्ययन साइबर खतरों के कई आयामों पर चर्चा करता है। भारत में साइबर सुरक्षा के लिए नियामक ढाँचा। यह पेपर भारत में साइबर सुरक्षा के लिए अलग-अलग कानूनों की आवश्यकता पर अंतर्दृष्टि प्रदान करता है।

सी.पी., कृष्णा. (2024) डिजिटल बैंकिंग की तीव्र प्रगति ने साइबर सुरक्षा खतरों में वृद्धि की है, जिससे वित्तीय संस्थान और उनके ग्राहक खतरे में हैं। यह अध्ययन डिजिटल बैंकिंग में महत्वपूर्ण साइबर सुरक्षा चिंताओं, उनके परिणामों और रोकथाम के विकल्पों की जांच करता है। अध्ययन में अनुभवजन्य केस स्टडी और डेटा व्याख्या शामिल है, जो वर्तमान सुरक्षा समाधानों की प्रभावकारिता के बारे में जानकारी प्रदान करता है। विविध साइबर सुरक्षा चिंताओं, बदलते खतरे के माहौल और इन जोखिमों को कम करने में प्रौद्योगिकी के कार्य की गहन जांच प्रस्तुत की गई है। यह अध्ययन नियामक अनुपालन, नीतिगत सुझावों और साइबर सुरक्षा में उभरते रुझानों की जांच करता है।

पॉल (2024) यह सार बैंकिंग उद्योग के भीतर साइबर सुरक्षा का सारांश प्रस्तुत करता है, जिसमें भारतीय संस्थानों के लिए इसके महत्व, समस्याओं और निवारक रणनीतियों पर जोर दिया गया है। साइबर सुरक्षा में नेटवर्क सुरक्षा, एप्लिकेशन सुरक्षा और सूचना सुरक्षा जैसे क्षेत्रों सहित डिजिटल संपत्तियों को अवांछित पहुँच से सुरक्षित रखना शामिल है। भारतीय बैंकों को कई साइबर खतरों का सामना करना पड़ता है, जैसे फ़िशिंग योजनाएँ, डेटा उल्लंघन और रैनसमवेयर हमले, जिनके लिए मल्टी-फ़ैक्टर प्रमाणीकरण, नियमित सुरक्षा ऑडिट और स्टाफ़ प्रशिक्षण पहल जैसे कड़े निवारक उपायों की आवश्यकता होती है। साइबर जोखिमों से सफलतापूर्वक निपटने के लिए सेक्टर और सरकारी संस्थाओं के बीच सहयोग को ज़रूरी माना जाता है। तेज़ी से बदलते डिजिटल माहौल में बैंकिंग उद्योग में विश्वास, प्रतिष्ठा और स्थिरता को बनाए रखने के लिए साइबर सुरक्षा को महत्वपूर्ण माना जाता है।

शेखर (2023) 21वीं सदी में, इंटरनेट तकनीक को बेहतरीन प्रदर्शन के लिए बढ़ाया गया है और सभी उपयोगकर्ताओं द्वारा इसका व्यापक रूप से उपयोग किया जाता है। डिजिटल बैंकिंग क्षेत्र शीर्ष पांच में है और लगातार NEFT, Google Pay और Ponape जैसी ऑनलाइन तकनीकों का उपयोग करता है। ऑनलाइन बैंकिंग के बढ़ते उपयोग के बावजूद, बैंकिंग उद्योग के भीतर साइबर अपराध पिछले कुछ वर्षों में बढ़ रहे हैं। यह कहा गया है कि 50% साइबर अपराध एटीएम, डेबिट कार्ड और

ऑनलाइन बैंकिंग से जुड़े हैं। बैंकिंग उद्योग अन्य उद्योगों की तुलना में अधिक बार साइबर हमलों का सामना कर रहा है। यह अध्ययन बैंकिंग उद्योग में साइबर हमलों और ऐसे खतरों के खिलाफ साइबर सुरक्षा को बढ़ाने के तरीकों की जांच करता है।

मूंदड़ा, आदर्श (2024). इस शोध का उद्देश्य वित्तीय संस्थानों पर साइबर अपराध के हानिकारक प्रभावों की जांच करना और इसके परिणामों को कम करने के लिए एक मजबूत साइबर सुरक्षा ढाँचे का विकास करना है। हाल ही में बैंक इसके प्राथमिक लक्ष्य रहे हैं। भारत में कई बैंक अक्सर बड़े पैमाने पर मैलवेयर हमलों के अधीन होते हैं, जो निजी और संवेदनशील जानकारी से समझौता करते हैं और काफी वित्तीय नुकसान का कारण बनते हैं। इस शोध का उद्देश्य यह पहचानना है कि कौन से उद्योग क्षेत्र साइबर हमलों के लिए अधिक संवेदनशील हैं और साइबर सुरक्षा नीतियों के विकास और अनुकूलन को सुनिश्चित करना है। रिपोर्ट में विभिन्न साइबर खतरों और अपराधों की केस स्टडी जांच शामिल है, जिसके कारण काफी वित्तीय नुकसान हुआ है, साथ ही सरकारी वेबसाइटों, शैक्षणिक प्रकाशनों और शोध पत्रों सहित विभिन्न इंटरनेट संसाधनों से प्राप्त द्वितीयक डेटा विश्लेषण भी शामिल है। यह लेख साइबर शासन के बारे में अंतर्दृष्टि प्रदान करेगा जो वित्तीय संस्थानों, बैंकों और बड़े पैमाने पर समाज को लाभान्वित करेगा।

शोध पद्धति

अनुसंधान डिजाइन

शोध डिजाइन एक व्यापक योजना है जो शोध परियोजना के उद्देश्यों को परिभाषित करती है और उन उद्देश्यों को पूरा करने के लिए जो भी इच्छाएं पूरी की जानी हैं, उनके लिए दिशानिर्देश प्रदान करती है। दूसरे शब्दों में, यह शोध परियोजना को पूरा करने के लिए एक सामान्य योजना है।

डेटा संग्रहण के लिए उपकरण

डेटा संग्रह या डेटा का संग्रह अनुसंधान की प्रक्रिया में एक महत्वपूर्ण चरण हो सकता है। डेटा एकत्र करने के लिए आप जो उपकरण चुनते हैं, वह इस बात पर निर्भर करेगा कि आप किस तरह का डेटा एकत्र करना चाहते हैं और आप इसे कैसे एकत्र करने की योजना बना रहे हैं।

इस शोध को तैयार करने में कई सामान्य डेटा संग्रह उपकरणों का उपयोग किया गया

- प्रश्नावली
- बैठक
- व्याख्याओं
- सरकारी स्रोत
- प्रयोगशाला प्रयोग
- इलेक्ट्रॉनिक मेल या इलेक्ट्रॉनिक संदेश

नमूना डिजाइन

नमूनाकरण डिजाइन एक गणितीय फ़ंक्शन है जो आपको यह संभावना देता है कि एक निश्चित नमूना लिया जाएगा। चूंकि नमूनाकरण लगभग सभी शोध परियोजनाओं का आधार है, इसलिए नमूनाकरण डिजाइन का अध्ययन सांख्यिकी का एक महत्वपूर्ण हिस्सा है। प्रत्यक्ष अध्ययन एक खंड-आधारित अध्ययन हो सकता है। नतीजतन, नमूनाकरण तकनीक और नमूनाकरण डिजाइन समय पर लक्ष्य प्राप्त करने में महत्वपूर्ण भूमिका निभाते हैं।

डेटा विश्लेषण और परिकल्पना परीक्षण पूरा करना

डेटा विश्लेषण मुख्य रूप से वर्णनात्मक और भिन्न सांख्यिकीय परीक्षणों का उपयोग करके किया जाता है। डेटा को प्रस्तुत करने के लिए अभिव्यंजक सांख्यिकी और चार्ट / ग्राफ़ का उपयोग किया जाता है, जबकि अनुमानात्मक सांख्यिकी का उपयोग परिकल्पना का परीक्षण करने के लिए किया जाता है। डेटा विश्लेषण करने के लिए विभिन्न वर्णनात्मक और विभिन्न सांख्यिकीय परीक्षणों का उपयोग किया जाता है। वर्णनात्मक सांख्यिकी के साथ ग्राफ़ का उपयोग डेटा प्रस्तुत करने के लिए किया जाता है जबकि अनुमानात्मक सांख्यिकी का उपयोग परिकल्पना का परीक्षण करने के लिए किया जाता है।

- ची स्कायर टेस्ट
- एनोवा

डेटा विश्लेषण

यह अध्याय मात्रात्मक और गुणात्मक दोनों तरह के डेटा के विश्लेषण से संबंधित है। प्राथमिक डेटा इंटरनेट बैंकिंग के ग्राहकों के उपयोग, अपने बैंक खाते में साइबर अपराध का अनुभव करने वाले और पीड़ित बनने वाले ग्राहकों और साइबर अपराध का अनुभव न करने वाले या गैर-पीड़ित लोगों के संबंध में एकत्र किया गया था।

सभी लिंगों में साइबर सुरक्षा नियमों के बारे में जागरूकता

साइबर सुरक्षा के बारे में जागरूकता में लोगों को कार्यवाई करने के लिए पर्याप्त रूप से जागरूक करना शामिल है। इसके लिए सिर्फ नियमों का एक सेट नहीं, बल्कि सुरक्षा मानसिकता बनाने की ज़रूरत है। संक्षेप में, यह सिर्फ खतरों के बारे में जागरूक होने के बारे में नहीं है, बल्कि खतरों और संगठन और उसके लोगों पर उनके प्रभाव को समझने के बारे में भी है, जिसमें खुद भी शामिल हैं।

तालिका 1: साइबर सुरक्षा नियमों के बारे में लिंग के आधार पर जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		लिंग		कुल
		पुरुष	महिला	
पूरी तरह।	गिनती करना	119	76	195
	प्रतिशत (%)	27.5	25.9	26.9
थोड़ा	गिनती करना	261	190	451
	प्रतिशत (%)	60.4	64.6	62.1
बिल्कुल नहीं	गिनती करना	52	28	80
	प्रतिशत (%)	12.0	9.5	11.0
कुल	गिनती करना	432	294	726
	प्रतिशत (%)	100.0	100.0	100.0

उपरोक्त तालिका 1 से पता चलता है कि 119 पुरुष और 76 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में पूरी तरह से अवगत थे, 261 पुरुष और 190 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में आंशिक रूप से अवगत थीं। हालांकि, 52 पुरुष और 28 महिलाएं ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों के बारे में बिल्कुल भी नहीं जानती थीं।

तालिका 2: काई-स्कायर परीक्षण

	कीमत	डीएफ	असिम्प. सिग. (2-पक्षीय)
पियर्सन ची-स्कायर	1.689ए	2	.430
संभावना अनुपात	1.705	2	.426
रैखिक-दर-रैखिक एसोसिएशन	.033	1	.856
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को अस्वीकार नहीं किया गया है क्योंकि $p > 0.05$ (0.430) है। इसलिए, साइबर सुरक्षा नियमों और लिंग के बारे में जागरूकता एक दूसरे से स्वतंत्र हैं।

सभी आयु वर्गों में साइबर सुरक्षा नियमों के बारे में जागरूकता

सर्वेक्षण के लिए 18 से लेकर 60 वर्ष से अधिक आयु के विभिन्न आयु समूहों के 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका विभिन्न आयु समूहों के बीच साइबर सुरक्षा नियमों के बारे में जागरूकता को दर्शाती है।

तालिका 3: आयु वर्ग के अनुसार साइबर सुरक्षा नियमों के बारे में जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		आयु				कुल
		18 से 25	25 से 46	46 से 60	60 से ऊपर	
पूरी तरह	गिनती करना	96	95	2	2	195
	प्रतिशत (%)	30.3	25.1	7.1	100.0	26.9
थोड़ा	गिनती करना	183	252	16	0	451
	प्रतिशत (%)	57.7	66.5	57.1	0.0	62.1
बिल्कुल नहीं	गिनती करना	38	32	10	0	80
	प्रतिशत (%)	12.0	8.4	35.7	0.0	11.0
कुल	गिनती करना	317	379	28	2	726
	प्रतिशत (%)	100.0	100.0	100.0	100.0	100.0

उपरोक्त तालिका 3 यह निर्धारित करती है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 96 उत्तरदाता 18 से 25 आयु वर्ग के थे, 95 उत्तरदाता 25 से 46 आयु वर्ग के थे, 02 उत्तरदाता 46 से 60 आयु वर्ग के थे और 02 उत्तरदाता 60 वर्ष और उससे अधिक आयु वर्ग के थे जो ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से पूरी तरह अवगत थे। 18 से 25 आयु वर्ग के 183 उत्तरदाता, 25 से 46 आयु वर्ग के 252 उत्तरदाता और 46 से 60 आयु वर्ग के 16 उत्तरदाता ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से आंशिक रूप से अवगत थे। हालांकि, 18 से 25 आयु वर्ग के 38 उत्तरदाता, 25 से 46 आयु वर्ग के 32 उत्तरदाता और 46 से 60 आयु वर्ग के 10 उत्तरदाता ऑनलाइन लेनदेन में साइबर सुरक्षा नियमों से बिल्कुल भी अवगत नहीं थे।

तालिका 4: काई-स्कायर परीक्षण

	कीमत	डीएफ	असिम्प. सिग. (2-पक्षीय)
पियर्सन ची-स्कायर	31.646ए	6	.000
संभावना अनुपात	27.492	6	.000
रैखिक-दर-रैखिक एसोसिएशन	3.327	1	.068
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को $p < 0.05$ (0.000) के रूप में खारिज कर दिया गया है। इसलिए, साइबर सुरक्षा नियमों के बारे में जागरूकता और आयु एक दूसरे से स्वतंत्र नहीं हैं।

उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका अलग-अलग शैक्षणिक पृष्ठभूमि वाले विभिन्न उत्तरदाताओं के बीच साइबर सुरक्षा नियमों के बारे में जागरूकता को दर्शाती है।

शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता:
सर्वेक्षण के लिए अलग-अलग शैक्षणिक पृष्ठभूमि वाले 726

तालिका 5: शिक्षा जगत में साइबर सुरक्षा नियमों के बारे में जागरूकता

ऑनलाइन लेनदेन में सुरक्षा नियमों के प्रति आप कितने चिंतित और जागरूक हैं?		शिक्षा							कुल
		एच एस सी तक	डिप्लोमा	स्नातक	स्नातकोत्तर	पी एच. डी.	सीए	रिसर्च स्कॉलर	
पूरी तरह	गिनती करना	21	0	69	95	2	8	0	195
	%	39.6	0	24.9	26.2	16.7	57.1	0	26.9
थोड़ा	गिनती करना	22	4	165	246	6	6	2	451
	%	41.5	66.7	59.6	68	50	42.9	100	62.1
बिल्कुल नहीं	गिनती करना	10	2	43	21	4	0	0	80
	%	18.9	33.3	15.5	5.8	33.3	0	0	11
कुल	गिनती करना	53	6	277	362	12	14	2	726
	%	100	100	100	100	100	100	100	100

उपरोक्त तालिका 5 में बताया गया है कि सर्वेक्षण में शामिल कुल 726 उत्तरदाताओं में से 195 (21 एच.एस.सी. तक, 69 स्नातक, 95 स्नातकोत्तर, 02 पी.एच.डी. और 08 चार्टर्ड अकाउंटेंट) उत्तरदाता साइबर सुरक्षा नियमों के बारे में चिंतित और पूरी तरह से अवगत थे। 451 (22 एच.एस.सी. तक, 4 डिप्लोमा, 165 स्नातक, 246 स्नातकोत्तर, 06 पी.एच.डी., 06 चार्टर्ड अकाउंटेंट और 02 रिसर्च स्कॉलर) उत्तरदाता भी चिंतित थे, लेकिन साइबर सुरक्षा नियमों के बारे में आंशिक रूप से जानते थे। हालांकि, 80 (10 एच.एस.सी. तक, 02 डिप्लोमा, 43 स्नातक, 21 स्नातकोत्तर और 04 पी.एच.डी.) उत्तरदाता बिल्कुल भी चिंतित नहीं थे और न ही वे साइबर सुरक्षा नियमों के बारे में जानते थे।

तालिका 6: कार्ड-स्कायर परीक्षण

	कीमत	डीएफ	असिम्प. सिग. (2-पक्षीय)
पियर्सन ची-स्कायर	45.457ए	12	.000
संभावना अनुपात	46.234	12	.000
रैखिक-दर-रैखिक एसोसिएशन	2.264	1	.132
वैध मामलों की संख्या N	726		

उपरोक्त परीक्षण में शून्य परिकल्पना को $p < 0.05$ (0.000) के रूप में खारिज कर दिया गया है। इसलिए, साइबर सुरक्षा नियमों और शिक्षा के बारे में जागरूकता एक दूसरे से स्वतंत्र नहीं हैं।

तालिका 8: कार्ड-स्कायर परीक्षण

	कीमत	डीएफ	असिम्प. सिग. (दो तरफा)	सटीक सिग. (दो तरफा)	सटीक सिग. (1-पक्षीय)
पियर्सन ची-स्कायर	.444ए	1	0.505		
निरंतरता सुधार	0.349	1	0.555		
संभावना अनुपात	0.444	1	0.505		
फिशर का सटीक परीक्षण				0.545	0.277
रैखिक-दर-रैखिक एसोसिएशन	0.443	1	0.506		
वैध मामलों की संख्या N	726				

विभिन्न लिंगों के बीच नकद जमा के वित्तीय लेनदेन

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 7 विभिन्न लिंगों द्वारा किए गए नकद जमा के वित्तीय लेन-देन को दर्शाती है।

तालिका 7: विभिन्न लिंगों में नकद जमा के वित्तीय लेनदेन

			नकद जमा		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	221	211	432
		लिंग के भीतर %	51.2	48.8	100
	महिला	गिनती करना	143	151	294
		लिंग के भीतर %	48.6	51.4	100
कुल	गिनती करना		364	362	726
	लिंग के भीतर %		50.1	49.9	100

तालिका 7 से पता चलता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 211 पुरुष नकद जमा का वित्तीय लेन-देन करना पसंद करते हैं जबकि 221 पुरुष नकद जमा का वित्तीय लेन-देन ऑनलाइन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 151 महिलाएँ नकद जमा का वित्तीय लेन-देन करना पसंद करती हैं जबकि 143 महिलाएँ नकद जमा भेजना ऑनलाइन करना पसंद नहीं करती हैं।

ऊपर प्रस्तुत किए गए काई-स्कायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि नकद जमा का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्कायर 0.444, df 1, $p > 0.05$)। इस प्रकार, नकद जमा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है। कोई भी व्यक्ति नकद जमा कर सकता है, चाहे वह परिवार का कमाने वाला सदस्य हो या आश्रित सदस्य। इसलिए, नकद जमा जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

विभिन्न लिंगों के बीच नकद निकासी के वित्तीय लेनदेन

सर्वेक्षण के लिए लिंग के आधार पर 726 उत्तरदाताओं से डेटा एकत्र किया गया था। नीचे दी गई तालिका 9 विभिन्न लिंगों द्वारा किए गए नकद निकासी के वित्तीय लेन-देन को दर्शाती है।

तालिका 9: विभिन्न लिंगों में नकद निकासी के वित्तीय लेनदेन

			नकद निकासी		कुल
			नहीं	हाँ	
लिंग	पुरुष	गिनती करना	211	221	432
		लिंग के भीतर %	48.8	51.2	100
	महिला	गिनती करना	130	164	294
		लिंग के भीतर %	44.2	55.8	100
कुल		गिनती करना	341	385	726
		लिंग के भीतर %	47	53	100

तालिका 9 से यह देखा जा सकता है कि सर्वेक्षण में शामिल 726 उत्तरदाताओं में से 432 पुरुष थे जबकि 294 महिलाएँ थीं। इन 432 पुरुषों में से 221 पुरुष नकद निकासी के वित्तीय लेन-देन करना पसंद करते हैं जबकि 211 पुरुष ऑनलाइन नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करते हैं। इसी तरह, इन 294 महिलाओं में से 164 महिलाएँ नकद निकासी के वित्तीय लेन-देन करना पसंद करती हैं जबकि 130 महिलाएँ ऑनलाइन नकद निकासी के वित्तीय लेन-देन करना पसंद नहीं करती हैं।

तालिका 10: काई-स्कायर परीक्षण

	कीमत	डीएफ	असिम्ट. सिग. (1-पक्षीय)	सटीक सिग. (1-पक्षीय)	सटीक सिग. (1-पक्षीय)
पियर्सन ची-स्कायर	1.502	1	0.22		
निरंतरता सुधार	1.32	1	0.25		
संभावना अनुपात	1.5	1	0.22		
फिशर का सटीक परीक्षण				0.23	0.13
रैखिक-दर-रैखिक एसोसिएशन	1.5	1	0.22		
वैध मामलों की संख्या N	726				

ऊपर प्रस्तुत किए गए काई-स्कायर परीक्षण के परिणाम शून्य परिकल्पना को अस्वीकार नहीं करते हैं कि नकद निकासी का उपयोग और लिंग स्वतंत्र नहीं हैं (काई-स्कायर 0.444, df 1, $p > 0.05$)। इस प्रकार, नकद निकासी जैसे वित्तीय लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है। कोई भी व्यक्ति नकद निकाल सकता है, चाहे वह परिवार का कमाने वाला सदस्य हो या आश्रित सदस्य। इसलिए, नकद निकासी जैसे वित्तीय

लेनदेन का उपयोग किसी व्यक्ति के लिंग पर निर्भर नहीं करता है।

निष्कर्ष

हमारा समाज एक साइबर-भौतिक समाज बन रहा है जो हमारे दैनिक जीवन के सभी पहलुओं में सूचना और संचार प्रौद्योगिकी (ICT) पर आधारित है, जिससे IT सुरक्षा की आवश्यकता मौलिक हो गई है। साइबर सुरक्षा की अमूर्त प्रकृति, सामाजिक-तकनीकी निर्भरता, साइबर सुरक्षा के खिलाफ लड़ाई का अस्पष्ट प्रभाव और विवादास्पद प्रकृति इसे उपयोगकर्ताओं के लिए एक उत्तेजक क्षेत्र बनाती है। अध्ययन से पता चलता है कि मात्रात्मक तरीकों का उद्देश्य साइबर सुरक्षा के बारे में जागरूकता पैदा करना है जिसके लिए भविष्य में उपयोग के लिए कुछ नियमों और विनियमों का पालन किया जाना चाहिए। व्यक्ति को हमेशा नियमों और विनियमों का पालन करना चाहिए।

संदर्भ

1. इकबाल स, नवाज द. साइबर सुरक्षा में उभरते रुझान और भविष्य की चुनौतियाँ: एक व्यापक समीक्षा. 2024.
2. नेग्रेया पीसी. उच्च प्रभाव वाली साइबर सुरक्षा घटनाओं का व्यापक विश्लेषण: केस स्टडीज़ और निहितार्थ. 2023. doi:10.13140/RG.2.2.17461.65763.
3. शुक्र फ, शुक्र स. IoT आधारित साइबर सुरक्षा खतरों का व्यापक विश्लेषण. जर्नल ऑफ एप्लाइड आर्टिफिशियल इंटेलिजेंस. 2023;4:12–21. doi:10.48185/jaai.v4i2.920.
4. अहमद अ, मौलाना र, यासिर म. डिजिटल परिवर्तन के युग में साइबर सुरक्षा चुनौतियाँ: सूचना प्रणालियों का एक व्यापक विश्लेषण. जर्नल इंफॉर्मेटिक, एजुकेशन एंड मैनेजमेंट (जेआईईएम). 2024;6:7–11. doi:10.61992/jiem.v6i1.57.
5. अकेलो ब. संगठनात्मक सूचना सुरक्षा खतरे: स्थिति और चुनौतियाँ. वर्ल्ड जर्नल ऑफ एडवांस्ड इंजीनियरिंग टेक्नोलॉजी एंड साइंसेज. 2023;11:148–162. doi:10.30574/wjaets.2024.11.1.0152.
6. ज़ेबारी द, असद र. साइबर सुरक्षा खतरे, भेद्यता, चुनौतियाँ और प्रस्तावित समाधान. एप्लाइड कंप्यूटिंग जर्नल. 2022;227–244. doi:10.52098/acj.202260.
7. रेहान अ. डिजिटल युग में साइबर सुरक्षा: खतरों का आकलन और बचाव को मजबूत करना. 2024. doi:10.13140/RG.2.2.31480.25607.
8. गोराई स, बेरा स, कुमार म. भारत में साइबर सुरक्षा के मुद्दे और चुनौतियाँ. कंप्यूटर विज्ञान, इंजीनियरिंग और सूचना प्रौद्योगिकी में वैज्ञानिक अनुसंधान के अंतर्राष्ट्रीय जर्नल. 2025;11:159–166. doi:10.32628/CSEIT251112.
9. अलसैफ उ, शहाथा अ. साइबर सुरक्षा खतरों के लिए दृष्टिकोण और कठिनाइयों का एक व्यापक विश्लेषण: लेख समीक्षा. मुस्तनसिरिया जर्नल ऑफ प्योर एंड एप्लाइड साइंसेज. 2024;2:126–139. doi:10.47831/mjpas.v2i4.164.
10. गोनी अ, जहाँगीर मउ, रॉय चौधरी र. साइबर सुरक्षा पर एक अध्ययन: वर्तमान खतरों का विश्लेषण, जटिलताओं को समझना और रोकथाम रणनीतियों को लागू करना. इंटरनेशनल जर्नल ऑफ रिसर्च एंड साइंटिफिक इनोवेशन. 2024;10:507–522. doi:10.51244/IJRSI.2023.1012039.
11. सिंह ह, खत्री अ, कौर अ. नवीनतम तकनीकों पर साइबर

- सुरक्षा चुनौतियों और इसके उभरते रुझानों का एक अध्ययन. इंजीनियरिंग प्रौद्योगिकी और विज्ञान में आधुनिकीकरण का अंतर्राष्ट्रीय अनुसंधान जर्नल. 2023;5:1085–1090. doi:10.56726/IRJMETS47270.
12. फिशर ईए. साइबर सुरक्षा मुद्दे और चुनौतियाँ: संक्षेप में. 2015.
 13. सलमान ह, अलसाजरी अ. साइबर सुरक्षा खतरों का विकास और प्रभावी सुरक्षा के लिए रणनीतियाँ: एक समीक्षा. SHIFRA. 2023;1–13. doi:10.70470/SHIFRA/2023/009.
 14. लेस्माना द, अफिफुद्दीन म, एड्रियान्टो अ. डिजिटल आर्थिक परिवर्तन में चुनौतियाँ और साइबर सुरक्षा खतरे. इंटरनेशनल जर्नल ऑफ ह्यूमैनिटीज एजुकेशन एंड सोशल साइंसेज (IJHES). 2023;2. doi:10.55227/ijhess.v2i6.515.
 15. महतो स, साह र, सपकोटा स. साइबर सुरक्षा चुनौतियाँ और खतरे: डिजिटल दुनिया में जोखिम. विज्ञान, संचार और प्रौद्योगिकी में उन्नत अनुसंधान के अंतर्राष्ट्रीय जर्नल. 2024;651–655. doi:10.48175/IJARSCT-22497.

Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.



भारतीय बैंकिंग प्रणाली में साइबर खतरों की पहचान और वर्गीकरण करना

¹Rakesh Kumar Rai, ²Dr. Subhasish Basu and ³Dr. Aiman Fatma

¹Research Scholar, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

²Supervisor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

³Associate Professor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

DOI: <https://doi.org/10.5281/zenodo.18696295>

Corresponding Author: Rakesh Kumar Rai

सारांश

साइबर अपराधी तेज़ी से कॉर्पोरेट के रूप में कार्य कर रहे हैं, नए उत्पाद विकास दल और कुछ संगठन उनकी सेवाएँ दे रहे हैं या उन्हें अन्य आपराधिक गिरोहों के साथ एकीकृत कर रहे हैं। साइबर अपराध अन्य अपराधों की तुलना में अधिक लाभदायक है, इसलिए बैंकों को इसके विरुद्ध सुरक्षा बनाने में बहुत अधिक संसाधनों का निवेश करना जारी रखना चाहिए। यदि कॉर्पोरेट ग्राहक जानते हैं कि बैंक धोखाधड़ी और साइबर हमलों को रोकने के लिए प्रतिबद्ध है, तो बैंक में विश्वास बढ़ेगा तथा अच्छे संबंध स्थापित होंगे। साइबर अपराध से निपटने के लिए बैंकों को सिस्टम और लोगों में भारी निवेश करना चाहिए।

मूल शब्द: साइबर, भारतीय बैंकिंग, कॉर्पोरेट, साइबर अपराध, खतरों।

प्रस्तावना

बैंकिंग क्षेत्र में प्रौद्योगिकी द्वारा पैदा किए गए अवसरों और संभावनाओं के बावजूद, यह बैंकिंग क्षेत्र और वित्तीय सेवा संस्थानों के लिए एक विशेष चुनौती भी प्रस्तुत करती है। हम सभी जानते हैं कि प्रौद्योगिकी के दुर्भावनापूर्ण उपयोग से बैंकों और वित्तीय सेवा संस्थानों के बुनियादी ढांचे में व्यवधान, सुरक्षा का उल्लंघन, ग्राहक विश्वास, वित्तीय स्थिरता को खतरे में डालना और अन्य साइबर अपराध होते हैं। सूचना सुरक्षा उल्लंघन कभी भी अचानक हो सकता है क्योंकि सब कुछ इंटरनेट के साथ एकीकृत है और साइबर अपराधी जो बैंकों और वित्तीय सेवा संस्थानों की इंटरनेट चीजों में हेरफेर कर रहे हैं, वे बैंकों के ग्राहक डेटा को हक करने और वित्तीय संस्थानों के ग्राहकों के पैसे को डिजिटल रूप से चुराने में सक्षम हैं।

बैंकिंग क्षेत्र में प्रौद्योगिकी के महत्वपूर्ण विकास के साथ, प्रौद्योगिकी से जुड़े जोखिम भी बढ़ गए हैं। इसलिए, बैंकिंग क्षेत्र के संबंध में हर दिन कई प्रकार और रूप में साइबर सुरक्षा हमले/खतरे सामने आते हैं। साइबर सुरक्षा हमले पूरे वित्तीय तंत्र के लिए खतरा पैदा करते हैं, इस तथ्य की पुष्टि अंतर्राष्ट्रीय, क्षेत्रीय और स्थानीय स्तर पर इस संबंध में जारी रिपोर्टों से होती है। इस संदर्भ में, विश्व बैंक की रिपोर्ट बैंकिंग क्षेत्र और वित्तीय सेवा संस्थानों में साइबर सुरक्षा

हमलों की एकाग्रता का संकेत देती है, जिसमें 2016 में साइबर सुरक्षा हमलों में 65% की उल्लेखनीय वृद्धि देखी गई, जो पिछले वर्ष की तुलना में 29% की वृद्धि को दर्शाता है। इसके अलावा, वैश्विक बैंक की रिपोर्ट बताती है कि मैलवेयर का उपयोग करके वित्तीय क्षेत्र के खिलाफ चोरी पिछले वर्ष की तुलना में 2015 में प्रति वर्ष 80% बढ़ी है, जबकि इन हमलों में 2015 में रिपोर्ट की गई घटनाओं का 38% हिस्सा था, जो 2014 में 23% था।

वित्तीय संस्थानों के सामने आने वाले साइबर अपराध पर चर्चा करने के लिए ग्रुप आईबी विशेषज्ञों के आकलन के आधार पर, वित्तीय संस्थानों के सामने आने वाले लगभग 99% साइबर अपराध पैसे की चोरी हैं, जिसने 2017 में कई कंपनियों को बर्बाद कर दिया, जैसे कि MDLZ और DLA Piper, पहचान की चोरी के अलावा, और इकिफैक्स उन पीड़ितों में से एक था जहाँ साइबर अपराधी संवेदनशील व्यक्तिगत जानकारी का उपयोग करते हैं और इसका उपयोग पहचान की चोरी के लिए करते हैं। 2018 में, विश्व आर्थिक मंच ने धोखाधड़ी और वित्तीय अपराधों पर ध्यान दिया, जिनकी राशि इस वर्ष एक ट्रिलियन डॉलर थी, जिसने निजी कंपनियों को 2017 में धन शोधन अपराधों से निपटने पर लगभग 8.2 बिलियन डॉलर खर्च करने के लिए प्रेरित किया।

साइबर सुरक्षा का उल्लंघन इस उद्योग के लिए सबसे गंभीर खतरों

में से एक बन गया है। साइबर अपराध और सुरक्षा सर्वेक्षण रिपोर्ट के अनुसार, मैलवेयर, फ़िशिंग, कंप्यूटर चोरी और बॉट हमले साइबर हमलों के लिए प्रचलित रणनीति हैं। तंजानिया ने कई साइबर अपराध घटनाओं के परिणामस्वरूप \$6 मिलियन का नुकसान उठाया है, जिससे देश को CCU और CERT बनाने के लिए मजबूर होना पड़ा है। आभासी दुनिया में गोपनीयता की रक्षा के लिए, नए सुरक्षा उपायों की आवश्यकता है। वांग एट अल., (2020) चार घटकों के माध्यम से साइबरनेटिक रक्षात्मक चक्र को प्राप्त करने के लिए साइबर-हमला प्रबंधन समाधान प्रदान करता है। साइबर हमले और जोखिम चिंता का एक प्रमुख स्रोत बन गए हैं। महत्वपूर्ण खोज यह थी कि चाहे कोई भी मजबूत हमला हो, इराकी निजी बैंक एक निश्चित स्तर की सुरक्षा बनाए रखते हैं।

साहित्य समीक्षा

अकेलो (2023)समकालीन नेटवर्क और डेटा-केंद्रित वातावरण में संगठनात्मक सूचना सुरक्षा एक महत्वपूर्ण मुद्दा है। जैसे-जैसे साइबर हमले अधिक लगातार और परिष्कृत होते जा रहे हैं, फर्मों को अपने संवेदनशील डेटा की गोपनीयता, अखंडता और उपलब्धता के लिए पर्याप्त जोखिम का सामना करना पड़ रहा है। यह दस्तावेज़ कॉर्पोरेट सूचना सुरक्षा से जुड़ी प्रमुख विशेषताओं और मुद्दों का अवलोकन प्रस्तुत करता है। यह बाहरी हमलों से बचाव के लिए फायरवॉल, घुसपैठ का पता लगाने वाली प्रणाली, एन्क्रिप्शन तकनीक और सुरक्षित कोडिंग पद्धतियों सहित कड़े सुरक्षा प्रोटोकॉल स्थापित करने की आवश्यकता को रेखांकित करता है। यह सुरक्षा घटनाओं की कुशलतापूर्वक पहचान करने और उनका समाधान करने के लिए निरंतर निगरानी, खतरे की खुफिया जानकारी के प्रसार और घटना प्रतिक्रिया क्षमताओं की आवश्यकता को रेखांकित करता है। य

अहमद (2024)कंपनी परिवर्तन में बढ़े हुए डिजिटलीकरण ने पर्याप्त लाभ दिए हैं, साथ ही सूचना सुरक्षा के लिए नई समस्याएं भी पेश की हैं। यह अध्ययन डिजिटल परिवर्तन अवधि के दौरान सामने आई साइबर सुरक्षा चिंताओं की जांच करना चाहता है, जो सूचना प्रणालियों पर केंद्रित है। उपयोग की गई शोध तकनीक इन कठिनाइयों की गहन समझ प्राप्त करने के लिए साहित्य और केस स्टडीज की गहन समीक्षा है। यह अध्ययन डिजिटल परिवर्तन के कार्यान्वयन में साइबर सुरक्षा से जुड़े कई महत्वपूर्ण मुद्दों की पहचान करता है, जिसमें मैलवेयर हमले, फ़िशिंग, अपर्याप्त नेटवर्क सुरक्षा और गोपनीयता उल्लंघन शामिल हैं। कारण विश्लेषण से पता चला कि अपर्याप्त प्रशिक्षण और सुरक्षा जागरूकता, सूचना प्रणालियों में खराब डिज़ाइन के साथ, प्राथमिक जोखिम कारक थे।

शुक्र (2023)रोजमर्रा की गतिविधियों में इंटरनेट ऑफ थिंग्स (IoT) के तेजी से विस्तार ने संभावित साइबर सुरक्षा कमजोरियों के बारे में महत्वपूर्ण चिंताएँ पैदा की हैं। नतीजतन, सक्रिय और सक्रिय प्रतिक्रियाओं की वास्तविक आवश्यकता है। यह पत्र विभिन्न IoT उपकरणों से जुड़े वर्तमान साइबर सुरक्षा चिंताओं और खतरों का व्यापक साहित्य मूल्यांकन करता है। इसके अतिरिक्त, यह संरचनात्मक रूपरेखाओं के साथ-साथ प्रस्तावित उपाय भी प्रस्तुत करता है। इसके अलावा, यह विभिन्न तरीकों से संभावित जोखिमों का पता लगाने और उनकी पहचान करने में सहायता करता है। इसके अलावा, यह IoT से संबंधित औद्योगिक और आर्थिक क्षेत्रों में शोध की कमियों को उजागर करके योगदान देता है। हमारे परिणाम संकेत देते हैं कि IoT प्रणालियों में प्राथमिक चिंताएँ साइबर अपराध और गोपनीयता की समस्याएँ हैं।

पेत्रु-क्रिस्टियन (2023)इस अध्ययन का उद्देश्य विकासशील जटिलता को स्पष्ट करना है, समकालीन साइबर युद्धों और उनके कई प्रभावों के बारे में पूरी जानकारी की तत्काल आवश्यकता पर प्रकाश डालना है। यह विश्लेषणात्मक उपकरणों की एक सरणी के साथ ऐसा करने का प्रयास करता है। 2011 से 2020 के दशक में, 50 उल्लेखनीय साइबर घटनाएँ साइबर जोखिम और सुरक्षा के क्षेत्र में महत्वपूर्ण केस स्टडी रही हैं। इन केस स्टडीज़ का विश्लेषण साइबर सुरक्षा के व्यापक प्रभावों और कठिनाइयों को समझने के लिए एक अलग दृष्टिकोण प्रदान करता है। इसके अतिरिक्त, 2011 से 2020 तक के 50 केस स्टडीज़ में से प्रत्येक अलग-अलग कठिनाइयों, परिणाम और अंतर्दृष्टि प्रस्तुत करता है। इकबाल (2024)अध्ययन लेख का सारांश दें, साइबर सुरक्षा में नए रुझानों और संभावित मुद्दों को समझने के महत्व पर जोर दें। उद्देश्यों, दृष्टिकोण और प्रमुख परिणामों की जांच करें। उभरते साइबर खतरों से निपटने और डिजिटल बुनियादी ढांचे की सुरक्षा के लिए सक्रिय रणनीतियों की आवश्यकता पर प्रकाश डालें।

साइबर सुरक्षा

बैंकिंग में साइबर सुरक्षा उपायों का अवलोकन

साइबर हमलों के विभिन्न प्रकारों को कई श्रेणियों में वर्गीकृत करके विस्तृत रूप से समझाया गया है। विभिन्न प्रकार के साइबर हमलों में SQL इंजेक्शन, सोशल इंजीनियरिंग, साइबरस्टॉकिंग, डेनियल ऑफ सर्विस अटैक, डिस्ट्रिब्यूटेड डेनियल ऑफ सर्विस अटैक, क्रॉस-साइट स्क्रिप्टिंग, एटीएम क्लोनिंग, पाइरेसी, मैन इन द मिडल अटैक, बर्थडे अटैक, रैनसमवेयर अटैक, बॉटनेट अटैक, ब्रूट फोर्स अटैक शामिल हैं। आईटी एक्ट के अनुसार, 2014 से 2016 तक 29 भारतीय राज्यों में से 10 में साइबर अपराधों में वृद्धि हुई है।

डिजिटल बैंकिंग में प्रमुख साइबर सुरक्षा खतरों को कई कारकों द्वारा सुव्यवस्थित किया जा सकता है, जैसे, अनएन्क्रिप्टेड डेटा, मैलवेयर, थर्ड-पार्टी सेवाएँ, स्फूफिंग, फ़िशिंग, आदि। कोविड के बाद के वर्षों में, दुनिया भर में साइबर खतरे बढ़ गए हैं, जिसमें प्रमुख बैंकिंग सर्वर हैकर्स द्वारा अपहृत किए जा रहे हैं। प्रमाणीकरण, गोपनीयता और डेटा अखंडता सहित कथित सुरक्षा कारक, इंटरनेट बैंकिंग सेवाओं का उपयोग जारी रखने के लिए ग्राहकों की इच्छा को महत्वपूर्ण रूप से प्रभावित करते हैं। यह सूचना सुरक्षा के मुख्य स्तंभों- गोपनीयता, अखंडता और उपलब्धता के महत्व को उजागर करता है - जो साइबर सुरक्षा खतरों से जुड़ी व्यापक चिंताओं के साथ संरेखित है।

पाकिस्तान के बैंकिंग क्षेत्र में साइबर अपराध के मामलों के विश्लेषण से पता चला है कि साइबर अपराध सीधे संगठनात्मक प्रदर्शन को प्रभावित करते हैं, जैसा कि पाकिस्तानी बैंकिंग क्षेत्र के भीतर अनुसंधान द्वारा उजागर किया गया है। अध्ययन प्रदर्शन पर साइबर अपराध की घटनाओं के पर्याप्त नकारात्मक प्रभाव की पहचान करता है, जो साइबर सुरक्षा खतरों से जुड़े हानिकारक परिणामों की व्यापक कथा को पुष्ट करता है।

हालाँकि, सूचना सुरक्षा जागरूकता एक महत्वपूर्ण शमन कारक के रूप में उभरती है, जो संगठनात्मक प्रदर्शन पर साइबर अपराधों के प्रतिकूल प्रभावों को कम करने में महत्वपूर्ण भूमिका निभाती है। अध्ययन में यह भी पाया गया कि साइबर अपराधों का संगठनात्मक प्रदर्शन पर प्रभाव सूचना सुरक्षा जागरूकता के स्तर के आधार पर भिन्न होता है। साइबर सुरक्षा जागरूकता बढ़ाना और वित्तीय संस्थानों के बीच सहयोग बढ़ाना डिजिटल बैंकिंग को अपनाने को बढ़ावा देने के लिए महत्वपूर्ण उपाय हैं, साथ ही

डिजिटल युग में वित्तीय लेनदेन की सुरक्षा और अखंडता सुनिश्चित करना भी महत्वपूर्ण है।

भारतीय बैंकिंग क्षेत्र और साइबर सुरक्षा

भारतीय बैंकिंग क्षेत्र में साइबर हमलों और बचाव रणनीतियों का विस्तृत विश्लेषण प्रस्तुत किया। अध्ययन में बैंकों द्वारा सामना किए जाने वाले विभिन्न साइबर खतरों पर प्रकाश डाला गया है, जिसमें 60% अधिकारियों ने ऑनलाइन पहचान चोरी की घटनाओं की रिपोर्ट की है, और सेवा से वंचित (DoS) हमलों, फ़िशिंग, विशिंग और स्पूफिंग पर महत्वपूर्ण चिंता व्यक्त की है, बाद वाले की पुष्टि 76% उत्तरदाताओं ने की है। अन्य कमजोरियों में दुर्भावनापूर्ण कोड, SQL इंजेक्शन और ब्रूट-फोर्स हमले शामिल हैं, जिसमें पहचान धोखा 80% अधिकारियों द्वारा बताई गई एक प्रमुख रणनीति है।

एन्क्रिप्शन, अद्वितीय लॉगिन, बायोमेट्रिक्स और नियमित एंटीवायरस अपडेट सहित मजबूत सुरक्षा उपायों को अपनाने के बावजूद, डेटा ग्रेन्युलैरिटी, उपयोगकर्ता पहुँच नीतियाँ और लॉगिंग गतिविधियों जैसे क्षेत्रों पर अधिक ध्यान देने की आवश्यकता है। अध्ययन सक्रिय उपायों के महत्व को रेखांकित करता है, जैसे घुसपैठ का पता लगाने वाले उपकरण, लगातार नीति समीक्षा और संदिग्ध गतिविधियों के लिए उपयोगकर्ता अलर्ट। इसके अलावा, हैकिंग, फ़िशिंग और पहचान की चोरी जैसे खतरों को कम करने के लिए साइबर सुरक्षा और सुरक्षित प्रथाओं के बारे में ग्राहकों को शिक्षित करने के लिए सरकारों और निजी संस्थाओं के साथ सहयोग करना आवश्यक है। मुंढे एट अल. (2024) द्वारा किए गए एक अन्य अध्ययन ने यह निष्कर्ष निकाला कि भारतीय बैंकिंग क्षेत्र का डिजिटल परिवर्तन महत्वपूर्ण साइबर सुरक्षा चुनौतियों के साथ-साथ महत्वपूर्ण अवसर भी लाता है। जैसे-जैसे बैंक तेजी से डिजिटल चैनल अपना रहे हैं, डेटा उल्लंघन और सिस्टम कमजोरियों सहित साइबर सुरक्षा जोखिम प्रमुख चिंता का विषय बन गए हैं।

डिजिटल संचालन की सुरक्षा के लिए AI, मशीन लर्निंग और ब्लॉकचेन जैसी उन्नत तकनीकों जैसे साइबर सुरक्षा उपायों में मजबूत निवेश आवश्यक है। विश्वास और परिचालन अखंडता बनाए रखने के लिए विकसित नियामक आवश्यकताओं का अनुपालन भी उतना ही महत्वपूर्ण है। फ़िनटेक फ़र्मों और प्रौद्योगिकी प्रदाताओं के साथ सहयोग सुरक्षा ढाँचे और उभरते खतरों के लिए अनुकूलनशीलता को और बढ़ा सकता है। इसके अतिरिक्त, डिजिटल उपकरणों को प्रभावी ढंग से लागू करने और प्रबंधित करने के लिए कार्यबल का निरंतर कौशल विकास महत्वपूर्ण है, जिससे एक सुरक्षित और लचीला बैंकिंग पारिस्थितिकी तंत्र सुनिश्चित होता है।

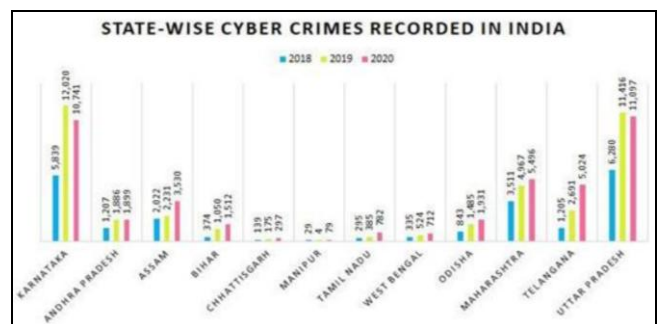
UPI, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, मोबाइल वॉलेट और QR कोड जैसी विभिन्न डिजिटल तकनीकों को अपनाने के साथ भारत में डिजिटल बैंकिंग में उल्लेखनीय प्रगति हुई है। डिजिटल बैंकिंग की प्रगति ने बैंकिंग और वित्तीय क्षेत्र में सुविधा, वैयक्तिकरण, दक्षता, पारदर्शिता और नवाचार को बढ़ाया है। हालाँकि, डिजिटल बैंकिंग सुरक्षा, डेटा गोपनीयता और तेजी से विकसित हो रहे प्रौद्योगिकी रुझानों के साथ तालमेल बनाए रखने के लिए निरंतर अनुकूलन की आवश्यकता से संबंधित चुनौतियाँ भी प्रस्तुत करती हैं।

बैंकिंग उद्योग में साइबर अपराध

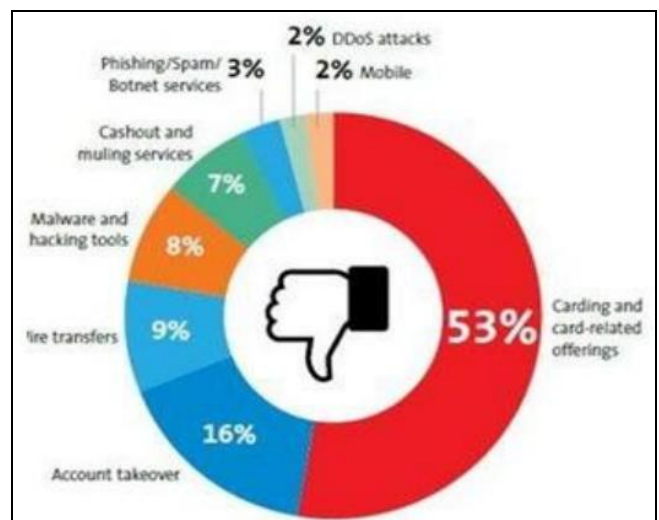
साइबर अपराध कोई भी अवैध गतिविधि है जो ऑनलाइन या

कंप्यूटर के माध्यम से होती है। दूसरे शब्दों में कहें तो डिजिटल कदाचार को साइबर अपराध भी कहा जाता है, जब कोई अपराधी कंप्यूटर या किसी अन्य इलेक्ट्रॉनिक डिवाइस और इंटरनेट का उपयोग करके कई तरह के अपराध करता है, जिसमें अनधिकृत पहुँच के माध्यम से धन हस्तांतरण और निकासी शामिल है।

आज की वैश्वीकृत दुनिया में, बैंकिंग उद्योग अपने ग्राहकों को क्रेडिट कार्ड सेवाओं और इंटरनेट बैंकिंग सहित कई तरह की सेवाएँ प्रदान करता है। "डेबिट कार्ड से ऑनलाइन भुगतान करना" उपभोक्ताओं को सभी बैंक सेवाओं तक चौबीसों घंटे पहुँच मिलती है, और वे अपने फ़ोन और इंटरनेट का उपयोग करके दुनिया के किसी भी स्थान से सुविधाजनक रूप से व्यवसाय कर सकते हैं और अपने खातों का प्रबंधन कर सकते हैं।" हालाँकि ये सेवाएँ उपयोगकर्ताओं के लिए मददगार हैं, जैसा कि हम सभी जानते हैं, इनका एक नकारात्मक पहलू भी है जिसमें डकैती और हैकर शामिल हैं।



बैंकिंग क्षेत्र से जुड़े साइबर अपराध के प्रकार



हैकिंग

हैकिंग एक प्रकार का साइबर अपराध है, जिसमें कोई व्यक्ति बैंकिंग वेबसाइट या ग्राहक खातों में सेंध लगाकर सुरक्षा उपायों को भंग करने का प्रयास करता है, या सिस्टम तक अनधिकृत पहुँच प्राप्त कर लेता है।

वायरस

यह एक प्रकार का स्व-प्रतिकृति सॉफ्टवेयर है जो संक्रमित करने के लिए दस्तावेज़ों या निष्पादन योग्य कोड में अपनी प्रतियाँ सम्मिलित करता है। एक निष्पादन योग्य फ़ाइल जिसे किसी

प्रोग्राम द्वारा संक्रमित किया गया है जो इसे अजीब तरह से व्यवहार करता है उसे वायरस कहा जाता है। यह ऑपरेटिंग सिस्टम और प्रोग्राम फ़ाइलों सहित निष्पादन योग्य फ़ाइलों से खुद को जोड़कर फैलता है। निष्पादन योग्य फ़ाइल लोड करने की प्रक्रिया वायरस को खुद को दोहराने का कारण बन सकती है। दूसरी ओर, वर्म ऐसे प्रोग्राम होते हैं जो पीड़ित के कंप्यूटर से खुद को कॉपी करने और अन्य कंप्यूटरों को प्रतियां भेजने की क्षमता रखते हैं। वर्म बिना किसी फ़ाइल को बदले या हटाए उपयोगकर्ता के कंप्यूटर से खुद की प्रतियों को दूसरे कंप्यूटरों में कॉपी और ट्रांसफर करते हैं।

स्पाइवेयर

ऑनलाइन बैंकिंग क्रेडेंशियल्स लेने और उन्हें धोखाधड़ी से इस्तेमाल करने का सबसे लोकप्रिय तरीका स्पाइवेयर है। स्पाइवेयर द्वारा कंप्यूटर और वेबसाइटों के बीच जानकारी एकत्र की जाती है या भेजी जाती है। अधिकतर, इसे झूठे "पॉप अप" विज्ञापनों द्वारा इंस्टॉल किया जाता है जो सॉफ्टवेयर डाउनलोड करने का अनुरोध करते हैं। इस तरह के सॉफ्टवेयर को उद्योग-मानक एंटीवायरस प्रोग्राम द्वारा खोजा और समाप्त किया जाता है, ज्यादातर कंप्यूटर को संक्रमित करने से पहले प्रोग्राम के डाउनलोड और इंस्टॉलेशन को रोककर।

फ़िशिंग

फ़िशिंग एक प्रकार का घोटाला है जिसमें प्रतिष्ठित स्रोतों से आने वाले ईमेल का उपयोग ग्राहक आईडी, आईपिन, सीवीवी नंबर, डेबिट/क्रेडिट कार्ड नंबर और समाप्ति तिथि जैसी व्यक्तिगत जानकारी चुराने के लिए किया जाता है। ईमेल स्फूटिंग और इंस्टेंट मैसेजिंग फ़िशिंग में इस्तेमाल की जाने वाली दो विधियाँ हैं। इस तरह की धोखाधड़ी में, जालसाज बैंक कर्मचारियों के रूप में खुद को पेश करते हैं और एक सीधा लिंक बनाते हैं जो इच्छित शिकार के ब्राउज़र को एक नकली वेबपेज पर ले जाता है जो वास्तविक बैंक वेबसाइट की नकल करता है। ग्राहक के खाते पर, प्राप्त गोपनीय जानकारी का उपयोग करके बाद में धोखाधड़ी वाले लेनदेन किए जाते हैं। इन दिनों, फ़िशर्स अपने अपराधों को अंजाम देने के लिए मोबाइल (वॉयस फ़िशिंग) और एसएमएस (स्मैशिंग) तकनीकों का भी उपयोग करते हैं।

फ़ार्मिंग

इंटरनेट का इस्तेमाल औषधीय कार्यों के लिए किया जाता है। हैकर्स यूआरएल में हेरफेर करते हैं ताकि जब कोई उपभोक्ता बैंक की वेबसाइट पर जाए, तो उसे एक नकली वेबसाइट पर ले जाया जाए जो बैंक की मूल वेबसाइट की नकल करती है।

ATMSKIMMIN गैड बिक्री अपराध बिंदु

मशीन कीपैड के ऊपर स्कीमिंग डिवाइस लगाना ताकि यह असली कीपैड जैसा लगे या कार्ड रीडर से जुड़ा कोई उपकरण लगाना ताकि यह मशीन का ही एक घटक लगे, एटीएम या पॉइंट-ऑफ-सेल (POS) सिस्टम में घुसने का एक तरीका है। इन डिवाइस पर सीधे क्रेडिट कार्ड की जानकारी चुराने वाले मैलवेयर भी इंस्टॉल किए जा सकते हैं। कार्ड नंबर और व्यक्तिगत पहचान संख्या (पिन) उन एटीएम से प्राप्त किए जा सकते हैं जिनमें स्कimmer सफलतापूर्वक इंस्टॉल किए गए हैं। फिर इन विवरणों की नकल की जाती है और धोखाधड़ी वाले लेनदेन में उनका उपयोग किया जाता है।

DNS कैशपॉइज़निंग

किसी संगठन के नेटवर्क में, DNS सर्वर का उपयोग कैश में पहले से प्राप्त केरी परिणामों को संग्रहीत करके समाधान प्रतिक्रिया समय को तेज़ करने के लिए किया जाता है। DNS सॉफ्टवेयर में भेद्यता का लाभ उठाकर, DNS सर्वर के विरुद्ध ज़हर भरे हमले किए जाते हैं। सर्वर उन सभी उपयोगकर्ताओं को गलत प्रविष्टियाँ प्रदान करेगा जो इसके स्थानीय कैश से समान अनुरोध करते हैं। बैंक क्लाइंट को आपराधिक-नियंत्रित सर्वर पर पुनर्निर्देशित किया जा सकता है, जहाँ मैलवेयर परोसा जा सकता है या उन्हें धोखाधड़ी वाली वेबसाइट के लिए अपनी लॉगिन जानकारी दर्ज करने के लिए धोखा दिया जा सकता है। IP स्फूटिंग एक ऐसी तकनीक है जिसका उपयोग क्लाइंट पर नियंत्रण पाने के लिए किया जाता है। इसमें बैंक की वेबसाइट के DNS रिकॉर्ड को एक DNS सर्वर से दूसरे DNS सर्वर में बदलना शामिल है, जिसमें उनके स्वामित्व वाले सर्वर का IP पता इस्तेमाल किया जाता है।

बैंकों पर साइबर अपराध का प्रभाव

दैनिक जीवन में मोबाइल नेटवर्क के प्रसार और सूचना एवं प्रौद्योगिकी (आईटी) की उन्नति ने वित्तीय सेवाओं को व्यापक दर्शकों के लिए अधिक सुलभ बना दिया है। लेकिन जहाँ तकनीकी प्रगति ने बैंकिंग सेवाओं को अधिक सुलभ और किफ़ायती बना दिया है, वहीं इसने साइबर हमलों का लक्ष्य बनने के जोखिम को भी बढ़ा दिया है।

साइबर अपराधियों द्वारा पैसे चुराने, कंपनियों की जासूसी करने और निजी कंपनी की जानकारी तक पहुँचने के लिए इस्तेमाल किए जाने वाले सरल तरीकों का बैंक के वित्त पर अप्रत्यक्ष प्रभाव पड़ता है। इन साइबर अपराधों का मुकाबला करने के लिए, बैंकिंग उद्योग को नियंत्रण प्रतिमान बनाने के लिए सरकारी अधिकारियों और निगरानी समूहों के साथ मिलकर काम करना चाहिए।

इस मामले में मुख्य रुचि का विषय बैंकिंग क्षेत्र में एक प्रभावी संकलन सेवा का अभाव है, जो साइबर अपराध के पैटर्न की पहचान करने तथा उनके आधार पर एक मॉडल तैयार करने में सक्षम हो।

भारतीय बैंकिंग प्रणाली

बैंकिंग का अर्थ

बैंकिंग दूसरों के लिए पैसे की सुरक्षा का व्यवसाय है। बैंक इस पैसे को उधार देते हैं, जिससे ब्याज मिलता है जो बैंक और उसके ग्राहकों के लिए मुनाफ़ा पैदा करता है।

बैंक एक वित्तीय संस्था है जिसे जमा स्वीकार करने और ऋण देने का लाइसेंस दिया गया है। लेकिन वे अन्य वित्तीय सेवाएँ भी प्रदान कर सकते हैं।

वित्तीय लेनदेन का अर्थ

वित्तीय लेनदेन एक समझौता या संचार है, जो खरीदार और विक्रेता के बीच भुगतान के लिए वस्तुओं, सेवाओं या परिसंपत्तियों का आदान-प्रदान करने के लिए होता है। किसी भी लेनदेन में दो या अधिक व्यवसायों या व्यक्तियों के वित्त की स्थिति में बदलाव शामिल होता है। एक वित्तीय लेनदेन में हमेशा एक या अधिक वित्तीय परिसंपत्तियाँ शामिल होती हैं, सबसे आम तौर पर पैसा या कोई अन्य मूल्यवान वस्तु जैसे सोना या चाँदी।

वित्तीय लेन-देन के कई प्रकार हैं। सबसे आम प्रकार, खरीद, तब होती है जब कोई वस्तु, सेवा या अन्य वस्तु पैसे के बदले उपभोक्ता

को बेची जाती है। ज्यादातर खरीद नकद भुगतान के साथ की जाती है, जिसमें भौतिक मुद्रा, डेबिट कार्ड या चेक शामिल हैं। भुगतान का दूसरा मुख्य रूप क्रेडिट है, जो बाद की तारीख में पुनर्भुगतान के बदले में धन तक तत्काल पहुँच प्रदान करता है।

भारत में बैंकों का वर्गीकरण

भारत में बैंकिंग प्रणाली का हिस्सा बनने वाले बैंकों को दो श्रेणियों में विभाजित किया जा सकता है - अनुसूचित बैंक और गैर-अनुसूचित बैंक।

अनुसूचित बैंक

भारत में बैंकिंग प्रणाली के अंतर्गत अनुसूचित बैंकों से तात्पर्य उन वित्तीय संस्थाओं से है जो भारतीय रिज़र्व बैंक अधिनियम, 1934 की दूसरी अनुसूची में सूचीबद्ध हैं। इस समावेशन का अर्थ है कि वे आरबीआई द्वारा निर्धारित विशिष्ट मानदंडों को पूरा करते हैं और इसके सख्त नियमों के अधीन हैं।

गैर-अनुसूचित बैंक

भारत में बैंकिंग प्रणाली के अंतर्गत गैर-अनुसूचित बैंक उन वित्तीय संस्थाओं को कहा जाता है, जो भारतीय रिज़र्व बैंक अधिनियम, 1934 की दूसरी अनुसूची में शामिल किए जाने के मानदंडों को पूरा नहीं करते हैं। अनुसूची से बाहर रखे जाने का अर्थ है कि वे अनुसूचित बैंकों की तुलना में अलग नियमों के तहत काम करते हैं।

निष्कर्ष

साइबर सुरक्षा को अलग-अलग तरीकों से तैयार किया जा सकता है, जिसका लोगों पर अलग-अलग प्रभाव पड़ता है। साइबर सुरक्षा एक जटिल और बहुआयामी क्षेत्र है जिसका कोई स्पष्ट नायक या अपराधी नहीं है। साइबर सुरक्षा को तैयार करने में असमर्थता ने उचित कार्रवाई करना और पर्याप्त नीतियाँ विकसित करना असंभव बना दिया है। किसी कंपनी की सुरक्षा के लिए प्रत्येक कर्मचारी के समर्थन की आवश्यकता होगी। अधिकतम प्रभावशीलता के लिए अनुकूलित चल रहे सुरक्षा जागरूकता कार्यक्रम के साथ, एक संगठन सभी कर्मियों द्वारा समर्थित साइबर सुरक्षा संस्कृति बना सकता है। जबकि कई उपयोगकर्ता ऑनलाइन वित्तीय और गैर-वित्तीय लेनदेन का उपयोग करते हैं, वे साइबर सुरक्षा नियमों से अनजान हैं।

संदर्भ

1. सेले एनएन, केंडा एस. क्या साइबर सुरक्षा के खतरे और जोखिम डिजिटल बैंकिंग को अपनाने पर प्रभाव डालते हैं? एक व्यवस्थित साहित्य समीक्षा. जर्नल ऑफ फाइनेंशियल क्राइम. 2024.
2. बामरारा ए, सिंह जी, भट्ट एम. भारत में साइबर हमले और बचाव रणनीतियाँ: बैंकिंग क्षेत्र का एक अनुभवजन्य मूल्यांकन. एसएसआरएन इलेक्ट्रॉनिक जर्नल. 2013.
3. मुंथे ई. भारतीय बैंकिंग क्षेत्र में डिजिटल परिवर्तन: अवसर और चुनौतियाँ. विभिन्न विषयों में ज्ञान का विकास-समकालीन रुझान और अग्रगामी नवाचार. 2024:103.
4. प्रभाकर एस. भारत में डिजिटल बैंकिंग के रुझान, अवसर और चुनौतियाँ: एक समीक्षा.
5. अल-दोसारी के, फ़ेतैस एन, कुकुकवर एम. बैंकिंग उद्योग के लिए आर्टिफिशियल इंटेलिजेंस और साइबर डिफेंस सिस्टम:

एआई अनुप्रयोगों और चुनौतियों का एक गुणात्मक अध्ययन. साइबरनेटिक्स एंड सिस्टम्स. 2022;55(2):302-330.

6. फराजी एमआर, शिकदर एफ, हसन एमएच, इस्लाम एमएम, अक्तर यूके. साइबर सुरक्षा में कृत्रिम बुद्धिमत्ता की भूमिका की जांच: वित्तीय लेनदेन में संभावित समाधानों को रोकने के लिए एक व्यवस्थित समीक्षा. इंटरनेशनल जर्नल. 2024;5(10):4766-4782.
7. आचार्य एस, जोशी एस. भारत में बैंकिंग संस्थानों पर साइबर हमलों का प्रभाव: सुरक्षा तंत्र और निवारक उपायों का एक अध्ययन. प्लार्व जर्नल ऑफ आर्कियोलॉजी ऑफ इजिप्ट/इजिप्टोलॉजी. 2020;17(6). आईएसएसएन 1567-214.
8. बुख्त टीएफएन, रज़ा एमए, अवान जेएच, अहमद आर. पाकिस्तान के बैंकों और उनके समाधानों पर लक्षित साइबर हमलों का विश्लेषण. इंटरनेशनल जर्नल ऑफ कंप्यूटर साइंस एंड नेटवर्क सिक्योरिटी. 2020;20(2).
9. जोवेदा एन, खान एमटी, पाठक ए. साइबर लॉड्रिंग: बांग्लादेश में बैंकिंग उद्योगों के लिए खतरा-प्रभावी कानूनी ढांचे और वित्तीय जानकारी की साइबर सुरक्षा की तलाश में. इंटरनेशनल जर्नल ऑफ इकोनॉमिक्स एंड फाइनेंस. 2019;11(10).
10. बाउवेरेट ए. वित्तीय क्षेत्र के लिए साइबर जोखिम: मात्रात्मक मूल्यांकन के लिए एक रूपरेखा. अंतर्राष्ट्रीय मुद्रा कोष वर्किंग पेपर, रणनीति, नीति और समीक्षा विभाग. 2019 मई 27.
11. साइबर सुरक्षा: खतरे, कारण, चुनौतियाँ, कार्यप्रणाली और औद्योगिक अनुप्रयोगों के लिए अत्याधुनिक समाधान. स्कूल ऑफ इलेक्ट्रिकल इंजीनियरिंग एंड कंप्यूटर साइंस, नेशनल यूनिवर्सिटी ऑफ साइंसेज एंड टेक्नोलॉजी. 2019.
12. चिगाडा जे, मैडज़िगा आर. कोविड-19 के दौरान साइबर हमले और खतरे: एक व्यवस्थित साहित्य समीक्षा. साउथ अफ्रीकन जर्नल ऑफ इंफॉर्मेशन मैनेजमेंट.
13. क्रिसैंटो जेसी, प्रेनियो जे. बैंकों के साइबर-सुरक्षा ढांचे को बढ़ाने के लिए नियामक दृष्टिकोण. फाइनेंशियल स्टेबिलिटी इंस्टीट्यूट. 2017 अगस्त. आईएसबीएन: 978-92-9259-080-2.
14. अंतर्राष्ट्रीय मुद्रा कोष. एक ऐसा संकट जैसा कोई और नहीं, एक अनिश्चित रिकवरी. वर्ल्ड इकोनॉमिक आउटलुक अपडेट. 2020 जून.
15. चेक प्वाइंट सॉफ्टवेयर टेक्नोलॉजीज लिमिटेड. चेक प्वाइंट रिसर्च: क्षेत्रवार साइबर हमले की श्रेणियाँ एच1 2020. 2020.

Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.



International Conference On

**Innovations and Development: A recent Trend
in Commerce, Science and Humanities**

Jointly Organized By



South Gujarat Chapter
RESEARCH FOUNDATION OF INDIA
रिसर्च फाउंडेशन ऑफ इंडिया
(South Gujarat Chapter)



Sponsored By



IC-IDTCSH-RFI/2025/225

This is to Certify that Prof./Dr./Mr./Ms./Mrs.

RAKESH KUMAR RAI

Participated in the International Conference On “Innovations and Development: A recent Trend in
Commerce, Science and Humanities Jointly Organized by South Gujarat Chapter–Research
Foundation of India & RFI-CARE on 02 February 2025 and Presented a Research Paper Titled

II

भारतीय बैंकिंग क्षेत्र में डिजिटल विस्तार और साइबर हमलों की बढ़ती प्रवृत्ति: चुनौतियों एवं नीतिगत उत्तरदायित्व का अध्ययन

in Technical Session:

Dr. Manish Dubey

President, Central India Board
Research Foundation of India

Dr. Ajay Jain

National Coordinator
Research Foundation of India

Prof. Dr. Ashok Kumar Gupta

Chief Managing Director
Research Foundation of India, RFI-CARE

Dr. Reshu Jain

Director
RFI-CARE

Dr. Sourabh Jain

Chairman & CEO
Research Foundation of India
Director, RFI-CARE

02 FEB
2025

www.care.researchfoundationofindia.com,

www.researchfoundationofindia.com



IC-RU-RFI/2024/244

28 DEC
2024



International Conference On

**A MULTIDISCIPLINARY APPROACH TOWARDS SUSTAINABILITY AND
DEVELOPMENT BY UNLOCKING NEW OPPORTUNITIES IN THE
WORLD OF CONSTANT DISRUPTION**

Jointly Organized By



**Renaissance
University, Indore**



RESEARCH FOUNDATION OF INDIA
रिसर्च फाउंडेशन ऑफ इंडिया
Research Foundation of India



Sponsored By



HERF



CERTIFICATE

This is to Certified that Prof./Dr./Mr./Ms./Mrs.

RAKESH KUMAR RAI

**Participated in the International Conference On “A MULTIDISCIPLINARY APPROACH TOWARDS
SUSTAINABILITY AND DEVELOPMENT BY UNLOCKING NEW OPPORTUNITIES IN THE WORLD OF CONSTANT
DISRUPTION” Jointly Organized by Renaissance University-Indore, RFI CARE & Research Foundation of India
on 28 December, 2024 and Presented a Research Paper Titled**

भारतीय बैंकिंग प्रणाली में साइबर सुरक्षा जोखिम प्रबंधन: तकनीकी, कानूनी एवं संस्थागत उपायों का तुलनात्मक विश्लेषण

in Technical Session: ||

Swapnil Kothari

CA Swapnil Kothari

Chancellor

Renaissance University, Indore

Rajesh Dixit

Prof. (Dr.) Rajesh Dixit

Vice-Chancellor

Renaissance University, Indore

Amit Kumar Hasija

Prof. (Dr.) Amit Kumar Hasija

Registrar

Renaissance University, Indore

Jayesh Shah

Prof. (Dr.) Jayesh Shah

Organizing Chair

Renaissance University, Indore

Ajay Jain

Dr. Ajay Jain

National Coordinator

Research Foundation of India

Ashok Kumar Gupta

Prof. Dr. Ashok Kumar Gupta

Chief Managing Director

Research Foundation of India, RFI-CARE

Sourabh Jain

Dr. Sourabh Jain

Chairman & CEO
Research Foundation of India
Director, RFI-CARE