Cybersecurity Challenges in the Age of Digital Finance

Dr.C.Mallesha[1], Ayesha Thabassum [2]
[1]*Associate.Professor, School of Management, Anurag University.*
[2]*Student, School of Management, Anurag University.*

Abstract: **Digitalization of financial systems in the post-COVID era has rapidly transformed how companies and individuals manage service access, investments, and transactions. But this shift has also significantly increased cybersecurity issues, therefore compromising individuals to crimes including identity theft, data breaches, phishing, and financial fraud. This paper examines the evolving cybersecurity challenges in digital finance by emphasizing post-pandemic threats, vulnerabilities caused by new technologies, the impact of cyberattacks on individuals, and the effectiveness of current regulatory systems. A systematic survey of 269 Hyderabad residents yielded primary data indicating a moderate level of awareness of cyber threats and poor reporting behavior among victims. Among the findings are lack of knowledge of reporting channels, psychological stress following attacks, and the continuous human error as a main vulnerability. Depending on the study, the report recommends targeted awareness campaigns, improved legal and institutional support systems, adoption of contemporary security architectures, and greater public-private collaboration. The results underline the urgent need of a whole and proactive approach to safeguard digital finance ecosystems and strengthen user resilience against more sophisticated cyber-attacks.**

Keywords: **Cybersecurity, Digital Finance, Post-COVID, Cyber Threats, Financial Fraud**

1. INTRODUCTION

Digital financial services like contactless payments, mobile banking, and digital wallets were adopted more quickly because of the COVID-19 epidemic. Although this change increased convenience and financial inclusion, it also made people and organizations more vulnerable to more cyber threats. Through phishing, ransomware, and fraud, cybercriminals took advantage of remote work arrangements, poor personal device security, and rising online financial activity.Though they have created new vulnerabilities such smart contract errors, algorithmic manipulation, and data breaches, emerging technologies such artificial intelligence, blockchain, cloud computing, and IoT have spurred innovation. Cyberattacks now target people directly, causing identity theft, financial trouble, and emotional suffering.

Examining the major cybersecurity threats that have arisen or grown in the post-COVID era, this paper investigates the vulnerabilities connected to digital finance technologies, evaluates the human and institutional effects of cyberattacks, and assesses the efficacy of current cybersecurity policies and controls.

2. NEED OF THE STUDY

While security policies have fallen behind, the COVID-19 epidemic hastened the move to digital finance, which has increased phishing, fraud, and identity theft. While they provide creativity, emerging technologies like blockchain and artificial intelligence also pose fresh vulnerabilities. Often undervalued, the human and financial consequences of cyberattacks are also underappreciated; current laws fall short.This paper investigates changing cybersecurity threats, technological hazards, user effects, and the efficacy of present safeguards to support the creation of a more robust digital finance system.

3. SCOPE OF THE STUDY

Focusing on mobile banking, digital wallets, fintech, and cryptocurrency, this paper investigates the growth and complexity of cybersecurity threats in digital finance post-COVID. It looks at vulnerabilities created by new technologies such as blockchain, artificial intelligence, and IoT and evaluates the effects of cyberattacks on both people and organizations—especially with respect to financial loss, privacy violations, and psychological consequences. With a worldwide viewpoint stressing issues in developing nations, it also assesses the efficacy of present laws and industry practices, giving strategic and human-centered elements top priority over technical specifics.

4. OBJECTIVES OF THE STUDY

1. Identify and analyze the major cybersecurity threats during the post-COVID period.
2. Evaluate the impact of cyberattacks on individuals.

5. RESEARCH METHODOLOGY

Research is the process of systematic and in- depth study or search for any particular topic, subject or area of investigation, backed by collection, compilation, presentation and interpretation of relevant details of data.

Population and Sample Size of the study: The sample would be obtained from about 269 individuals present in and around of Ghatkesar Mandal, Hyderabad.

Sampling Technique The researcher has used random sampling method for this study. A random sampling is a probability sampling method where a sample is taken from a group of people through survey method.

Sources of data collection Data collection is one of the most important aspects of research. The study used both primary and secondary data.

1. Primary Data

The researcher used well-structured questionnaires, which contained open ended and closed ended questions. The researcher personally went to collect data from the respondents.

2. Secondary Data

Secondary data means that are already available i.e., they refers to the data which has already been collected and analyzed by someone else. The secondary data for the study was collected from books, company websites, magazines and other sources.

Statistical Tool Used for Analysis The data collection are classified, analyzed and calculated by simple percentage method.

7. LIMITATIONS OF THE STUDY

1. Geographical Limitation: Concentrated just on Ghatkesar Mandal, Hyderabad users, therefore restricting more general relevance.
2. Based on 269 replies, which might not completely reflect the larger population.
3. Responses might be affected by memory bias or hesitancy to reveal personal information.
4. Emphasizes personal experiences, therefore ignoring organizational or institutional effects.
5. Threats Rapidly Changing: Trends in cybersecurity could change quickly, therefore influencing the long-term relevance of the research.
6. Emphasizes user awareness above thorough technical study of systems or vulnerabilities.

REVIEW OF LITERATURE

Recent studies highlight the vital importance of enhanced digital finance cybersecurity. Emphasizing innovation, consumer education, and regulatory compliance as fundamental, Adejumo and Ogburie (2025) underline artificial intelligence, blockchain, and multi-factor authentication for fighting cyber threats. Though issues including data integrity and openness persist, Yussuf et al. (2020) and Williams et al. (2021) demonstrate how machine learning improves threat detection. Okoye et al. (2024) advocate multi-stakeholder collaboration and adaptive rules. Green (2022) emphasizes the need of worldwide cooperation against changing cyber threats.

Examining weaknesses in financial mobile apps, Mustapha et al. (2023) support tighter encryption and compliance policies. Pavlidis (2021) addresses the EU's proactive control of crypto-assets following COVID. Revealing cybersecurity holes resulting from digital transformation in companies, Saeed et al. (2023) advocate gradual cybersecurity preparedness. Finally, Buckley et al. (2019) caution on systematic dangers from tech-driven finance and advocate proactive regulation using RegTech.

Objective-1: Identify and analyze the major cybersecurity threats during the post-COVID period

1. Ransomware Attacks: Ransomware grew post-COVID as companies hastily digitalized lacking strong security. Targeting at-risk industries like healthcare and education, attackers encrypted files and sought bitcoin payments. The 2021 Colonial Pipeline assault made clear the urgent danger to national infrastructure.

2. Using phishing emails and false vaccine or benefit updates, cybercriminals took advantage of pandemic-related anxieties. Spear phishing and deepfakes among other advanced techniques grew, making it more difficult to tell genuine from phony communications.

3. Remote work revealed companies new risks from personal device use, unprotected networks, and

outmoded software. Data leaks and malware infections followed from missing VPNs, MFA, and staff education.

4. Though many companies misconfigured settings and lacked cloud security knowledge, cloud adoption surged. Breaches were caused by weak encryption, inadequate access controls, and insider mistakes, particularly with misunderstood shared responsibilities.

5. Attackers went after third-party suppliers to penetrate bigger networks. The SolarWinds hack demonstrated how one damaged supplier could impact thousands. Tech integration motivated by the epidemic increased attack surfaces.

6. The growth of IoT devices created security holes including unpatched firmware and default credentials. These were used to start more attacks or gain illegal access, therefore increasing danger in homes and businesses.

7. Economic pressure and remote work increased insider threats from both malicious and careless workers. Less monitoring made it more difficult to spot aberrant behaviour, therefore raising the likelihood of internal data leaks or sabotage.

8. State-sponsored individuals propagated false stories and focused vaccine research throughout the epidemic. While cyber espionage sought to steal sensitive health and strategic data, disinformation campaigns sought to create distrust.

Examining:

1. The epidemic set off fast digital transformation, so increasing cyber hazards. Especially with the increase in remote work, cloud adoption, and digital tools, threats grew more frequent and complex.

2. Reliable data from sources including incident reports, threat feeds, breach logs, and case studies helps to drive efficient threat analysis. Patterns indicate rising attacks across sectors, particularly by means of phishing and ransomware.

3. Classifying and Profiling Types of threats are analyzed: Ransomware, phishing, supply chain, insider threats, Assault Vector: Cloud misconfigurations, VPN, email, Targets: Government, finance, healthcare, other sectors Actors: Insiders, nation-states, criminals Helps to give response initiatives first importance.

4. Impact Evaluation falls under the following categories.

Operational: Recovery expenses, service interruption, downtime, Financial: Legal expenses, fines, ransom, Reputational: Loss of confidence, brand harm, drop in market value, Legal/Compliance: Lawsuits, breach alerts

5. Vulnerability Analysis: Weak authentication (e.g., lack of MFA), Unpatched software

Cloud settings that are misconfigured. Human mistakes—phishing, social engineering.

6. Risk Assessment and Prioritization: Probability of threats, Impact severity, Resource allocation priority ranking to allocate resources efficiently

Revise access controls and security policies; apply modern security technologies and monitoring. Regularly train staff members, keep incident response plans in place and test them.

Objective-2: Evaluate the impact of cyberattacks on individuals.

Personal & Demographic Information

1. Age

Age Group	Responses	Percentage
Below 18	33	12.3%
18–25	234	87.0%
26–35	0	0.0%
36–45	1	0.4%
46–60	0	0.0%
60+	1	0.4%
Total	269	100%

Interpretation: Most of the answers (87%) are in the 18–25 age range, suggesting a mostly young population. Very few participants are under 18 (12.3%) or above 25 (less than 1% each for other age categories). This implies that the data mostly reflects young people or early adults.

2. Gender

Gender	Responses	Percentage
Male	156	58.0%
Female	112	41.6%
Prefer not to say	1	0.4%
Total	269	100%

Interpretation: Of the total, 58% are men; 41.6% are women. Just one participant (0.4%) opted not to reveal their gender. This suggests a rather balanced gender distribution, with a small male majority

3. Education Level

Education Level	Responses	Percentage
High School	5	1.9%
Undergraduate	257	95.5%

Postgraduate	6	2.2%
Doctorate	1	0.4%
Total	269	100%

Interpretation: The survey mostly interacted with bachelor's level students since 95.5% of respondents are undergraduates. Participants from postgraduate (2.2%), high school (1.9%), or doctoral (0.4%) levels are very few in terms of number. This implies the information strongly represents the viewpoint of undergraduate students.

4. Occupation:

Occupation	Responses	Percentage
Student	264	98.1%
Employed	3	1.1%
Self-Employed	1	0.4%
Unemployed	0	0.0%
Retired	1	0.4%
Total	269	100%

Interpretation: An overwhelming majority of respondents (98.1%) are students, indicating that the survey primarily reached an academic or educational audience. Very few participants are employed, self-employed, or retired, with no respondents identifying as unemployed. This highlights a strong student-centric sample population.

5. Average Hours spent in online per day

Time Spent Online	Responses	Percentage
Less than 1 hour	14	5.2%
1–3 hours	128	47.6%
4–6 hours	86	32.0%
More than 6 hours	40	14.9%
Total	269	100%

Interpretation: Most of the answers (47.6%) indicate they spend 1–3 hours online each day; 32% spend 4–6 hours. Though just 5.2% are online for under an hour, 14.9% spend more than six hours. This implies that most people use the internet moderately to highly daily.

Experience with Cyber attacks

6. Are you aware of different types of cyber attacks

Response	Number of Responses aware of different types of cyber attacks	Percentage
Yes	141	52.4%
No	78	29.0%
Not Sure	50	18.6%
Total	269	100%

Interpretation: More than half of the replies (52.4%) know about various kinds of cyber-attacks, suggesting a fair degree of cyber awareness. Of those, though, a notable 29% are ignorant and 18.6% are uncertain. This emphasizes the need of better initiatives for awareness and education on cyber security.

7.Persons experienced any cyber attack

Response	Persons experienced any cyber attack	Percentage
Yes	57	21.2%
No	182	67.7%
Not Sure	30	11.2%
Total	269	100%

Interpretation: While most (67.7%) have not, only 21.2% of those polled have suffered a cyber-attack. Furthermore, 11.2% are uncertain whether they have been targeted. This implies that although direct interactions with cyber-attacks are fairly low, there is uncertainty that may be caused by ignorance or unnoticed events

8. Type of Cyber-attack experienced.

Type of Cyberattack	Number of Responses	Percentage
Phishing (fraudulent emails/messages)	70	26.0%
Identity Theft	24	8.9%
Ransom ware Attack	5	1.9%
Hacked Social Media Account	60	22.3%
Financial Fraud or Scam	46	17.1%
Other (please specify)	112	41.6%

Interpretation: The most often reported cyber-attacks are phishing (26%) and hacked social media accounts (22.3%), followed by financial fraud (17.1%) and identity theft (8.9%). At 1.9%, ransom ware attacks are rather uncommon. Interestingly, 41.6% chose "Other," suggesting a great range of cyber events not included in the primary categories

9. Did you ever Report to any authority or service provider about cyber attack

Report to any authority or service provider about cyber attack	Number of Responses	Percentage
Yes	53	19.7%
No	173	64.3%
I didn't know where to report	43	16%
Total	269	100%

Interpretation: While a great majority (64.3%) did not act, only 19.7% of those polled reported cyber-attacks to an authority or service provider. Especially 16% were unsure of where to report, which shows a lack of public knowledge on cybercrime reporting systems. This underlines the need of improved direction and easily available reporting routes.

Impact Assessment

10. Lost money due to cyber attack

Lost money due to cyber attack	Number of Responses	Percentage
Strongly Agree (SA)	30	11.2%
Agree (A)	24	8.9%
Neutral (N)	66	24.5%
Disagree (D)	103	38.3%
Strongly Disagree (SD)	46	17.1%
Total	269	100%

Interpretation: Most of the people (55.4%) either disagree or strongly disagree that a cyber-attack cost them money, implying little financial effect for most. Of those polled, 20.1% said yes or strongly so, suggesting that a significant minority did suffer financial loss. The 24.5% neutral replies could indicate ignorance or uncertainty regarding possible losses.

11. Recovering financial losses was difficult

Recovering financial losses was difficult	Number of Responses	Percentage
Strongly Agree (SA)	51	19%
Agree (A)	52	19.3%
Neutral (N)	79	29.4%
Disagree (D)	57	21.2%
Strongly Disagree (SD)	30	11.2%
Total	269	100%

Interpretation: Many of those polled (38.3%) either agree or strongly agree that recovering financial losses from cyber-attacks was challenging, implying difficulties in mitigation or recovery. Of course, 32.4% disagree or strongly disagree, suggesting that for certain people, recovery was not as difficult. The rest 29.4% are neutral, perhaps indicating uncertainty or different experiences with recovery procedures.

12. Felt anxious or disturbed after cyber attack

Felt anxious or disturbed after cyber attack	Number of Responses	Percentage
Strongly Agree (SA)	34	12.6%
Agree (A)	61	22.7%
Neutral (N)	85	31.6%
Disagree (D)	59	21.9%
Strongly Disagree (SD)	30	11.2%
Total	269	100%

Interpretation: A total of 35.3% of respondents either strongly agree or agree that a cyber-attack made them anxious or disturbed, suggesting a significant emotional impact for certain people. Of the rest, 33.1% either disagree or strongly disagree, implying that others were less emotionally impacted. The rest 31.6% are neutral, maybe indicating different emotional reactions or doubt regarding the effect.

13. Felt anxious or disturbed after cyber attack

Reputation or privacy was affected	Number of Responses	Percentage
Strongly Agree (SA)	28	10.4%
Agree (A)	49	18.2%
Neutral (N)	95	35.3%
Disagree (D)	66	24.5%
Strongly Disagree (SD)	31	11.5%
Total	269	100%

Interpretation: Of the total, 28.6% either strongly agree or agree that a cyberattack harmed their reputation or privacy, suggesting a notable effect on personal or professional privacy for certain people. Of those, 35.3% are still neutral, which may indicate uncertainty or ignorance of the effect. The remaining 36% disagree or strongly disagree, suggesting that for many, their reputation or privacy remained intact.

14. Changed by online habits after cyber attack

Changed by online habits after cyber attack	Number of Responses	Percentage

Strongly Agree (SA)	43	16.0%
Agree (A)	73	27.1%
Neutral (N)	89	33.1%
Disagree (D)	39	14.5%
Strongly Disagree (SD)	25	9.3%
Total	269	100%

Interpretation: Indicating that the event caused a change in their behaviour, 43.1% of respondents either strongly agree or agree that they altered their online practices following a cyber-attack. Of those, 33.1% are neutral, which could indicate uncertainty or mixed reactions to the incident. Of the rest, 23.8% either disagree or strongly disagree, indicating the attack had little effect on their online behaviour.

15. Now using stronger passwords and two factor authentication

Now using stronger passwords and two factor authentication	Number of Responses	Percentage
Strongly Agree (SA)	111	41.3%
Agree (A)	86	32.0%
Neutral (N)	48	17.8%
Disagree (D)	16	5.9%
Strongly Disagree (SD)	6	2.2%
Total	269	100%

Interpretation: Indicating a growing awareness and use of security measures, most respondents (73.3%) either strongly agree or agree that they now use two-factor authentication and stronger passwords. Just 8.1% disagree or strongly disagree, implying that a tiny fraction has not changed these. The other 17.8% are neutral, which could suggest different degrees of dedication to strengthening online security.

16. Avoid sharing personal or financial info online

Avoid sharing personal or financial info online	Number of Responses	Percentage
Strongly Agree (SA)	108	40.1%
Agree (A)	80	29.7%
Neutral (N)	54	20.1%
Disagree (D)	21	7.8%
Strongly Disagree (SD)	6	2.2%
Total	269	100%

Interpretation: Reflecting increased concern about online security, a notable majority of respondents (69.8%) either strongly agree or agree that they refrain from disclosing personal or financial information online. Of the rest, only 10% disagree or strongly disagree, indicating that a small number still shares such data. The remaining 20.1% are neutral, possibly indicating mixed feelings or uncertainty about when and how to share online.

17. Cyber security protections ad legal support for individuals are sufficient

Cyber security protections and legal support for individuals are sufficient	Number of Responses	Percentage
Strongly Agree (SA)	59	21.9%
Agree (A)	76	28.3%
Neutral (N)	83	30.9%
Disagree (D)	39	14.5%
Strongly Disagree (SD)	12	4.5%
Total	269	100%

Interpretation: Respondents' total of 50.2% either strongly agree or agree that legal support for people and cyber security measures are adequate, suggesting a fair degree of confidence in existing systems. Of those, 30.9% stayed neutral, perhaps indicating doubt or conflicting views on how well these safeguards work. A total of 19% either disagree or strongly disagree, indicating issues or unhappiness with the present condition of legal support and cyber security.

18. Trust digital systems after experiencing or hearing about cyber attacks

Trust digital systems after experiencing or hearing about cyber attacks	Number of Responses	Percentage
Strongly Agree (SA)	62	23%
Agree (A)	79	29.4%
Neutral (N)	91	33.8%
Disagree (D)	21	7.8%
Strongly Disagree (SD)	16	6%
Total	269	100%

Interpretation: After experiencing or hearing about cyberattacks, 52.4% of respondents either strongly agree or agree that they trust digital systems, suggesting a fairly high degree of confidence in digital systems. Of those, 33.8% are neutral, which indicates ambiguity or mixed opinions. A total of 13.8% disagree or strongly disagree, suggesting that some of the people still feel wary or skeptical of digital systems after such events.

FINDINGS

1. A large portion of the survey respondents are young undergraduate students who are moderately active online (1–6 hours daily).
2. While 52.4% are aware of cyberattacks, a significant 47.6% either lack awareness or are unsure, suggesting knowledge gaps.
3. Only 21.2% of respondents experienced a cyberattack, but uncertainty remains due to lack of awareness.
4. Phishing, hacked social media accounts, and financial fraud are the most common attack types.
5. A striking 64.3% of victims did not report incidents, and 16% didn't know where to report, indicating weak reporting mechanisms.
6. Most respondents (55.4%) did not lose money, but a notable 20.1% did, and 38.3% found financial recovery difficult.
7. Cyber-attacks had a moderate psychological impact, with 35.3% reporting anxiety or disturbance.
8. Only 28.6% reported privacy or reputational damage, but a third were neutral—suggesting unawareness of consequences.
9. 43.1% changed online habits after attacks, with 73.3% adopting stronger passwords and 2FA.
10. 69.8% are more cautious about sharing personal or financial data online.
11. Half of respondents believe cybersecurity protections and legal support are adequate; 30.9% are unsure.
12. Trust in digital systems remains relatively strong, with 52.4% expressing confidence post-attack.
13. Ransom ware and phishing attacks surged post-COVID, exploiting fear and remote infrastructure weaknesses.
14. Remote work and cloud migration introduced vulnerabilities due to poor configurations and security gaps.

CONCLUSION

This study highlights the growing cybersecurity challenges in digital finance, especially post-COVID. Despite increasing use of digital financial services, gaps in awareness, preparedness, and response remain. Many users experience phishing and fraud but often fail to report incidents due to confusion. Financial and psychological impacts are moderate but real. While stronger digital hygiene practices are emerging, new vulnerabilities from remote work, cloud services, AI, and fintech innovations complicate the landscape. Key drivers of breaches include human error and regulatory gaps. The study recommends focused awareness programs, simplified reporting, stronger incident response, and collaborative efforts across sectors to enhance resilience and trust in the digital financial ecosystem.

REFERENCES

[1] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. World Journal of Advanced Research and Reviews, 25.

[2] Adejumo, A., & Ogburie, C. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. World Journal of Advanced Research and Reviews, 25.

[3] Yussuf, M. F., Oladokun, P., & Williams, M. (2020). Enhancing cybersecurity risk assessment in digital finance through advanced machine learning algorithms. Int J Comput Appl Technol Res, 9(6), 217-235.

[4] WILLIAMS, M., YUSSUF, M. F., & OLUKOYA, A. O. (2021). Machine learning for proactive cybersecurity risk analysis and fraud prevention in digital finance ecosystems. ecosystems, 20, 21.

[5] Okoye, C. C., Nwankwo, E. E., Usman, F. O., Mhlongo, N. Z., Odeyemi, O., & Ike, C. U. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. International Journal of Science and Research Archive, 11(1), 1968-1983.

[6] Green, J. (2022). Cybersecurity Challenges in the Digital Age. International Multidisciplinary Journal Of Science, Technology & Business, 1(4), 19-23.

[7] Mustapha, I., Vaicondam, Y., Jahanzeb, A., Usmanovich, B. A., & Yusof, S. H. B. (2023). Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem. International

Journal of Interactive Mobile Technologies, 17(22).

[8] Pavlidis, G. (2021). Europe in the digital age: regulating digital finance without suffocating innovation. Law, Innovation and Technology, 13(2), 464-477.

[9] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.

[10] Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019). The dark side of digital financial transformation: the new risks of fintech and the rise of techrisk. UNSW Law Research Paper, (19-89).