ISSN (ELECTRONIC): 2945-3135

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH & REVIEWS

journal homepage: www.ijmrr.online/index.php/home

CYBER CRIME & FINANCIAL FRAUDS IN DIGITAL BANKING

Chaitra V P[1*] & Nikhil Kumar M[2]

[1]Assistant Professor Department of Commerce Aps College 0f Commerce.

[2]Assistant Professor Department of Commerce Aps College of Commerce.

Corresponding Author: Chaitra006.Raju@Gmail.Com

How to Cite the Article: Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-102.*

https://doi.org/10.56815/ijmrr.v5si2.2026.90-102

Keywords

Abstract

Payment options evolved as an impact of the modernization of banking transactions. The acceptance of electronic payment methods has been increasing substantially and rapidly. The probability that humans will be targeted by cyberattack such as fraud on the internet, theft of identity and harmful software or malware infections continues to rise as increasing numbers of individuals to select to make payments online. Electronic transactions have culminated in an upward trend in crimes committed online known as "cyber frauds." The illegal practice of attackers exploiting internet pages, browsers from the internet and applications on the internet is known as cyber fraud. For every corporation which conducts digital payment activities, reliable payments are necessary. Cryptography represents one among the foremost issues confronting participants in the electronic payment ecosystem. A lack of awareness and inadequate digital payment infrastructure are the factors contributing to the rise in the rise in these cyberattacks. There are several techniques used for safeguarding from potential risks of cyberattacks. Studying the background, risks, solutions and legislative actions to cyberattack on electronic payment techniques is the primary objective of the present article.

1. INTRODUCTION

There is an enormous rise in electronic payment methods in India in recent years, especially due to demonetization process in 2016 and the Covid-19 outbreak. it is believed that there are several methods for user to perform electronic payments, which include via the unified payments interface

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

(UPI), mobile banking, wallets, QR codes for payment and more. UPI has proved vital in assisting electronic transactions emerge in India. However, the rapid adoption of these sophisticated payment methods has additionally provided cybercriminals with novel ways for committing fraudulent by leveraging weaknesses in humans and electronic payment systems.

Cybercrime magazine states that by 2025, online crimes will have cost globally $10.5 trillion yearly. In addition, overall expenditures from cybercrime may rise by nearly 15 percentage per year over the subsequent period of 4years. In accordance to the RBI's annual report 6,659 card and electronic frauds of Rs 276 crore were reported in 2022-2023. This is more than the 3,596 illegal transactions involving Rs 155 crore that had been identified the previous year. Though enormous percentage of users make use of electronic means of payment, certain variables including an inadequate level of cognition, an inadequate ecosystem for cashless transactions, safety issues a preference for payments in cash, an absence of compatible digital laws and regulations and an absence of effective complaint and redressal techniques act as barriers to the development of electronic payment systems. It also raises the possibility of getting hooked by online criminals and subsequently enduring monetary damages. The rapid growth in electronic payments generated by everyday technological advancements is contributing to an explosion in fraud via the internet.

When so many individuals currently prefer to make payment electronically, hackers have become encouraged to develop innovative techniques to deceive customers. Despite providing up confidential data, several customers ended up losing their entire investment due to these scam artists. The increasing incidence of money laundering was made worse by online activity and the presence of devices with intelligence, thereby enhanced customers sensitivity to scam. Between 2022 to 2027, online shopping revenue losses through digital payment fraud could increase by 131%. Furthermore, as technology improves, scammers become increasingly sophisticated through digitalization. Some of the most significant challenges confronting banks and other financial companies currently is establishing an equilibrium among security and simple payments.

2. FRAUD IN DIGITAL PAYMENT AND CYBER SECURITY

Over the past decade, numerous instances of significant impact malware incidents have been discovered reported from a broad spectrum of business secto0rs, which includes, medical care, electronic commerce, telecommunications, banking, insurance, government agencies, producing goods and the hospitality industry. These incidents have produced a major impact as well as created cyber security as on of the biggest business risks. Geographical dimension regulates have no impact on potential of fraud via the internet. Organizations within India may have been considerably sensitive to such issue. Approximately 72% of companies have encountered cyberattack in some form, according to the KPMG report from 2017.The phishing attacks on channels for payment are the consequences of the increased scrutiny and intense drive for the adoption of technology. Denial of service (DDoS) attacks and spamming among the finest prevalent forms of attack. The total amount of cyber incidents increased in conjunction to the increase in the utilization of smartphones for banking via the internet, payments as well as commerce.

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

- **ONLINE PAYMENT FRAUDS**

Illegal activity can be performed at any stage in time. Several prominent methods and strategies employed by fraudsters to carry out such schemes throughout the entire payment system are described in the following

3. COMMON TYPES OF FRAUD

1. Theft of identification and fake identities:

Hackers gather customer personal data (such PAN/Aadhaar details or social media credentials) or crucial data regarding their banking accounts for the purpose to gain authorization and make payments via the internet or open a payment account to complete transaction. Hackers are able to carry through these kinds of scam due to the unprotected network exposes user's private data accessible to everyone. Additionally, there has been numerous instances within India wherein victim of identities stealing, financial institutions and payment processors have shared that scammer have utilized their private data to engage in a scam, particularly getting financial cards. Fraudsters can also claim to be an authorized representative (bank the staff member, cop, official from the government, healthcare professional etc.) or an approved access of their target.

2. Vishing and phishing:

The culprits of vishing scams pretend as the financial institution client service agents & encourage customers to upgrade or finish their electronic know-your-customer (eKYC) online data in order to maintain by employing their banking information. Criminals can get sensitive data whenever an end user finishes the procedure via the interest and them, they might use the publicly accessible OTP to perform crimes. Phishing fraud occurs whenever criminals transmit malicious hyperlinks in messages or emails which redirect victim to an internet address that seems extremely comparable to the official website of the financial institution. Customers eventually misinterpret the fake websites for authentic one and reveal confidential data, resulting in criminals can use to carry out illegal activities.

3. Skimming the web:

By inserting malicious programs on a software application's payments or confirmation pages of content, fraudsters may get confidential financial details using a form of security breach called web skimming. Scammers can introduce their malicious code into a trustworthy independent host site because e-commerce platforms, for example, employ third-party programs. Additionally, there have been numerous reported cases of web skimming in India, web hackers use online shopping platforms to obtain the card number, CVV, and date of expiration of unsuspecting customers. Websites for e-commerce have been specially called out because of their acceptance and availability.

4. Using QR codes:

Scammers offer the unknowing customer a fraudulent QR code, which they can scan to transfer funds to their bank account. Rather, whenever the QR code is scanned, the amount of money gets deducted from the customer's bank account. Fraudsters can additionally utilize their personal QR

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

code in place of the authentic one at commercial store areas, misleading consumers towards sending to the wrong account.

5. Social marketing:

a common method used in fraudulent transaction strikes is to mislead innocent customers towards sharing sensitive data by stating that they are experiencing a serious issue with their financial institutions.

6. Account transfer:

Hackers attempt to obtain unauthorized entry to a customer's account with such instances of scam involves stealing their login credentials while making payment. being that they modify the details that they obtained first before they make payment, fraudsters usually avoid identification.

7. Assistance with remote access:

The fraudsters involved in kind of scams encourage victims to allow them a wireless connection to their gadget so that they may resolve specific technical glitches. They typically accomplish this through posing an employee of the bank assisting with account unlocking or KYC assistance, or as a member of the technical support team of a service provider. After gaining remote access, the hackers gather all personal information related to the user's bank accounts and use it fraudulently to make purchases.

8. The network attack:

For carrying out systematic network assaults, hackers install dangerous software often referred to as "bots" into a network of computers. This renders it accessible to hackers to access user's devices and get past their privacy policies in order to obtain private data.

4. ANTICIPATED TECHNIQUES

A comprehensive approach involving legislative structures, education for the public and technological development is required for tracking money laundering and online scams. A comprehensive breakdown for some effective safety measures is given below

1. **Complex forms of authenticating:**

By seeking customers for confirmation of their true identity through different approaches such as biometrics, passwords or only one-time codes, multi-factor authentication also known as MFA provides an additional level of security. By recognizing abnormalities in user conduct, behavioral biometrics such as mouse clicks and the keyboard dynamics can increase privacy substantially.

2. Illegal activity detection technologies powers by artificial intelligence (AI):

Algorithmic procedures for machine learning and AI may immediately spot activities that are suspicious through analysis of patterns of internet transactions such systems offer anticipatory actions to potential hazards by using detection of glitches and to identify anomalies from conventional user conduct.

3. Encryption and secure communication:

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

Information that is sensitive, include banking information or username and password, remains secure during transfer through encrypted communication. Criminals were less likely to obtain data when safe protocols like HTTPA and encrypted messages on email services are in existence.

4. Customer awareness and cyber safety:

Programs for public education may educate consumers about regular frauds, suspicious activity as well as secure internet procedures companies may prevent human mistakes which result violations in the sense fall for emails that are phishing by regularly training staff member.

5. Global collaboration and legislation:

Comprehensive privacy laws have to be implemented by authorities and enforcement agencies and businesses are ultimately liable for having robust safety precautions in place. Law enforcement groups working together across borders might render it simpler to identify and apprehend criminals who operates across the globe.

6. Fraud prevention measures and secure payment platforms:

Fraudulent transactions can be detected and prevented by payment processors having inbuilt systems for detecting fraud. The tool such as encoding substitute responsive payment information with distinctive identification numbers, decreasing the possibility of information break in throughout actions.

7. Strategies for emergency retaliation and restoration:

To reduce harm in attacks via the internet, companies should set established specified incident handling processes such as recognizing and informing partners and separating compromised networks. In the case of attacks by ransomware or additional breaches of security, frequent backups of crucial information will ensure quick recovery.

8. Computerized for secure transactions:

Blockchain innovation may enhance monetary transaction safety and openness thereby rendering it tougher for the criminals to modify information. contractual arrangements can be mechanized and protected with smart contracts thereby reducing the potential for manipulation and mistakes made by humans.

9. Dissemination of threat information:

Initial alerts about novel frauds and loopholes can be obtained through enterprises and cyber security firms by collaborating to exchange threat information. Continuous vulnerability exchange of data is made feasible by systems such as data sharing and assessment centers (ISACs)

10. Insights and perception:

Using analytics applications to constantly track online systems may help to find weaknesses and address them swiftly. Organizations may take preventive measures through employing statistical analysis to spot emerging patterns of fraud.

11. Collaboration between the public and private sectors:

Working together between legislatures, commercial entities and charitable organizations may improve the impact and effectiveness of fraud prevention measures campaigns. Coordination could

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

concentrate upon standardization security protocols, strengthening reporting mechanisms and offering funds for the invention of new approaches.

12. Preventative measures for users:

For the sake of customers and financial organizations could offer more measures including expenditure rrestraints and transactions alerts. For the purpose of minimise financial damages for people as well as businesses, insurance companies may establish fraudulent activity insurance.

Thus, incorporating these measures may boost the web's ecosystem's resilience toward money laundering as well as online fraudulent activities avoiding serious damage to individuals as well as companies.

5. REACTIVE BEHAVIORS AS COMPARED TO PROACTIVE ONE

When it comes to preventing fraud, as great deal of security solutions is reacting addressing after it occurs. As a case study, fraud detection systems sometimes detect suspicious activity after a transaction, resulting in delayed responses. Before remedies are taken scammers do significant damage through taking advantages of frame between fraud executing and exploration.

- **Ecosystem disintegration:**

1. Diverse stakeholders: since banks, payment processors, websites and regulators frequently operate independently, safety precautions can differ.

2. Incompatibility: security solutions set up by different organizations might not function properly shared which makes points of integration exposed.

- **Exploits of societal manipulation:**

It may be complicated to defeat frauds using traditional technological tools since many of them rely more on psychological manipulation than their technical shortcomings. Among the instances are Attacks employing phishing that take benefit of human error. scams targeting individuals that might not be proficient in computers such the elderly. the sophistication of deceptive tactics.

- In an effort to avoid security measures, fraudsters are using innovative technologies:

1. **Automation and AI:** Bots are used to automate phishing attempts, create realistic looking fake websites and avoid exploration.
2. **Deepfakes:** bypassing traditional identity verification techniques, synthetic media is used to imitate actual individuals in voice or video communications.
3. **Cryptocurrencies:** untraceable digital currencies are used by fraudsters to launder money.
4. **Global variability:** security standards and laws differ per nation and region, thus creates gaps for international counterfeiters.
5. **Inconsistent adhering:** financial institutions can employ PCI DSS alongside additional standards or GDPR in a different way, causing vulnerabilities.

- **Limitations on resources:**

1. Financial: smaller businesses frequently don't have the funds to put strong security measures in place.

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

2. Human resources: the absence of competent cybersecurity professionals limits the ability to correctly track, examine and react to threats.

- **User-centric issues:**

1. Password vulnerabilities: credential stuffing attacks are possible since many users repeat weak passwords across platforms.

2. Awareness disparities: if people are n to aware of frauds, they make mistakes like relying on showing personal information or engaging on forged links. BYOD recommendations: since personal device protections are factor, Bring Your Own Device or BYOD guidelines in organisations regularly undermine security.

- **Absence of openness and trust:**

1. Opaque processes: mistrust results from users' frequent knowledge of the safeguards in place

2. Reputational risk: companies that fail to effectively communicate their work could suffer harm to their reputation even if they are healthy.

- **New technologies and weaknesses in the internet of things:**

Since many Internets of Things (IoT) devices lack strong security safeguards the rapid adoption of IOT devices introduces new vulnerabilities. these weaknesses are used by fraudsters to enter networks and carried out their schemes.

- **Insider dangers:**

Security systems may be accidentally or deliberately hacked by unfriendly insiders or employees lacking adequate instruction.

- **Limited cooperative:**

Data silos: companies often hesitate to share fraudulent data for economic or privacy reasons which lowers overall intelligence.

Reporting scams may be put delayed by victims, making it harder to recognize and eliminate threats in real time.

- **Challenging landscape of threats:**

Scammers and security providers are involved in an arms race as a consequence of their constant adjustment to new security measures.

Thus, it is noticeable that present security measures for money laundering as well as online frauds deals with a variety of challenges, including one which is the swiftly changing strategies of fraudsters who continually modify their strategies in order to get beyond established defenses. The increasing complexity of cutting-edge malicious software, spoofing and phishing make it challenging for present detecting technology to recognize attacks in instantaneously, in addition, scammers may choose an increased number of victims due to the increasingly complex nature of banking transactions and our dependence on online services. Most safety devices have difficulty finding an equilibrium between adequate safety and user comfort, which often results in resistance that discourages individuals from utilizing them. Attempts to tackle global money laundering are made

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

harder by the absence of standardized security procedures throughout networks and geographic regions that exposes both consumers and businesses to losses.

6. FUTURE RECOMMENDATIONS AS WELL AS RESEARCH

Since the fraudulent transactions in banks and fraudulent websites are now more advanced to contemporary safety precautions, there are multiple lacks of research that could represent avenues for improvements. Some of the most significant study gaps and various possibilities to strengthen cybersecurity towards money laundering and fraudulent websites are listed below.

1. Collaboration and data transmission across disciplines:

When government agencies, cybersecurity entities and financial companies acquire information regarding deception, there is a minimal interchange of threat information due to security concerns. Legislative restrictions and commercial considerations. the development of a coherent defense to fraudsters is hindered because this dispersion. The development of a united defense towards fraudsters is severely hampered by the limited exchange of threat data because of security concerns, legal constraints and commercial factors. Firms generally refuse to share confidential details regarding fraudulent activities or cyberattack for the fear of breaches of privacy, data security legislation breaches, or the potential destruction of their competitive edge. Businesses lack the ability to benefit from an increased thorough, unified knowledge of constantly evolving scamming methods as an outcome of this disintegration, which results in to specialized outcomes to new threats. In addition to this scammer may choose disordered systems by taking advantage of the vulnerabilities of individuals defenses. Using secure, anonymized threat data exchange platforms & well-defined legislative structures that manage privacy and legal problems while enabling an increasingly unified and effective fight against fraud, industry sectors have to collaborate together to prevent this. Cross-domain engagement could be improved by studies on safe sharing of information protocols and norms. A blockchain-based sharing of information platforms is a prime instance of a technology that could guarantee safe and open participation from stakeholders while preserving security and complying to regulations.

2. Monitoring and preventing fraud in real time:

The majority of fraud prevention techniques that businesses use presently rely upon on post-transaction assessment and rule-driven techniques, leading to responds to get prolonged. Rules-based systems operate through contrasting payments to predefined criteria or structures, including substantial payments or unusual behavior. Nevertheless, these regulations tend to be rigid and cannot be modified to swiftly adapt to shifting fraudulent techniques. Because post-transaction monitoring typically occurs once a transaction has been finished, fraudulent can go undetected until it is too late, which contributes to the issue further. substantial financial losses, damage to one's credibility and legal consequences may arise due to implement innovative, artificial intelligent-driven tactics that utilize machine learning techniques to identify new risks immediately, enabling more rapid and proactively actions to fraudulent attempt prior to they get more severe. Scammers are effectively conducting their fraudulent transactions through taking benefit of the delay. Investigating AI and

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

machines learning powered real-time systems for fraud detection might help detect misconduct prior to it occurs. To improve the accuracy and rapidity if preventing fraud, future technologies could use biometrics for behavior, immediate information analysis and machine learning to recognize abnormalities instantly as they happen.

3. AI and machine learning for fraud detection:

Phishing, vishing and other fraudulent methods are employed in a significant number of internet scams. Phishing typically involves fake messages or webpages that pose as legitimate businesses in an attempt to steal confidential data including login credentials or bank account information. In contrast, vishing involves making calls or audio messages where by attackers pose to be trustworthy people, like financial institution executives or government officials, in an effort to confuse victim into disclosing private data or transferring funds. These fraudulent activities are difficult to see and prevent as they often rely on emotions like uncertainty, hurry or excitement. The establishment of artificial intelligence models that can identify and prevent acts of social engineering requires additional research. To identify problematic language indicating of attempts at phishing or fake interactions, for example, natural language processing (NLP) tools may be used to analyze patterns of communication in emails, texts and phone calls.

4. Privacy-protecting measures:

Regulations which place a greater focus on privacy of data might conflict with security measures, especially when it comes to fraudulent activity identification, which requires to have access to enormous data sets for the purpose to detect fraud efficiently. Developing security preserving algorithms for machine learning such as federated learning where by enable algorithms to gain insight into data while risking people's confidentiality, may ai in striking a balance between security and privacy issues. Federated training allows model to be taught across scattered smartphones or computers without a requirement for hierarchical facilities. The significance of communicating directly with confidential data. The algorithm only sends aggregate insights such model developments with a centralized server after analyzing information local on the device being used by the user instead of collecting it all in a single location. This approach protects confidentiality while allowing systems to develop and acquire knowledge from a variety of data. Companies may enhance user safety and confidentiality through the use of federated learning techniques especially in sectors that manage private information such as banking, healthcare and the internet of things, but still utilizing artificial intelligence's ability to detect fraud or enhance services. Such methods could make it practicable for identifying fraud utilizing private user information without going beyond privacy regulations. Several decentralized devices. By ensuring that sensitive or private information never leaves the gadget, this method lowers the potential of hacking and enhances security and confidentiality. Federated machine learning can be utilized in cybercrime to reduce potential attack paths associated with centralized storage of information, protect user privacy and find deviations, identify hazards or improve safety algorithms.

5. Utilizing and safeguarding multiple-factor authentication (MFA):

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

Although having a frequently employed safety solution, multi-factor authorization can be challenging for customers to comprehend and is still susceptible to advanced attacks like phishing and SIM swapping. MFA is a common safety precaution which improves safety by requiring customers to prove their true identity utilizing numerous avenues such as a one-time code, biometrics and password. Even yet, MFA, may be hard for user to utilize which may result in resistance and lower adoption rates, especially when extra procedures interfere with the user experience. Additionally, even MFA is vulnerable to sophisticated phishing tactics that deceive users into disclosing MFA credentials or SIM swapping in which fraudsters misuse the victim's telephone number to obtain authenticating codes. without compromising privacy studies show that a blockchain- based identification of fraud systems could help in keeping track of illegal activity. For transparency actions, intelligent agreements and publicly accessible databases might be used, ensuring fast recognition of fraud and decentralized illegal transaction avoidance.

6. Protecting personal identity and reputation:

One crucial area that is highly at risk for deception is authentication of identity, especially if control of accounts or fake identities happen. An instance of trusted and federation authentication system. accounts mergers and acquisitions occur when scammers obtain unauthorized use of authentic accounts, often through using passwords which were accidentally obtained from phishing or breaches of data. In contrast, artificial identity fraud enables fraudsters to get beyond conventional verification systems by creating fake identities by merging authentic and fake data. These methods take advantage of flaws in outdated authentication processes, such as relying on easily exposed static information such as the social security number or knowledge driven verification. Innovative methods including biometrics and surveillance

Based on artificial intelligence detection of anomalies and multiple authentication methods have to be used for strengthening authentication of identities and ensure restricted individuals have to access to account and services. Companies may boost consumer confidence as well as identity related fraud avoidance by giving emphasis to multilayered and flexible techniques. The fixed personal information utilized in numerous current offerings (passwords, identification numbers etc.) are growing increasingly susceptible to hacking. Multiple kinds of identification, involving biometric info, behavioral analysis and contextual information, might be the focus of subsequent studies on flexible and adaptable identities management systems. In addition, individuals may have more control of their online profiles and be less vulnerable to digital identity theft when self-sovereign identities (SSIs) are created using blockchain-based technologies.

7. Security of decentralized finance:

Due to their decentralized design and uncertain laws, the development of decentralized finance structures has provided fresh possibilities for fraud, exploitation and scams. Decentralized finance structures rely on blockchain systems and attracts users who want transparency and independence by enabling peer-to-peer transactions without the need for middlemen. Because there is less centralized oversight, scammers can also exploit coding errors, alter smart contracts and carry out rug pulls

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

which are schemes were developers stop working on a project after receiving investor funding. Since these systems manage major user funds and do not have central oversight, secured electronic contracts, oracles and auditing processes are crucial for guaranteeing the reliability of the protocols used by decentralized finance. Oracles, which link intelligent agreements to actual information are vital but they need adequate.

8. Emerging technologies effects on fraud (AI, IOT,5G)

new technologies like IOT, 5G, AI challenge conventional safety precautions while offering up fresh opportunities for scammers. A dual-edged issue, machine learning (AI) allows hackers to develop complex frauds while simultaneously improving the identification of fraud through unusual and predicative analytics. Research could concentrate on building strong security foundations particular to new methods, such as creating secure IOT networks, minimizing hazards in 5g-enabled settings and assuring AI-powered systems are resistance to malicious attacks and theft.

9. Research in law and regulation:

There is an absence of homogeneous, worldwide laws that may provide specific guidance regarding how to deal with and punish new forms of fraud as financial institution fraud and online fraud emerge. Standards have to be standardized by regulators in order to reduce the jurisdictional gaps that fraudsters make use of, and coordination between the public and commercial sectors is needed to enhance reaction and tracking. In order to guarantee that authorities have the ability to effectively tracking. In order to guarantee that authorities have the ability to effectively track and identify scammers working across boundaries, this could involve setting out fresh rules for identifying and prosecuting perpetrators of international fraud. The subsequent attempts to tackle online fraud may be more successful if coordination keeps going, innovation expands, and laws are revised.

7. CONCLUSION

Scams on the internet and financial frauds have evolved significantly as a consequence of the rapid growth of technological advances, presenting previously unheard-of difficulties for people, companies and government. To protect against these new hazards, innovative and adaptable safety measures need to be developed at the same pace as this technological change. There are major weaknesses in the current state of internet security, especially in the fields of real-time identification, multi-platform harmony and instruction for users as shown by the constant dispute among scammers and safety vendors. Real-time data analysis, artificial intelligence and secure innovations ought to be prioritized in future avoidance techniques that can be recognize and mitigate crime before it arises. we may enhance safeguards against financial deception and internet scams by tackling current issues and investigating gaps, ensuring a more secure and reliable internet experience for every user. In order to conquer these lasting hazards and safeguard the security of internet-based financial institutions in the years that follow, cooperation, creativity, and a positive mentality will be necessary.

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

8. AUTHOR(S) CONTRIBUTION

The writers affirm that they have no connections to, or engagement with, any group or body that provides financial or non-financial assistance for the topics or resources covered in this manuscript.

9. CONFLICTS OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

10. PLAGIARISM POLICY

All authors declare that any kind of violation of plagiarism, copyright and ethical matters will take care by all authors. Journal and editors are not liable for aforesaid matters.

11. SOURCES OF FUNDING

The authors received no financial aid to support for the research.

REFERENCES

[1] Agarwal U,Rishwal V, tanwar S, Yadav M. Blockchain and crypto forensics; Investigating crypto frauds. International Journal of Network Management.2024 Mar;34(2);e2255

[2] Allahrakha N. Transformation of Crimes (Cybercrimes) in Digital Age. International Journal of Law and Policy.2024 Feb 25;2(2).

[3] Bhat AH, Kolhe D. Crime and fraud at the Community level: Social Networking Understanding into Economic crimes and psychology Motivations. JOURNAL OF Social Science and Economics. 2024 Nov 21;3(2):127-46

[4] Bansal U, Bharatwal S,Bagiyam DS, Kismawadi ER. Fraud detection in the era of AI: harnessing technology for a safer digital economy-InAI-Driven Decentralized Finance and the future of finance 2024

[5] De Andres P, Arroya D, Correia R, rezola A. Challenges of the market for initial coin offerings. International review of financial analysis.2022 Jan 1;79:101966.

[6] Fayyad-kazan H, Hejase HJ, Darwish CD, Hejase AJ. A Pilot Study to assess the success rate of email scams by phishing; Case in Lebanon. Contemproary Studies in Applied Sciences.

[7] Falade PV. Analysis of 419 Scams: The trends and New Variants in emerging Types.Int.J. Sci.Res.in Computer Science AND engineering Vol.2023 Oct;11(5).

[8] Gowda C. Understanding Fraud Risk in E-commerce with Special Emphasis on Credit Card Fraud and Triangulation Fraud.Issue 6 Indian JL & Legal Rsch.. 2022;4:1.

[9] Hazra R, Chatterjee P, Singh Y, Podder G, Das T.Data Encryption and Secure Communication Protocols. InStrategies for E-Commerce data Security: Cloud, Blockchain, AI and Machine Learning 2024

Chaitra V P, Nikhil Kumar M (2026). *Cyber Crime & Financial Frauds in Digital Banking, International Journal of Multidisciplinary Research & Review, 5(si2). 90-101.*

[10] Jimmy FN. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS)ISSN:3006-4023.2024 Apr 12;2(1);129-71.

[11] Makhdoom I ABolhasan M, Lipman J, Liu Rp,NI W. Anatomy of threats to the internet of things. IEEE Communications surveys and tutorials.2018 Oct 11:21(2):1636-75.

[12] Nayangareshi VO,Petrovic N. Efficient PUF based authentication protocol for internet of drones.In 2021 International Telecommunications Conference(ITC-Egypt)2021 Jul 13.

[13] Omollo VN,Musyoki S, Blue bugging java enabled phones via Bluetooth protocol for internet of drones.In2021 international telecommunications conference(ITC-Egypt) 2021 jul 13 (pp.1-4.IEEE.

[14] Peters A, Jordin A. countering the cyber enforcement gap: strengthening global capacity on cybercrime.J.Nat'l sec.L.&Pol'y. 2019:10:487.