



International Journal of Advance Studies and Growth Evaluation

डिजिटल भुगतान एवं बढ़ते साइबर धोखादड़ी पर विश्लेषणात्मक अध्ययन

*¹ Dimpal Agrawal

*¹ Assistant Professor, Department of Commerce, Naveen Govt College Chaple, Raigarh, Chhattisgarh, India.

Article Info.

E-ISSN: 2583-6528

Impact Factor (SJIF): 6.876

Peer Reviewed Journal

Available online:

www.alladvancejournal.com

Received: 13/Sep/2025

Accepted: 11/Oct/2025

सारांश:

आज का युग डिजिटल युग है, इस डिजिटल युग में डिजिटल भुगतान तेजी से हो रहा है इसलिए इस समय जो साइबर अपराध बढ़ रहा है उन कारणों को इस पत्र के माध्यम से जाना जा रहा है साथ ही इसे रोकने के लिए आवश्यक सुझाव भी जाने जाएंगे। व्यक्ति बहुत मेहनत से अपनी जमा पूंजी को निवेश करता है और साइबर अपराध होने से उसकी सारी जमा पूंजी चली जाती है व्यक्ति इससे बहुत निराश होता है बहुत कुछ करना चाहता है लेकिन कर नहीं पाता है वह पुलिस के पास भी सहायता के लिए नहीं जा पाता है इसलिए यह पेपर उन सभी व्यक्तियों को सचेत करेगा जो जाने अनजाने में डिजिटल साइबर अपराध के शिकार हो जाते हैं। इस शोध पत्र के लिए कुल 200 महिलाओं का डाटा लिया गया है क्योंकि परिकल्पना एवं उद्देश्य के अनुसार यह जाना गया है कि महिलाएं डिजिटल भुगतान कर सकती हैं या नहीं और कर सकती हैं तो उनके साथ साइबर अपराध हो रहा है या नहीं।

*Corresponding Author

Dimpal Agrawal

Assistant Professor, Department of
Commerce, Naveen Govt College
Chaple, Raigarh, Chhattisgarh, India.

मुख्य शब्द: डिजिटल भुगतान, साइबर अपराध।

प्रस्तावना:

अभी के समय में डिजिटल भुगतान तेजी से बढ़ रहा है चाहे वे पेटीएम, गूगल पे, फोन पे के द्वारा हो डिजिटल भुगतान बढ़ रहा है तकरीबन 75% लोग जिसमें महिला एवं पुरुष दोनों शामिल हैं डिजिटल रुप से भुगतान कर रहे हैं इसमें वे लोग भी डिजिटल भुगतान कर रहे हैं जो पढ़े-लिखे नहीं हैं लेकिन वे भी जागरूक होकर प्रशिक्षण प्राप्त कर इस कार्य को कर रहे हैं। जो फोन पे, गूगल पे, अमेजन, फ्लिप कार्ट ये सभी में आधार एवं पैन कार्ड अनिवार्य कर दिया गया है जिससे चाहे एक बैंक के जानकारी वे फोन पे, गूगल पे, डाले लेकिन जब साइबर अपराध होता है तो उससे सभी बैंक प्रभावित होते हैं।

साइबर धोखादड़ी (अपराध): साइबर धोखादड़ी (अपराध) अपराधियों द्वारा की जाने वाली अवैध गतिविधि है जिसमें हैकिंग, फिशिंग, पहचान की चोरी, रैनसमवेयर और मैलवेयर हमले शामिल हैं। साइबर अपराध अभी वर्तमान में इतना तेजी से बढ़ गया है कि लिंक को क्लिक करते ही लोगों के खाते से पैसे निकल जाते हैं यह कई रुपों में होने वाला एक साइबर अपराध है जैसे ओटीपी के द्वारा साइबर अपराध होना, लिंक को क्लिक करके खाते से पैसे गायब हो जाना आजकल तो ऐसे तरीके से पैसे गायब हो जाते हैं जिनमें अपराधी पीडीएफ फाइल बनाकर सेंड करते हैं और उसको ओपन करते ही पैसे गायब हो जाते हैं। अभी के समय में तकरीबन 80 प्रतिशत लोग इस साइबर अपराध के शिकारी हो रहे हैं। पढ़े लिखे

लोग हैं या अनपढ़ दोनों में कोई भिन्नता नहीं है अर्थात् पढ़े-लिखे लोग इसके ज्यादा शिकार हो रहे हैं। पहले तो ऐसा था कि मोबाइल में ओटीपी बताते ही पैसे गायब हो जाते हैं लेकिन अभी के समय में साइबर अपराधियों ने इतना कर दिया है कि जैसे ही हमने अंजान लिंक में क्लिक किया वैसे ही पैसे गायब हो जाते हैं। कुछ एप ऐसे हैं जिसको कि हम डाउनलोड किए उसमें डिटेल डालते ही खाते से पैसे गायब हो जाते हैं यदि साइबर अपराध की बात करे तो यह तेजी से बढ़ रहा है और यह लोगों के मन में इतना हो रहा है कि लोग डिजिटल भुगतान नहीं करना चाह रहे हैं उन्होंने अपने मोबाइल से गूगल पे, फोन पे, जैसे एप हटा दिए हैं इनका सोचना है कि न तो डिजिटल भुगतान होगा और न साइबर धोखादड़ी तो यही डर है कि लोग जितनी तेजी से डिजिटल भुगतान कर रहे हैं उतना ही डिजिटल भुगतान से पीछे भाग रहे हैं।

आरबीआई के आंकड़ों से पता चलता है कि दो सालों में डिजिटल धोखधड़ी के मामलों में 10 प्रतिशत से ज्यादा की बढ़ोत्तरी हुई है। NCRP (National Crime Report Organisation) ने बताया कि यह अपराध 2020 जब भारत देश में कोविड-19 आया तब से ज्यादा बढ़ा है और अबकि इन सालों में 2020 से 2024 तक की बात की जाए तो तेजी से बढ़ोत्तरी हुई है और तकरीबन 15000 करोड़ का नुकसान हुआ है।

संबंधित साहित्य का अध्ययन: फर्ग्यूसन, के.जी एवं अन्य (2019) ने अपने शोध अध्ययन “अफ्रीका में डिजिटल भुगतान-मांग,

प्रौद्योगिकी और विनियमन डिजिटल भुगतान प्रणालियों को कैसे बाधित करते हैं मैं बताया कि आज का समय किस तरीके से डिजिटल तरीके से भुगतान कर रहा है उन्होंने अपने शोध अध्ययन में डिजिटल भुगतान के विभिन्न तरीकों के बारे में बताया।

परिकल्पना

1. **HO:-** जो व्यक्ति पढ़े लिखे नहीं है वे आनलाइन भुगतान नहीं करते हैं।
2. **H1:-** जो व्यक्ति पढ़े लिखे नहीं है वे आनलाइन भुगतान करते हैं।
3. **HO:-** पुरुषों की तुलना में महिलाएं डिजिटल भुगतान नहीं करती हैं।
4. **HO:-** पुरुषों की तुलना में महिलाएं डिजिटल भुगतान करती हैं।

उद्देश्य

1. ग्रामीण क्षेत्र में हो रहे डिजिटल भुगतान को जानना।
2. पुरुषों की तुलना में स्त्रियों की भुगतान क्षमता को जानना।

अध्ययन का क्षेत्र: अध्ययन के लिए डाटा का एकत्रीकरण प्रश्रावली के माध्यम से प्रश्नों का एकत्रीकरण करके किया गया एवं कई व्यक्ति जिन पर यह साइबर अपराध हुआ था उस व्यक्ति से प्रत्यक्ष रूप से मुलाकात कर उनसे पूछा गया इस तरह का चयन कर निष्कर्ष निकाला गया और आंकड़ों के लिए सरकारी आंकड़ों अभी वर्तमान में डिजिटल साइबर अपराध हो रहे हैं उस पर निकाला गया इस प्रकार रैण्डम आधार पर 200 महिलाओं का एवं 100 पुरुषों को लिया गया और उनसे प्रश्न पूछा गया यह छ.ग. के किसी विशेष जिले से नहीं बल्कि 33 जिलों में ग्रामीण क्षेत्र का चयन कर उनसे डाटा का एकत्रीकरण किया गया।

अध्ययन की विधि: इस शोध अध्ययन के लिए काई स्कावर टेस्ट लगाया गया इसके आधार पर निष्कर्ष प्रस्तुत किया गया कि डिजिटल अपराध की स्थिति किस प्रकार की है और महिलाओं पर इसका कितना प्रभाव पड़ रहा है इस तरह से इस टेस्ट के माध्यम से इसका पता लगाया गया।

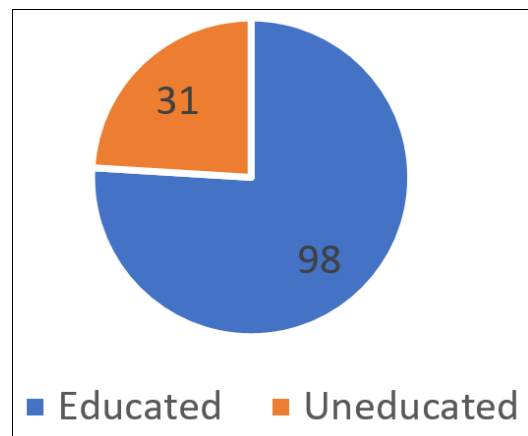
तालिका क्र. 1: महिलाओं द्वारा डिजिटल भुगतान की स्थिति

आयु	डिजिटल भुगतान करने वाली महिलाएं	%
25-30	36	18%
30-35	62	31%
35-40	47	23-5%
40-45	38	19%
45 वर्ष से अधिक	27	13-5%
योग	200	100%

इस तालिका में दिखाया गया है कि महिलाएं भी डिजिटल भुगतान करती हैं जो 25 से 30 वर्ष की आयु की महिलाएं हैं उनकी संख्या 36 है, 30 से 35 वर्ष की आयु की महिलाओं की संख्या 62 है 35 से 40 वर्ष की आयु की महिलाओं की संख्या 47 है 40 से 45 वर्ष की आयु की महिलाओं की संख्या 38 है तथा 45 वर्ष से अधिक आयु की महिलाओं की संख्या 27 है इसका तात्पर्य है कि महिलाएं भी डिजिटल भुगतान करती हैं।

तालिका क्र. 2: महिलाओं की साक्षरता निरक्षरता की स्थिति

महिलाएं	संख्या
साक्षर	98
निरक्षर	31
योग	129



रेखाचित्र क्र. 2: महिलाओं की साक्षरता निरक्षरता की स्थिति

परिकल्पना का सत्यापन: इन दोनों टेबल एवं रेखाचित्र के माध्यम से स्पष्ट होता है कि χ^2 का परिगणित मूल्य 3.967 है जो कि सारणी मूल्य 3.841 से कम है अतः हमारी यह शून्य परिकल्पना कि महिलाएं डिजिटल भुगतान नहीं करती हैं यह असत्य पाई गई अर्थात् महिलाएं चाहे वे ग्रामीण क्षेत्र की हो या शहरी क्षेत्र की वे डिजिटल भुगतान करती हैं।

उद्देश्यों की पूर्ति

1. ग्रामीण क्षेत्र में डिजिटल भुगतान की स्थिति काफी अच्छी है हम यह सोचते हैं कि ग्रामीण क्षेत्रों में डिजिटल भुगतान नहीं हो रहा है या कम हो रहा है लेकिन ऐसा नहीं है डिजिटल भुगतान ग्रामीण क्षेत्रों में भी तेजी से हो रहा है।
2. पुरुषों की तुलना में स्त्रियों की भुगतान क्षमता को जानना यह मानकर चलते हैं कि ग्रामीण क्षेत्रों में महिलाएं डिजिटल भुगतान नहीं करती हैं लेकिन ऐसा नहीं है जब महिलाओं से पूछा गया तो उसमें 80% महिलाओं ने कहा कि वे डिजिटल भुगतान करती हैं।



रेखाचित्र क्र. 2: साइबर अपराध का बढ़ता परिदृश्य

इस टेबल को देखने के बाद पता चलता है कि इसमें वर्ष में होते हुए डिजिटल साइबर अपराध को दर्शाया गया कि किस तरह से वर्ष 2023 से 2025 तक स्थिति किस प्रकार की है अर्थात् 2023 में साइबर अपराध बढ़ रहा है और 2025 तक यह और अधिक बढ़ जाएगा यदि हम इसमें सावधानी नहीं बरते तो हम भी इस साइबर फ्रॉड के शिकारी बन जाएंगे इसलिए इस चित्र के माध्यम से संदेश दिया जा रहा है कि हमें साइबर फ्रॉड से बचना चाहिए।

कुछ व्यक्तियों पर हुए साइबर अपराध

1. **एम एल पटेल:** ये छ.ग. के रायगढ़ जिले के निवासी हैं पेशे से वे सहायक प्राध्यापक हैं एक दिन हैकर्स ने इनसे क्रेडिट कार्ड की जानकारी पूछ कर इनके खाते से 5 लाख रुपए उड़ा लिए जब

इनके खाते से 5 लाख रुपए उड़ गए ये मानसिक रुप से बहुत परेशान हो गए कि इनके मेहनत की कमाई को हैकर्स ने उड़ा लिए ये मानसिक रुप से बहुत परेशान रहते थे इन्होंने पुलिस में एफआईआर दर्ज की और उससे इन्हें सहायता मिली और जो हैकर्स ने इनके पैसे खाते से उड़ाए थे पुलिस ने उनका पता लगाकर उनके पैसे वापस कराए इस तरह से साइबर अपराध से बचे और उसके बाद ये सचेत हो गए और इन्होंने किसी से भी अपनी जानकारी साझा करने की सलाह दी।

2. **राजन अग्रवाल:** ये छ.ग. के कोरबा जिले के रहने वाले है ये एक व्यापारी है इन्होंने अपनी मोबाईल में आए लिंक को टच कर दिया और टच करते ही इनका मोबाईल हैक हो गया ये बहुत परेशान हो गए और इनकी लिंक बहुत अच्छी थी इसलिए इन्होंने अपनी शिकायत दर्ज करा के अपने आप को नुकसान होने से बचा लिया लेकिन इन्होंने अपना डाटा पूरा खो दिया इसलिए इन्होंने भी किसी भी अंजान लिंक पर टच न करने की सलाह दी।
3. **टीनी अग्रवाल:** ये छ.ग. के रायगढ़ जिले की निवासी है ये एक गृहणी है लेकिन आनलाइन रुप में व्यवसाय भी करती है एक दिन इन्होंने मोबाइल में क्रोम में देखते-देखते गलत साइट में जाकर के टच कर दिया और उसके बाद इनका मोबाईल हैक हो गया उस समय इनके खाते में पैसे थे और इनका फोन पे, गूगल पे सब हैक हो गया बहुत दिनों तक इन्होंने उसे ठीक करने के लिए काम किया बहुत दिनों तक कोशिश करने के बाद इनका मोबाईल ठीक हुआ इन्होंने सलाह दी कि यदि गूगल पे हम कुछ सर्व करते है तो हमें अंजान साइट में नहीं जाना चाहिए।

सुझाव

व्यक्ति जो पैसे कमाते है वे दिन रात मेहनत करके अपनी छोटी-छोटी बचतों को इकट्ठा करके करता है और साइबर फ्रॉड उसके सारे पैसे सिर्फ एक मिनट में खाते से निकाल देता है इसलिए आरबीआई को इसके लिए एक ऐसा साफ्टवेयर बनाना चाहिए जिसमें साइबर अपराध जो बढ़ रहा है उसमें नियंत्रण हो और जो पैसे खाते से अपराधियों के द्वारा उड़ा दिए जाते है उसके लिए ऐसे सिस्टम होना चाहिए जिससे कि जैसे ही वे ये सोच रखे है कि किसी के साथ इस तरह का साइबर अपराध करे उन्हें तुरंत सजा हो ताकि अपराधी ऐसा करने की सोचे भी नहीं ऐसा सिस्टम आरबीआई को करना चाहिए कि यदि किसी के खाते से पैसे गायब हो जाए तो भी वह जिसने गायब किए है उसकी रिकवरी ब्याज सहित हो जाए। सुरक्षा के लिए ऐसा भी हो कि जैसे अगर व्यक्ति को पता चले कि साइबर अपराध हो रहा है तो आरबीआई के द्वारा ऐसा करना चाहिए कि जिस व्यक्ति को हमें पैसे देना है केवल उसी को हो अन्य को नहीं तो काफी हद तक साइबर अपराध पर नियंत्रण किया जा सकेगा।

निष्कर्ष:

वैसे तो आज के समय में जितना तेजी से डिजिटल भुगतान बढ़ रहा है उतनी तेजी से साइबर अपराध भी बढ़ रहा है आरबीआई के द्वारा समय-समय पर गाइड लाइन दी जाती है कि अनजान लिंक पर क्लिक न करे तथा अपनी जानकारी किसी के साथ साझा न करे इसके अलावा आरबीआई ने एक नई जानकारी भी दी है कि यदि हम किसी को भुगतान करते है या भुगतान प्राप्त करते है तो हमें मोबाईल नहीं देना चाहिए क्यूआर कोड देना चाहिए ताकि जो साइबर अपराध करने वाले व्यक्ति है उन्हें जानकारी नहीं हो मोबाईल नम्बर नहीं होगा तो वे कॉल या मैसेज से परेशान नहीं करेंगे। छ.ग.में यह समस्या तेजी से बढ़ रही है इसलिए सरकार ने रायपुर में साइबर अपराध के लिए पुलिस थाना खोला है जिसमें केवल साइबर अपराध जो बढ़ रहे है उन्ही समस्या का जल्दी से निपटारा हो सके। आरबीआई यह भी

दिशा निर्देश दे रहा है कि हमें एप में सावधानी रखनी चाहिए यदि अंजान लिंक आए तो उस पर क्लिक नहीं करना चाहिए इसलिए आरबीआई यह दिशा निर्देश लोगों को जागरूक करने के लिए विज्ञापन के माध्यम से दे रही है। आरबीआई के द्वारा अभी वर्तमान में ऐसा किया कि यदि हमें किसी व्यक्ति को 5000 से ज्यादा देना है तो उसका पैन कार्ड नम्बर देना होगा यह एक अच्छी पहल है जिससे कि काफी हद तक साइबर अपराध से बचा जा सके। आजकल फोन पर डिजिटल अरेस्ट जैसे फ्रॉड हो रहे है इसके लिए फिरौती मांगी जा रही है अपनी तरफ से रिजर्व बैंक ऑफ इंडिया जनता को जागरूक कर रहा है कि ये सभी फ्रॉड है और हम इनके झांसे में न पड़े लेकिन फिर भी बहुत से लोग इस प्रकार के साइबर क्राइम के शिकार हो रहे है इसके लिए हमें जागरूक रहने की आवश्यकता है साइबर अपराध तेजी से बढ़ रहा लोग अपने जमा पूंजी को अब बैंक में रखने से भी डर रहे है डिजिटल लेन-देन होने के बाद भी डर बना हुआ है इसलिए हमें जागरूक होने के साथ समझना भी होगा कि किस तरह से इस फ्रॉड से बचा जा सके।

References

1. Neelam Marwah. *et al.* (2020) "A study of electronic payment system doi:10.1088/1757-899/767/1/01/2008
2. Fatonah S (2018). "A Review of E-payment system in E-commerce doi:10/1088/1742-6596/1140/1/01/2023
3. Peralta-Ochoa AM, Chaca-Asmal PA, Guerrero-Vásquez LF, Ordoñez-Ordoñez JO, Coronel-González EJ. Smart Healthcare Applications over 5G Networks: A Systematic Review [Review of Smart Healthcare Applications over 5G Networks: A Systematic Review]. *Applied Sciences*. 2023; 13(3):1469. Multidisciplinary Digital Publishing Institute. <https://doi.org/10.3390/app13031469>
4. Pradhan P, Costa L, Rybski D, Lucht W, Kropp JP. A Systematic Study of Sustainable Development Goal (SDG) Interactions. *Earth s Future*. 2017; 5(11):1169. <https://doi.org/10.1002/2017ef000632>
5. Pwavodi J, Ibrahim AU, Pwavodi PC, Al-Turjman F, Mohand-Said A. The role of artificial intelligence and IoT in prediction of earthquakes: Review. *Artificial Intelligence in Geosciences*. 2024; 5:100075. <https://doi.org/10.1016/j.aig.2024.100075>
6. Qin Z, Li FY, Li GY, McCann JA, Ni Q. Low-Power Wide-Area Networks for Sustainable IoT. *IEEE Wireless Communications*. 2019; 26(3):140. <https://doi.org/10.1109/mwc.2018.1800264>
7. Sahu SK, Mazumdar K. Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance. *Frontiers in Artificial Intelligence*, 2024, 7. <https://doi.org/10.3389/frai.2024.1397480>
8. Savec VF, Jedrinović S. The Role of AI Implementation in Higher Education in Achieving the Sustainable Development Goals: A Case Study from Slovenia. *Sustainability*. 2024; 17(1):183. <https://doi.org/10.3390/su17010183>
9. Shehab M, Kassem I, Kutty AA, Küçükvar M, Onat NC, Khattab T. 5G Networks Towards Smart and Sustainable Cities: A Review of Recent Developments, Applications and Future Perspectives [Review of 5G Networks Towards Smart and Sustainable Cities: A Review of Recent Developments, Applications and Future Perspectives]. *IEEE Access*. 2021; 10:2987. Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/access.2021.3139436>