© June 2025 | V-IJCELM | JU2504 | Volume 1 | Issue 1 | ISSN: ISSN: 3107-7536 (Online)
Vyavahāra: International Journal of Commerce, Ethics, Law & Management

The Dark Side of Digital Marketing: Understanding Financial Fraud in the Digital Age

Dr. D. Venkadesh
Assistant Professor and Research Advisor
PG and Research Department of Commerce
A.V.V.M.Sri Pushpam College.
Thanjavur District
prof.d.venkadesh@gmail.com

Ramya.S
Research Scholor
A.V.V.M.Sri Pushpam College.
Thanjavur District

Abstract: The rapid digitization of the banking industry has brought about a double-edged transformation while it has enhanced convenience and accessibility for customers; it has simultaneously opened new avenues for cybercriminals. In today's digital landscape, efficient and robust fraud detection systems have become indispensable to maintaining the integrity of banking operations and ensuring the safety of customer assets. As banks continue to expand their online services to meet growing customer expectations, they also inadvertently increase the potential target base for fraudsters operating in the cyber world.

This growing digital exposure makes it essential to understand, analyze, and mitigate cyber threats. Hence, this study draws upon a wide range of scholarly articles and research papers accessed from reputable databases, offering comprehensive insights into the nature of banking fraud, preventive technologies, and the evolving strategies used by both attackers and defenders in the financial ecosystem.

Key Words: Digital marketing, Financial Fraud, Online scams, Fraud detection, Phishing attacks, Social Media Fraud, E-commerce fraud, Fraud prevention, AI in fraud detection.

Introduction:

Digital marketing has revolutionized how businesses connect with consumers, offering cost-effective and wide-reaching tools to promote products and services. From social media campaigns to search engine optimization, digital marketing channels have become

indispensable in today's economy. However, the very attributes that make digital marketing so impact its accessibility, scalability, and technological reliance also make it vulnerable to exploitation by malicious actors.

Financial fraud in digital marketing is a growing concern, characterized by deceptive practices such as phishing, fake advertisements, click fraud, and identity theft. These fraudulent activities harm individual consumers and tarnish legitimate businesses' reputations, leading to significant economic losses globally. According to industry reports, billions of dollars are lost annually due to online scams leveraging digital marketing tools.

The intersection of digital marketing and financial fraud presents a critical challenge in the digital age. Understanding how fraudsters manipulate digital platforms to deceive consumers and businesses is essential for crafting effective prevention strategies. This paper explores the mechanisms of financial fraud in digital marketing, examines real-world case studies, and proposes actionable solutions to mitigate risks. Addressing this issue is vital to ensuring trust in digital platforms and safeguarding the interests of businesses, consumers, and regulatory bodies.

Definition of Key Terms:

- **Digital Marketing:**
  Digital marketing refers to the use of online platforms, tools, and strategies to promote products, services, or brands to a targeted audience. It encompasses various channels such as social media, search engines, email, websites, and mobile apps to engage consumers and drive business growth. Key elements of digital marketing include content creation, search engine optimization (SEO), pay-per-click advertising (PPC), and analytics-driven campaigns, all aimed at improving visibility, customer engagement, and sales in the digital space.
- **Financial Fraud:**
  Financial fraud involves deceptive practices aimed at illegally obtaining money, property, or other valuable assets. In the context of digital platforms, it often includes activities such as phishing (tricking individuals into sharing sensitive information), click fraud (manipulating online advertising metrics), fake e-commerce sites, and scams conducted through email, social media, or fraudulent advertisements. Financial fraud can result in

substantial financial losses, damaged trust, and compromised personal or corporate data, affecting both individuals and organizations.

Research Objectives:

- To analyze the intersection of digital marketing and financial fraud.
- To identify methods used by fraudsters to exploit digital marketing platforms.
- To explore the impact of financial fraud on consumers, businesses, and the digital economy.
- To assess the role of technology (e.g., AI, machine learning) in both perpetrating and preventing fraud.
- To examine the effectiveness of existing regulatory frameworks in combating digital marketing fraud.
- To propose mitigation strategies for businesses and consumers to reduce exposure to digital marketing fraud.
- To analyze consumer awareness and digital literacy levels in preventing financial fraud.
- To investigate case studies of digital marketing fraud incidents and their resolution.

Literature Review:

The growing trends of internet has created a vast arena of services to the customers such as online banking, online shopping, digital payments for even small amounts, bill payments etc. These activities have provided new vectors for fraudulent activities. The emergence of robust and novel digital platforms has changed the scenario in the world of finance. The damage caused by world-wide cyber-crimes is estimated to cost $ 10.5 trillion per year by 2025. Threats and attacks on online banking are of many types such as malware, phishing , password cracking, port scanners, server bugs, packet sniffers, denial of service attack, Trojans, malicious hacking, mobile viruses etc.

Traditional methods of fraud detection often rely on static rule-based systems or isolated machine learning models that fail to keep pace with the evolving nature of fraudulent activities. Modern fraudsters exploit vulnerabilities in digital infrastructures. The efficacy of fraud detection system directly influences the ability of financial institutions to prevent

fraudulent transactions, reduce false positives and manage operational costs. It enhances the overall efficiency and reliability of digital banking services.

It is important to the financial institutions to maintain security and trustworthiness of digital banking ecosystem. Supervised learning techniques are useful where historical fraud patterns are well-documented. And Unsupervised learning techniques excel in detecting unknown fraud patterns.

Trends in Digital Marketing Fraud

- **Phishing Attacks via Ads and Emails:** Fraudsters increasingly use targeted phishing campaigns through digital ads, social media posts, and emails to trick users into revealing sensitive information such as login credentials or financial details. These deceptive ads often appear as legitimate offers from well-known companies.
- **Click Fraud:** Click fraud occurs when fraudsters artificially inflate the number of clicks on digital ads (e.g., Google Ads or Facebook Ads), either manually or through automated bots. This results in businesses paying for clicks that do not lead to legitimate customer engagement, driving up advertising costs and damaging ROI.
- **Fake E-commerce and Investment Websites:** With the growth of online shopping, fraudsters create counterfeit e-commerce platforms that mimic legitimate businesses, often promoting fake products or investment schemes. These websites lure consumers with attractive offers, only to steal payment details or deliver non-existent goods.
- **Social Media Scams:** Fraudulent campaigns on social media platforms, such as fake giveaways or pyramid schemes, have become prevalent. Fraudsters create fake influencer accounts or mimic well-known brands to convince users to make payments or provide personal information under false pretences.
- **Ad Fraud Networks:** Fraudsters create fake networks of ad impressions and clicks by using bots to simulate real user interactions with online ads. This can occur through fake apps or websites that generate fraudulent ad traffic, leading businesses to waste money on non-existent views and clicks.
- **Malware and Ransomware Attacks through Ads:** Malicious software (malware) is increasingly being distributed through fraudulent digital ads. When clicked, these ads can download malware onto users' devices, stealing personal information, tracking online behavior, or even demanding ransom payments to unlock compromised files.

- **Fake Reviews and Testimonials:** Fraudsters manipulate the credibility of online businesses by posting fake reviews or testimonials on websites, social media, and e-commerce platforms. These fraudulent reviews often mislead consumers into purchasing products or services that do not meet expectations, or in some cases, may not even exist.
- **Influencer Fraud:** With the rise of influencer marketing, fraudsters exploit influencers by faking engagement metrics (e.g., likes, followers) or by promising large returns to businesses who unknowingly collaborate with them. This leads to businesses wasting marketing budgets on ineffective partnerships.
- **Traffic Fraud and Bot-Driven Content:** Automated bots are used to generate fake traffic and engagement on websites, content, and social media platforms. This fraud skews analytics and can trick businesses into thinking their campaigns are more successful than they actually are, resulting in misguided marketing strategies.
- **Fake Scholarships and Financial Aid Scams:** Digital marketing is used to promote fake scholarship and financial aid schemes, targeting students and parents. Fraudsters often promise financial assistance or easy loans, requiring personal and financial details in exchange, only to misuse that information for identity theft or financial scams.

Role of Technology

AI/ML in both Committing and Combating Fraud:

- **AI/ML in Committing Fraud**
    - **Bot-driven Fraud**: Fraudsters use AI and machine learning algorithms to automate the creation of fake accounts, generate fake clicks, and manipulate traffic in digital marketing campaigns. These bots can mimic human behavior, making it difficult to distinguish legitimate users from fraudulent ones.
    - **Phishing and Deepfake Technology**: AI-driven tools are used to create realistic phishing emails or fraudulent ads that appear highly credible, tricking users into sharing sensitive information. Additionally, deepfake technology allows fraudsters to manipulate videos and images to impersonate trusted brands or individuals, increasing the effectiveness of scams.
    - **Fake Reviews and Testimonials**: AI can be used to generate fake reviews or testimonials in bulk, enhancing the credibility of fraudulent products or services.

These reviews are tailored to specific customer personas, making them appear more authentic and convincing.

- **AI/ML in Combating Fraud**
  - **Fraud Detection and Prevention**: Machine learning algorithms are employed by businesses to analyze large datasets and identify unusual patterns or anomalies that may indicate fraudulent activity, such as click fraud or fake reviews. These systems can detect discrepancies in real time and flag suspicious activities automatically.
  - **Predictive Analytics**: AI can predict fraudulent behaviours by analyzing historical data and identifying patterns that are characteristic of fraudsters. This allows businesses to proactively identify and block fraudulent actions before they result in significant financial damage.
  - **Automated Fraud Prevention Tools**: AI-powered tools, such as CAPTCHA systems, biometric verification, and behavioral analysis, are used to prevent fraudulent activities like account takeover or payment fraud by analyzing user behavior and interactions to ensure authenticity.

Social Media Platforms as Tools for Fraud:

- **Phishing Scams on social media:** Social media platforms are increasingly used for phishing scams, where fraudsters create fake profiles or pages that appear to be legitimate brands or individuals. These fake profiles often engage with users through direct messages, offering fake deals or fraudulent services that steal personal information or money.
- **Fraudulent Ads and Fake Influencers:** Social media platforms are ripe for fraudulent ads and scams. Fraudsters often create deceptive ad campaigns that appear to promote legitimate products or services. These ads may lead to counterfeit e-commerce sites or fake investment opportunities. Furthermore, fake influencers with inflated follower counts or fake engagement metrics can mislead businesses into investing in non-performing campaigns, causing financial losses.
- **Fake Giveaways and Contests:** Fraudsters often run fake giveaway campaigns on social media, luring users with the promise of free products or rewards. To participate, users are asked to share personal information or make small payments, only to find

that the giveaway is a scam. These fraudulent campaigns exploit social media's wide reach and the trust users have in these platforms.

- **Crowd sourced Fraud through social media:** Fraudsters exploit the viral nature of social media by orchestrating scams that leverage large crowds of unsuspecting users. For example, they may promote fraudulent crowdfunding campaigns or fake charity drives that deceive people into donating money to non-existent causes.
- **Impersonation and Brand Hijacking:** Social media platforms are often used by fraudsters to impersonate well-known brands, celebrities, or organizations. They create fake profiles that resemble the real entities to trick followers into engaging with fraudulent content, such as fake promotions or product offers.

The role of AI/ML and social media platforms in both enabling and preventing fraud is a double-edged sword. While these technologies can be leveraged by fraudsters to increase the scale and sophistication of scams, they also present powerful tools to detect and mitigate fraudulent activities in real time.

Challenges and Limitations:

Challenges in Detecting Fraud: Sophistication of Techniques

- **Evolving Fraudulent Techniques:** Fraudsters continuously evolve their tactics, making it difficult to stay ahead of emerging threats. With the use of AI, machine learning, and automation, fraudsters can mimic human behaviour, creating fake clicks, reviews, or social media engagements that appear authentic. These increasingly sophisticated methods challenge traditional detection systems and require constant adaptation and innovation from businesses and regulatory bodies.
- **Deep fake Technology:** The rise of deepfake technology, which uses AI to create realistic fake images, videos, and audio recordings, adds another layer of complexity to fraud detection. Fraudsters can impersonate trusted individuals, such as CEOs or influencers, to deceive consumers into making fraudulent payments or revealing sensitive information. Detecting deepfakes requires advanced AI-based systems and deep learning algorithms, which are often not yet widespread or accessible.
- **Bot-driven Fraud :** Automated bots powered by AI can perform fraudulent actions at scale, including creating fake accounts, posting fraudulent reviews, and inflating web

traffic through click fraud. Bots can be designed to mimic human interactions closely, making it difficult for traditional systems (like CAPTCHA or IP tracking) to distinguish between legitimate users and malicious actors. Identifying bot networks that operate across multiple platforms adds to the challenge.

- **Data Overload:** The vast amount of data generated through digital marketing platforms makes it increasingly difficult for businesses to spot fraud in real time. Fraud detection systems can struggle to parse through huge volumes of information to identify patterns of fraudulent activity, especially when dealing with complex schemes that involve multiple steps or diverse fraudulent behaviors.
- **Cross-border Fraud:** Fraudsters often operate across borders, making it challenging for businesses to trace and prevent fraud effectively. Different regions have varying levels of enforcement and regulation, allowing fraudsters to exploit jurisdictional gaps. This global nature of fraud complicates detection and enforcement efforts.

Limitations of Current Measures: Policies, Tools, or Practices

- **Lack of Unified Regulatory Framework:** While various countries have established regulations to combat financial fraud, there is often no consistent global framework for digital marketing fraud. The absence of international coordination makes it difficult to implement standardized fraud prevention measures across platforms, leaving gaps that fraudsters can exploit. In India, for instance, the regulatory environment is still evolving, and some areas remain unaddressed by existing policies.
- **Inadequate Detection Tools:** Current fraud detection tools often rely on rule-based systems that can’t adapt quickly enough to new fraud techniques. While machine learning-based systems have shown promise, they still face limitations in accurately detecting complex fraud patterns, especially when fraudsters use AI and advanced techniques to disguise their actions.
- **Consumer Awareness and Education Gaps:** A significant limitation in tackling fraud is the lack of consumer awareness. Many users are not equipped to recognize fraudulent ads, phishing attempts, or suspicious online activities. Despite growing awareness campaigns, digital literacy remains a barrier, especially in rural areas, where individuals may not fully understand the risks posed by online fraud.

- **Limited Legal and Policy Enforcement:** Enforcement of laws surrounding digital marketing fraud is often slow and inconsistent. Many businesses may not report fraud due to reputational concerns, and when they do, the legal process is often time-consuming and inefficient. In some cases, even when fraud is detected, penalties may not be severe enough to deter future violations.
- **Difficulty in Attribution:** One of the biggest challenges in fraud detection is attributing the fraudulent activity to specific individuals or groups. Fraudsters often use fake or stolen identities, obfuscating their true locations or methods of operation. Digital marketing platforms can be misused by fraudsters to create multiple fake accounts, making it hard to identify and hold perpetrators accountable.
- **Over-reliance on Automated Solutions:** Many businesses rely on automated tools for fraud detection, but these systems can be easily bypassed by sophisticated fraud tactics. While automation can process large volumes of data quickly, it lacks the nuanced understanding that human oversight provides, potentially missing fraud patterns that require contextual analysis.
- **Privacy Concerns:** The growing concern over user privacy and data protection often limits the ability of businesses and regulatory bodies to track fraudulent activities effectively. Regulations such as GDPR and India's Personal Data Protection Bill restrict the use of personal data for fraud detection, making it harder to identify fraud in certain contexts while balancing privacy concerns.

These challenges and limitations underline the complexity of detecting and preventing digital marketing fraud, highlighting the need for more advanced tools, greater regulation, and increased consumer awareness to combat this growing threat.

Recommendations and Mitigation Strategies

For Businesses: Best Practices for Fraud Prevention in Digital Marketing

- **Implement Advanced Fraud Detection Tools:** Businesses should invest in AI and machine learning-powered fraud detection systems that can analyze vast amounts of data in real time and identify unusual patterns. These systems should be able to detect anomalies such as click fraud, fake reviews, and suspicious social media activities.

Regularly updating and improving these tools is essential to staying ahead of evolving fraud tactics.

- **Use Verified and Trusted Platforms:** Ensure that all digital marketing campaigns are conducted through verified, trustworthy platforms that offer built-in fraud prevention mechanisms. Platforms like Google Ads and Facebook offer ad verification tools that can help detect suspicious activity and improve transparency in advertising.
- **Regular Audits and Monitoring:** Conduct regular audits of digital marketing campaigns to spot any irregularities or fraudulent activity. Businesses should closely monitor ad performance, review customer feedback, and track social media engagements to identify any unusual behavior indicative of fraud. Automated tools can help streamline this process, but human oversight is also crucial for nuanced detection.
- **Educate Employees and Marketing Teams:** Conduct regular training for employees involved in digital marketing to familiarize them with the latest fraud techniques and best practices for avoiding them. Ensuring staff are equipped with the knowledge to recognize fraudulent tactics can help businesses act quickly in response to potential threats.
- **Multi-layered Authentication:** Implement multi-factor authentication (MFA) for critical systems and platforms to reduce the risk of unauthorized access and fraud. This includes securing access to advertising accounts, payment systems, and analytics dashboards, thereby adding an extra layer of protection against fraudsters.

For Consumers: Awareness Campaigns and Tips to Avoid Falling Prey

- **Educate Consumers about Fraud Risks:** Launch awareness campaigns to educate consumers on the risks of digital marketing fraud, particularly about phishing, fake ads, and online scams. These campaigns should focus on helping consumers recognize the signs of fraudulent content, such as unrealistic deals or suspicious URLs.
- **Verify the Authenticity of Websites and Ads:** Encourage consumers to always verify the authenticity of websites and ads before making purchases or providing personal information. Using secure payment methods, checking for "HTTPS" in website URLs, and researching the legitimacy of offers can help protect against fraudulent schemes.
- **Be Cautious of Fake Reviews:** Consumers should be aware that not all online reviews are genuine. Encourage users to look for patterns in reviews, such as overly positive or

overly negative comments, and to seek reviews on independent platforms to verify product legitimacy.

- **Report Suspicious Activity:** Empower consumers to report suspicious digital marketing activities, including fraudulent ads, phishing attempts, and fake e-commerce sites. Establishing clear reporting channels on social media platforms and e-commerce websites will help address scams quickly and prevent further harm.
- **Use Strong, Unique Passwords:** Advise consumers to use strong, unique passwords for their online accounts, especially when making purchases or engaging in financial transactions. Encourage the use of password managers to ensure better password security across various platforms.

For Regulators: Policy Suggestions to Curb Digital Marketing Fraud

- **Establish a Unified Global Regulatory Framework:** Advocate for the creation of a global regulatory framework that standardizes rules for detecting and preventing digital marketing fraud. This framework should set clear guidelines for businesses, social media platforms, and advertisers to ensure transparency and accountability in digital marketing practices.
- **Strengthen Consumer Protection Laws:** Strengthen and enforce consumer protection laws related to digital marketing, focusing on preventing fraudulent advertising, misleading promotions, and deceptive e-commerce practices. Ensure that penalties for violations are significant enough to deter fraudulent actors.
- **Promote Transparency in Digital Advertising:** Mandate full disclosure of ad targeting mechanisms and the identities of paid influencers to increase transparency in digital marketing campaigns. Regulations should require platforms to disclose when content is sponsored and ensure that ads are not misleading or deceptive.
- **Create a Digital Marketing Fraud Task Force:** Establish a dedicated task force within regulatory bodies to focus on tackling digital marketing fraud. This task force should collaborate with businesses, technology providers, and law enforcement to identify, track, and combat fraudulent activities in real time.
- **Encourage Collaboration with Technology Providers:** Regulators should collaborate with technology providers, such as social media platforms and search engines, to develop advanced tools that can help detect and prevent digital marketing fraud. Encouraging

innovation in fraud detection technologies, like machine learning and AI, is essential to staying ahead of fraudsters.

- **Implement Stricter Ad Verification Standards:** Regulators should enforce stricter ad verification processes to ensure that businesses comply with anti-fraud measures. This includes requiring regular audits of digital marketing campaigns, scrutinizing sources of traffic, and monitoring ad placement for potentially fraudulent activities.
- **Promote Consumer Education Initiatives:** Governments should fund and support public awareness initiatives that help educate consumers on identifying and avoiding digital marketing fraud. These initiatives could involve public service campaigns, collaboration with educational institutions, and partnerships with technology companies to create easy-to-access fraud prevention resources.

By implementing these recommendations, businesses, consumers, and regulators can work together to combat digital marketing fraud effectively. Addressing the issue at multiple levels will help safeguard the interests of both consumers and businesses, while maintaining trust in digital marketing platforms.

Conclusion

Digital marketing has become a cornerstone of modern business strategies, offering unprecedented reach, efficiency, and targeted consumer engagement. However, the rise of digital marketing has also given rise to a new wave of financial fraud, with fraudsters exploiting the very tools meant to enhance business growth. Techniques such as phishing, click fraud, fake e-commerce sites, and social media scams are increasingly sophisticated, making it difficult for businesses, consumers, and regulators to keep up.

The challenges in detecting fraud are compounded by the rapid evolution of fraudulent tactics, the complexity of data analysis, and the global nature of online crime. While AI and machine learning offer some solutions in both detecting and preventing fraud, their effectiveness is limited by the ongoing innovation in fraud methods. Additionally, regulatory frameworks remain fragmented, and the lack of consumer awareness further exacerbates the problem.

To address these challenges, businesses must adopt advanced fraud detection systems, regularly audit their digital marketing campaigns, and ensure that their teams are educated on

the latest fraud techniques. Consumers, on the other hand, must be made aware of potential scams and equipped with the knowledge to recognize fraudulent activity. Regulators must collaborate internationally, strengthen consumer protection laws, and implement clear standards for transparency in digital advertising.

Only through a multi-faceted approach involving businesses, consumers, and regulators can the digital marketing landscape be safeguarded against financial fraud, ensuring a secure and trustworthy online environment for all stakeholders.

References:

- Abbassi, H., E L Mendili, S., & Gahi, Y. (2024). Digital banking fortification: A real-time isolation forest architecture for detecting online transaction fraud. Engineering Research Express, 6(2), 025214. https://doi.org/10.1088/2631-8695/ad4958
- Ahmad, I., Iqbal, S., Jamil, S., & Kamran, M. (2021). A Systematic Literature Review of E-Banking Frauds: Current Scenario and Security Techniques. 2.
- Al-Maari, A.-A., & Abdulnabi, M. (2023). Credit Card Fraud Transaction Detection Using a Hybrid Machine Learning Model. 2023 IEEE 21st Student Conference on Research and Development (SCOReD), 119–123. https://doi.org/10.1109/SCOReD60679.2023.10563915
- Dillon, D., & Hadzic, M. (2009). A framework for detecting financial statement fraud through multiple data sources. 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies, 692–696. https://doi.org/10.1109/DEST.2009.5276674
- Eluwole, O. T., & Akande, S. (2022). Artificial Intelligence in Finance: Possibilities and Threats. 2022 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), 268–273. https://doi.org/ 10.1109/ IAICT55358. 2022.9887488
- Isa, H., Rahim, M. E. A., Ariffin, N. A. M., Embran, R. A., Han, S. H. M. R., Subramanian, U., Kawi, F., & Abdullah, N. (2022). Study on the Different Types of Accounting Fraud and Tools to Detect and Prevent Fraud. 2022 7th International Conference on Business and Industrial Research (ICBIR), 627–631. https://doi.org/10.1109/ICBIR54589.2022.9786440
- Khalifa, N., Elmedany, W., & Sharif, S. (2024). Leveraging Digital Identity and Open Banking Data for Fraud Prevention in the Financial Industry. 2024 11th International

Conference on Future Internet of Things and Cloud (FiCloud), 286–291. https://doi.org/10.1109/ FiCloud62933. 2024.00051

- Kumar, A., Sharma, M., Kathuria, S., Yamsani, N., Gehlot, A., & Kathuria, A. (2023). Banking Industry's Transformation with Aid of AI Technology. 2023 IEEE World Conference on Applied Intelligence and Computing (AIC), 441–445. https://doi.org/ 10.1109/ AIC57670. 2023.10263958
- Maulana, L. R., Fajar, A. N., & Meyliana. (2021). Extending the Design of Smart Mobile Application to Detect Fraud Theft of E-Banking Access Using Big Data Analytic and SOA. 2021 IEEE 5th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 360–364. https://doi.org/10.1109 /ICITISEE53823. 2021.9655805
- Melnychenko, S., Volosovych, S., & Baraniuk, Y. (2020). DOMINANT IDEAS OF FINANCIAL TECHNOLOGIES IN DIGITAL BANKING. Baltic Journal of Economic Studies, 6(1), 92. https://doi.org/10.30525/2256-0742/2020-6-1-92-99
- Rani, S., & Mittal, A. (2023). Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection. 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), 2345–2349. https://doi.org/10.1109/IC3I59117.2023.10397958
- Shete, N. L., Maddel, M., & Shaikh, Z. (2024). A Comparative Analysis of Cybersecurity Scams: Unveiling the Evolution from Past to Present. 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), 1–8. https://doi.org/10.1109/I2CT61223.2024.10543498
- Tewari, I., Bisht, S., Tiwari, A., Joshi, B., Arora, S., & Tewari, G. (2023). The Revolutionary Transformation of India's Banking Industry through Artificial Intelligence. 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 1–5. https://doi.org/10.1109/ICCCNT56998.2023.10307322
- Wewege, L., Lee, J., & Thomsett, M. C. (n.d.). Disruptions and Digital Banking Trends.