International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Ease vs. Security: A Comprehensive Study of Cyber Risk in Digitalized Banking

Mr. Piyush Agarwal[1], Dr. S. K. Singh[2], Ms. Arunima Konar[3]

[1]Research Scholar, Department of Commerce & Management, Binod Bihari Mahto Koyalanchal University, Dhanbad
[2]H.O.D., Department of Commerce, R.S. More College, Govindpur
[3]Guest Faculty, Department of Commerce, Guru Nanak College, Dhanbad

Abstract

In today's fast-paced world, digital technologies have completely changed the way we bank. Scheduled commercial banks have adopted e-banking platforms to make financial services more accessible and convenient than ever before. Over the past few years, the number of online transactions has grown significantly, reflecting how much people rely on these platforms. However, along with this convenience comes a growing concern—cyber risk.E-banking platforms are designed to make banking easy. Customers can transfer money, check balances, and perform countless other transactions from the comfort of their homes. But this ease of use has also opened doors for cyber threats like phishing, identity theft, and data breaches. For banks, the challenge is clear: how do they ensure security without compromising the user-friendly experience their customers expect?

Many studies have explored the risks and advantages of e-banking, highlighting both its transformative potential and its vulnerabilities. Despite this, there's still a gap in understanding how to balance ease of access with robust security measures. This is where our research steps in. By digging deeper into this topic, we hope to shed light on the trade-offs banks face and provide useful insights for policymakers, banks, and tech developers. Our ultimate goal is to help create a better understanding of the delicate balance between convenience and security in the digital banking landscape.

Overall, the convenience to manage the finances with ease and flexibility and psychological comfort provided by online banking platforms often outweigh the concerns about cyber security risks. So, after a proper analysis of all possible benefits provided by banks to their customer, it is no brain that these factors are the main reasons why customers continue to use and rely on these services even after knowing the possible cyber security breach which can lead to financial losses.

Keywords: Digital Technologies, E-banking, Financial Services, Online Transactions, Cyber Risks, Data Breaches, Phishing

1. Introduction

E-banking has come a long way since its inception, evolving through key milestones that have redefined how financial services are accessed. The introduction of internet banking revolutionized traditional banking, allowing customers to manage their accounts online without visiting a branch. Mobile banking apps further enhanced this convenience, enabling on-the-go access to financial transactions. More

recently, innovations like AI-driven platforms and instant fund transfer systems (e.g., UPI in India) have made banking faster and more personalized than ever before.

While these advancements have brought unprecedented convenience, they have also introduced new challenges. As e-banking platforms have become more sophisticated and widespread, they have increasingly attracted the attention of cybercriminals. With large volumes of sensitive financial data being processed online, the risks associated with digital transactions have grown significantly.

The trade-off between ease of use and security poses a critical dilemma for users. Adding multi-factor authentication and other security measures can enhance protection but may also make the user experience more cumbersome. Conversely, simplifying access for the sake of convenience can leave systems vulnerable to exploitation.

This paper looks at the relationship between how easy e-banking has become and the rising cyber risks associated with it. Using last10 years of data, we aim to identify trends and analyse the challenges. Instead of suggesting practical solutions, we focus on making informed assumptions about how future risks related to cyber security might increase because of evolving ease of using e-banking platforms. The integration of advanced technologies, such as AI-driven tools, into e-banking platforms has significantly enhanced the ease and accessibility of banking services. However, this convenience comes with the increased exposure of critical and sensitive personal information, including passwords, account details, and financial transactions, to online environments which will be available in few clicks. The growing reliance on open banking systems and digital channels amplifies the risks, making this data vulnerable to potential breaches and cyber threats. As digital banking continues to evolve, the associated cyber security risks are poised to escalate, posing significant challenges to ensuring the privacy and security of financial information in the future. Our study aims to offer a perspective that combines insights from the past with expectations for the future.

2. Literature Review

The research paper titled “Data Privacy and Cyber security Challenges in the Digital Transformation of the Banking Sector” delves into the complexities banks face as they integrate advanced technologies like cloud computing, big data analytics, artificial intelligence, and block chain into their operations. Through qualitative analysis of interviews with IT specialists, the study identifies primary challenges such as integrating legacy systems, evolving compliance management, managing vendor risks, maintaining customer confidence, and mitigating emerging threats.

The research paper titled “Cybersecurity Challenges in the Modern Banking Sector” by Kiran Yesugade, published in December 2024, provides an in-depth analysis of the evolving cyber security landscape within the banking industry. It highlights the increasing sophistication of cyber threats such as phishing, ransomware, and Advanced Persistent Threats (APTs), which exploit vulnerabilities in legacy systems and third-party integrations.

The research paper titled “Assessing the Influence of Cyber security Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review” by Md. Walliullah and colleagues offers a comprehensive analysis of how cyber security concerns impact digital banking. By reviewing 78 peer-reviewed articles from 2015 to 2024 using the PRISMA methodology, the study identifies phishing and malware as the most prevalent threats, leading to substantial financial losses and eroding consumer trust.

The research paper "Impact of Online Convenience on Mobile Banking Adoption Intention: A Moderated Mediation Approach" by Charles Jebarajakirthy examines how the convenience of online banking influences users' intentions to adopt mobile banking services. The study identifies key dimensions of online convenience, such as ease of use, accessibility, and time savings, which positively impact users' trust and perceived value of mobile banking platforms.

The paper "Adoption of Digital Payment Systems and its Influence on Consumer Behaviour in India" by Akshay Sunil Tribhan explores the rapid adoption of digital payment systems and their transformative impact on consumer behaviour in the Indian context. The study identifies key drivers of digital payment adoption, such as accessibility, convenience, and government initiatives like the Digital India campaign.

The research paper "Balancing Act: Cyber security Measures and Customer Behaviour in Online Banking" by Gaurav Dutta investigates the interplay between cyber security practices and customer behaviour in online banking environments. The study finds that robust cyber security measures, including encryption, multi-factor authentication, and fraud detection systems, significantly enhance customer trust and confidence in using online banking platforms.

The research paper titled “The Impact of Digital Payment Systems on Traditional Banking in India: Challenges and Opportunities” published on International Journal for Multidisciplinary Research (IJFMR) explores how digital payment systems like UPI, mobile wallets, and banking apps are reshaping the Indian banking landscape. It highlights a transformative shift in consumer behaviour, with a significant decline in branch visits and ATM usage as customers increasingly prefer digital channels for transactions.

The paper “The Impact of FinTech Adoption on Financial Inclusion and Investment Behaviour Among Indian Youth” published on International Journal for Multidisciplinary Research (IJFMR) examines how FinTech enhances financial inclusion and shapes investment habits. Basic tools like UPI and mobile wallets are widely used, but advanced services like digital lending and insurance remain underutilized. A strong positive correlation ($r = 0.68$) exists between FinTech adoption and financial inclusion, with improved digital credit and savings access.

The research paper “Artificial Intelligence in Banking and Finance” published in International Journal for Multidisciplinary Research (IJFMR) examines the integration of AI in the banking sector, highlighting both its potential benefits and significant risks. While AI applications like fraud detection, credit scoring, chatbots, and investment management offer operational improvements, the paper underscores that these benefits come with considerable challenges.

These studies provide valuable perspectives on the complexities and risks associated with integrating AI into banking systems, particularly concerning cyber security and data privacy.

3. Research Methodology

This research uses a descriptive analysis to explore how artificial intelligence (AI) is shaping the banking sector, particularly its impact on cyber security and data privacy. The goal is to bring together insights from existing studies to better understand the challenges and opportunities that come with integrating AI into banking platforms. Based on these insights, the study makes informed assumptions and projections about the future of cyber security and data privacy in this evolving landscape.

The data for this study was gathered from secondary sources, including journal articles, conference papers and industry reports published between 2016 and 2025. Trusted platforms like Research Gate,

IEEE Xplore, Springer Link, IJFMR and arXiv were key resources, along with reports from financial institutions and regulatory bodies.

To analyse this data, trend analysis was used to identify recurring themes, challenges, and opportunities related to AI in banking. Patterns in how AI technologies have been adopted and implemented were also explored to shape future projections. Using this information, the study proposes assumptions about how AI might influence cyber security risks and data privacy concerns going forward, providing a solid foundation for future research in this field.

This study focuses on reviewing existing knowledge rather than conducting primary research, which means its findings are limited by the scope of the secondary data. The assumptions made are theoretical and will need further validation through future empirical studies. Care has been taken to maintain academic integrity by properly citing all sources. Additionally, the study relies solely on publicly available data, ensuring privacy and confidentiality throughout the research process.

4. Research Questions

- Why are cyber fraud incidents increasing despite the implementation of advanced security technologies in banking platforms?
- What psychological and behavioural factors drive customer trust and continued usage of online banking platforms amid rising cyber security concerns?
- How do advancements in artificial intelligence in banking platforms inadvertently introduce new cyber security vulnerabilities?

5. Discussion and Findings

Government's Response to Rising Cyber Fraud According to Minister of State for Finance Pankaj Chaudhary, fraud cases involving card payments, internet transactions, and digital payments have surged significantly over the last decade. As per RBI data, cyber fraud losses were Rs 18.46 crore from 845 cases in 2014-15. In 2015-16, cases rose to 1,191, with losses climbing to Rs 26.90 crore. By 2017-18, fraud cases had reached 2,058, with losses surging to Rs 79.79 crore.

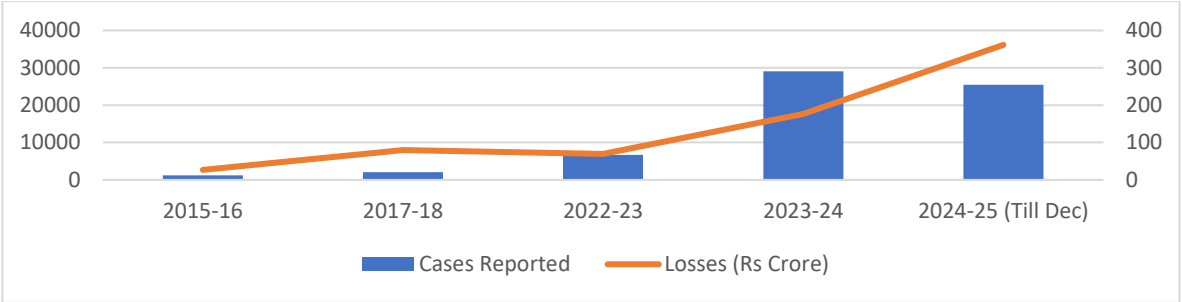
In 2022-23, cyber fraud losses stood at Rs 69.68 crore from 6,699 cases. The numbers spiked sharply in 2023-24, with 29,082 reported cases, causing losses to soar to Rs 177.05 crore .With data available until December 2024, the total estimates for FY 2024-25 may be considerably higher. Already, Rs 107.21 crore has been lost from April 2024 to December 2024.

As reported by the Reserve Bank of India (RBI), from FY 2014-15 to FY 2024-25 (till December), a total of 65,315 cyber fraud cases (amount involved Rs 1 lakh each and above) have been recorded, resulting in a cumulative financial loss of Rs 733.22 crore.

Table 1: Volume & Value of Cyber Frauds over the years

Financial Year	Cases Reported	Losses (Rs in Crore)
2015-16	1191	26.9
2017-18	2058	79.79
2022-23	6699	69.68
2023-24	29082	177.05
2024-25 (Till Dec'24)	25440	361.34

The above data is pictured in the next graph.



Source:https://www.outlookmoney.com/news/cyber-fraud-cases-surge-over-the-last-decade-reports-finance-ministry.

The increase in cyber fraud incidents, despite advanced security technologies in banking, can be attributed to several key factors. The rise in online banking has significantly increased the exposure of sensitive financial data, such as account details and passwords, making it an attractive target for cybercriminals. This exposure is compounded by evolving cyber threats like phishing, ransomware, and advanced persistent threats, which often outpace current security measures.

The rapid expansion of online banking platforms and the integration of technologies like AI and open banking APIs have widened the attack surface. Additionally, many users are unaware of secure online practices, which make them vulnerable to social engineering attacks and other cyber exploits.

Another critical factor is the reliance on legacy systems that cannot fully support modern security solutions, creating exploitable vulnerabilities. The sheer volume of digital transactions also increases the likelihood of fraud, even as security measures improve. Finally, global interconnectivity and uneven enforcement of data protection laws contribute to the challenges, highlighting the need for a comprehensive approach to cyber security in banking.

The Unified Payments Interface (UPI) has witnessed exponential growth since its inception, marked by a steady increase in both the number of participating banks and transaction volumes. A positive correlation can be observed between the expansion of institutional infrastructure namely, the number of banks going live on the platform and the surge in transactional activity. This correlation aligns with the growing rate of customer on boarding on UPI-enabled applications, suggesting that greater institutional availability facilitates user adoption. As more banks integrate UPI services, customers gain easier access to digital payment systems, thereby reinforcing usage and contributing to the platform's network effect. These trends underscore the significance of both supply-side (bank participation) and demand-side (consumer engagement) dynamics in the diffusion of digital financial technologies in emerging markets.

Table 2: Value & Volume of UPI transactions over the years

Year	No. of Bank live on UPI	Volume (in million)	Value (in crore)
April 2016- Dec 2016	221	2.74	892.09
Jan 2017-Dec 2017	626	429.15	56,820.87
Jan 2018-Dec 2018	1081	3,746.32	5,85,710.45
Jan 2019-Dec 2019	1646	10,787.54	18,36,638.18
Jan 2020-Dec 2020	2003	18,880.89	33,87,744.72
Jan 2021-Dec 2021	2869	38,744.55	71,59,285.8

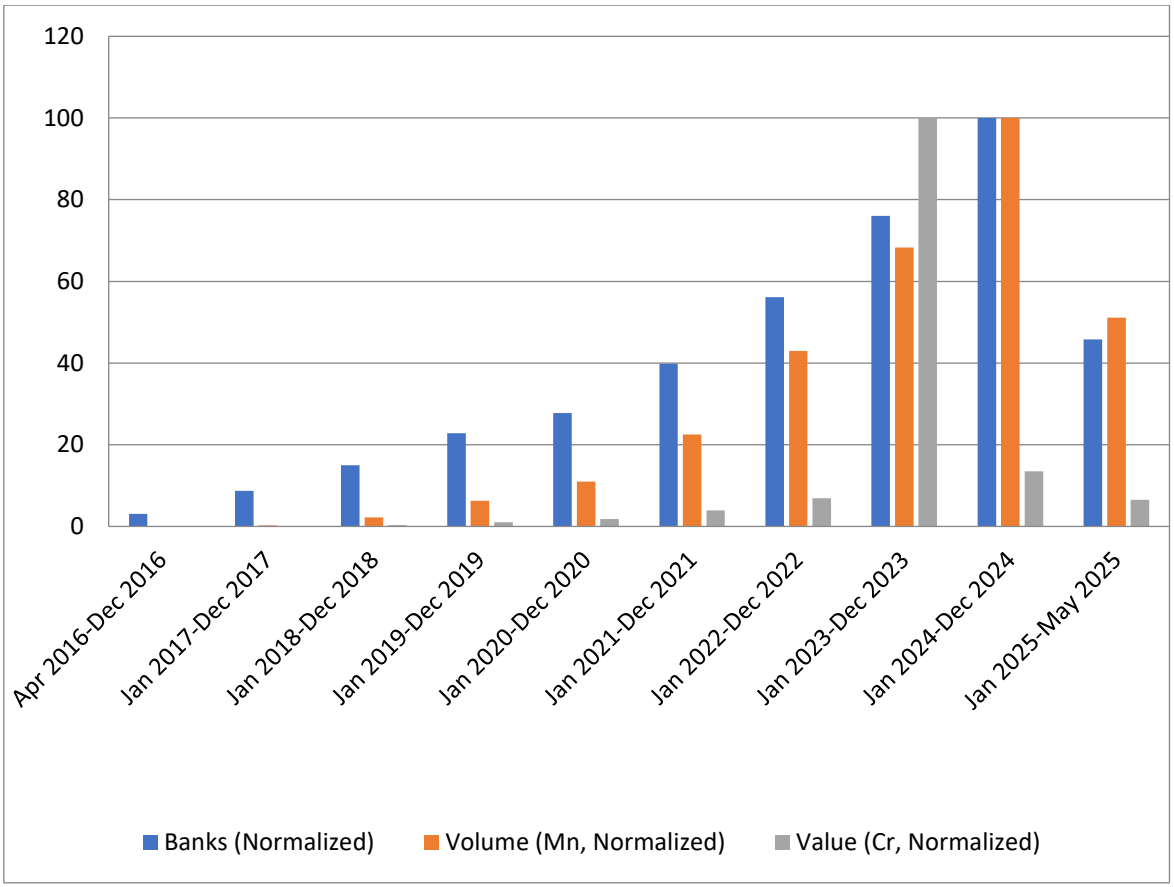
Jan 2022-Dec 2022	4049	74,044.48	125,95,077.87
Jan 2023-Dec 2023	5483	1,17,641.09	1829,92,795.2
Jan 2024-Dec 2024	7210	1,72,208.01	246,82,520.78
Jan 2025-May 2025	3302	87,974.58	119,30,963.3

Source: https://www.npci.org.in/what-we-do/upi/product-statistics

Table 3: Value & Volume of UPI transactions over the years (Normalized)

Year	**No. of Bank live on UPI (Normalized)**	**Volume (Mn, Normalized)**	**Value (Cr, Normalized)**
Apr 2016-Dec 2016	3.07	0	0
Jan 2017-Dec 2017	8.68	0.25	0.03
Jan 2018-Dec 2018	14.99	2.18	0.32
Jan 2019-Dec 2019	22.83	6.26	1
Jan 2020-Dec 2020	27.78	10.96	1.85
Jan 2021-Dec 2021	39.79	22.5	3.91
Jan 2022-Dec 2022	56.16	43	6.88
Jan 2023-Dec 2023	76.05	68.31	100
Jan 2024-Dec 2024	100	100	13.49
Jan 2025-May 2025	45.8	51.09	6.52

The above data is pictured in the next graph.



Overall, the convenience to manage the finances with ease and flexibility and psychological comfort provided by online banking platforms often outweigh the concerns about cyber security risks. So, after a proper analysis of all possible benefits provided by banks to their customer, it is no brain that these factors are the main reasons why customers continue to use and rely on these services even after knowing the possible cyber security breach which can lead to financial losses.

Here's an in-depth explanation of how advancements in artificial intelligence (AI) in banking platforms inadvertently introduce new cyber security vulnerabilities:

- Expanded Attack Surface: AI systems integrate across multiple banking functions—customer support, fraud detection, credit scoring, and financial advisory services. Each integration point becomes a potential vulnerability, increasing the likelihood of exploitation by attackers.
- Dependency on Large Data Sets: AI systems rely on extensive customer data for training and functioning, often stored in centralized or cloud-based systems. This data is a lucrative target for cybercriminals, as breaches can expose sensitive financial and personal information, leading to large-scale fraud.
- Adversarial Attacks and Data Poisoning: Adversarial attacks manipulate AI algorithms by injecting malicious data during training or deployment. For example:
- Data Poisoning: Alters training datasets to produce flawed outcomes, weakening fraud detection mechanisms.
- Evasion Tactics: Exploits algorithmic weaknesses to bypass security checks.
- Automation Blind Spots: Over-reliance on AI automation can create blind spots where human oversight is minimal. Attackers exploit these automated systems by triggering specific, predictable re

sponses, bypassing security protocols without immediate detection.

- Vulnerability in Open Banking Ecosystems: AI-powered banking platforms often involve third-party collaborations, such as FinTech integrations. These external tools may not adhere to the same security standards, creating vulnerabilities in an otherwise secure system.
- Sophistication of AI-Driven Threats: Cybercriminals are leveraging AI to enhance their own attack methods, such as:
- AI-Driven Phishing: Personalizes phishing attacks using AI to mimic trusted entities.
- Deep fake Fraud: Uses AI to create convincing fake identities, enabling fraudulent transactions.
- These threats evolve faster than the systems designed to counteract them (Md Waliullah, 2025).
- Insufficient Security Testing: Banks may implement AI systems rapidly to remain competitive, often prioritizing functionality over rigorous security testing. This rush to deploy can leave systems vulnerable to exploitation.
- Real-Time Data Vulnerabilities: AI systems require continuous, real-time data exchange to operate effectively. This constant flow of sensitive data creates opportunities for attackers to intercept, manipulate, or exploit these data streams (Gaurav Dutta, 2024)
- Insider Threats: AI systems often require privileged access for operation and maintenance. Insider threats—whether malicious or accidental—can exploit this access to compromise system security.
- Ethical and Compliance Gaps: The rapid adoption of AI in banking often outpaces regulatory frameworks, particularly in areas like algorithmic transparency and ethical data usage. This creates gaps that attackers can exploit, especially in regions with weaker cyber security laws.
- AI Model Updates and Exploitation: Frequent updates to AI algorithms to improve efficiency can inadvertently introduce new bugs or vulnerabilities, providing opportunities for exploitation.
- Black-Box Vulnerabilities: AI systems often function as “black boxes,” making it difficult to understand or predict their decision-making processes. This lack of transparency can mask vulnerabilities until they are exploited (Chinedu Callistus Onyeje et al., 2024).

6. Conclusion

The advancements in artificial intelligence (AI) and digital technologies in banking have undeniably revolutionized the way financial services are accessed and utilized. From UPI to net banking and mobile banking, the convenience offered by these platforms has reshaped the customer experience, allowing users to perform transactions with just a few clicks on their smart phone. Banks have integrated cutting-edge technologies such as AI and Blockchain to optimize services, enhance security, and reduce fraud. However, these advancements are not without significant risks.

AI, while improving operational efficiency, also gains access to sensitive customer data, such as account details, passwords, and transaction histories, which are stored on centralized servers. This creates a double-edged sword—while banks leverage AI to detect and prevent fraud, the very same technology could be exploited by malicious actors to perpetrate more sophisticated financial crimes. Currently, financial frauds are primarily human-driven, involving techniques like phishing, skimming, and OTP scams, often originating from hubs like Jamtara in Jharkhand. However, by 2050, there is a realistic possibility that AI itself would commit financial frauds on a much larger and more efficient scale.

As of now, AI enables fraudsters to carry out advanced data breaches, deploy deepfake identities, or manipulate banking systems with unparalleled precision. Automated AI tools could mimic legitimate banking communications, tricking users into sharing sensitive information. Additionally, the risks of

adversarial attacks on AI models could lead to systemic vulnerabilities, further exposing banks and their customers to financial threats. The misuse of AI to exploit customer data and bypass traditional security measures could render current protective technologies like multi-factor authentication ineffective.

If such trends continue unchecked, the financial ecosystem may find itself in a paradox where the very technologies designed to enhance security become the root cause of its vulnerabilities. This could potentially force the world to reconsider its reliance on digital banking and shift back toward traditional, manual banking methods. Such a regression would prioritize human oversight and offline interactions to ensure the security of financial transactions, although at the cost of convenience and efficiency.

While this future remains speculative, it underscores the need for robust AI governance, ethical AI development, and proactive security frameworks. Without these measures, the integration of AI in banking could pave the way for a new era of cyber fraud, reshaping the financial landscape in ways that may compel society to return to its traditional roots.

7. References

1. Wang, Shuang, et al. “Data Privacy and Cyber security Challenges in the Digital Transformation of the Banking Sector.” Journal of Digital Finance, 2024.
2. Yesugade, Kiran. “Cybersecurity Challenges in the Modern Banking Sector.” Cyber security Review, Dec. 2024.
3. Walliullah, Md., et al. “Assessing the Influence of Cyber security Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review.” Journal of Financial Technology, 2025.
4. Jebarajakirthy, Charles, et al. “Impact of Online Convenience on Mobile Banking Adoption Intention: A Moderated Mediation Approach.” International Journal of Banking Studies, 2021.
5. Tribhan, Akshay Sunil. “Adoption of Digital Payment Systems and Its Influence on Consumer Behaviour in India.” Journal of Consumer Research in Digital Transactions, 2024.
6. Dutta, Gaurav. “Balancing Act: Cybersecurity Measures and Customer Behaviour in Online Banking.” Journal of Cybersecurity and Finance, 2024.
7. Srivastava, Mauli. “The Impact of Digital Payment Systems on Traditional Banking in India: Challenges and Opportunities.” International Journal for Multidisciplinary Research (IJFMR), 2025.
8. Tomer, Archikey Singh. “The Impact of FinTech Adoption on Financial Inclusion and Investment Behaviour among Indian Youth.” International Journal for Multidisciplinary Research (IJFMR), 2025.
9. Narang, Ashima, et al. “Artificial Intelligence in Banking and Finance.” International Journal for Multidisciplinary Research (IJFMR), 2024.
10. Kovacevic, Ana, et al. “Artificial Intelligence and Cyber security in Banking Sector: Opportunities and Risks.” arXiv, 2024.
11. Onyeje, Chinedu Callistus, et al. “Data Privacy and Cyber security Challenges in AI-Enhanced Financial Services: A Comprehensive Analysis.” Research Gate, 2024.