Journal of Research and Development
A Multidisciplinary International Level Referred and Double Blind Peer Reviewed, Open Access
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-18, Issue-5| May-2026

Original Article

Composition and cyber security innovations perspectives on e-banking scams

Dr. D.jai Ganesh
Associate professor of commerce, Government first grade college, bangaru thirupathi
Email: jaisudhad@gmail.com

Manuscript ID:
JRD -2026-180516
ISSN: 2230-9578
Volume 18
Issue 5
Pp. 113-118
May- 2026
Submitted: 15 Apr. 2026
Revised: 25 Apr. 2026
Accepted: 10 May. 2026
Published: 31 May 2026

Abstract:

The rapid development of computer technology has had an impact on the global economy and has generally changed people and enterprises. This sophisticated insurgency has also led to an increase in online scams and budgetary extortion, posing serious risks to people, businesses, and financial education. This article examines how financial infractions and online scams have evolved in the modern era. It specifically examines common tactics including phishing, online installment extortion, cryptocurrency scams, social design attacks, and personality theft. The study examines the tactics employed by cybercriminals, examines the creative and psychological weaknesses that reveal victims, and evaluates the wider societal impact of these deceptive tacticsadditionally, it highlights the importance of regulations, cybersecurity developments, and open consciousness in combating online extortion. This article describes the problems caused by financial scams and online fraud. It also offers sensible solutions to lessen the effects of these transgressions in our increasingly interconnected society.

Keywords: *blockchain, the internet of things (iot), advancements, communication, cybercriminals, and cheating.*

Introduction

The era of computers has completely changed how individuals, businesses, and governments operate, offering extraordinary levels of convenience and connectivity. Recently, communication, shopping, and money management have become more accessible and useful than ever thanks to the internet, clever devices, and cloud computing. The first image shows a typical online purchasing structure. Despite its preferences, the computerized insurgency has also facilitated the spread of financial misconduct and online extortion. Cybercriminals have developed increasingly sophisticated techniques to take advantage of both human weaknesses and flaws in computer systems as innovation has advanced.

Picture 1: computerized fraud

The growing risk of advanced fraud

Phishing, ransomware, cryptocurrency tricks, and personality theft are all examples of illicit activities that fall under the broad category of online tricks and money-related extortion. These unavoidable infractions cause serious financial and psychological harm to individuals, small enterprises, and large organizations.

Address for correspondence:
Dr. D.jai ganesh Associate professor of commerce, Government first grade college, bangaru thirupathi.

How to cite this article:
Ganesh, D. jai. (2026). Composition and cyber security innovations perspectives on e-banking scams. Journal of Research & Development, 18(5), 113–118. https://doi.org/10.5281/zenodo.20914515

Quick Response Code:
Website: https://jrdrvb.org/
DOI: 10.5281/zenodo.20914515
OPEN ACCESS

Journal of Research and Development
A Multidisciplinary International Level Referred and Double Blind Peer Reviewed, Open Access
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-18, Issue-5| May-2026

The scope of these activities in india is alarming; according to cybersecurity and rbi investigations, electronic extortion has caused thousands of crores in losses annually, with many incidents being unreported or unclear. The fact that internet and financial extortion are always evolving and adaptable is a crucial feature. By utilizing emerging technologies like blockchain, artificial intelligence (ai), and the internet of things (iot), programmers are constantly evolving their tactics, making their plans increasingly intricate and challenginghowever, the global reach of the internet presents significant obstacles for indian law enforcement agencies in tracking down and prosecuting cybercriminals, especially when their activities take place across multiple jurisdictions. The primary reason for the increase in financial theft and online scams is our growing dependence on computers and the internet in our daily lives. As more people and organizations engage in online transactions, cybercriminals are grabbing hold of potential outcomes to exploit flaws in advanced phases and human behavior. The rapid growth of online banking, e-commerce, and sophisticated wallets in india has created greater opportunities for cyber extortion.

Cybercriminals' changing techniques

• **phishing attacks:** one of the most inevitable types of online deceptions, phishing attacks have evolved with a number of well-explained techniques, such as replicated websites and tailored messages designed to ensnare customers who reveal sensitive information. Character burglary, in which cybercriminals exploit stolen personal information to obtain illegal access to accounts, carry out financial extortion, or pose as victims, is closely connected. Because they take advantage of users' beliefs and need for mindfulness, these fakes are particularly successful. They frequently use phony emails or messages to trick consumers into disclosing personal information like passwords or credit card details. The real effects of these attacks are highlighted by high-profile breaches, such as those involving larger financial institutions and social media platforms.

• **cryptocurrency:** with the emergence of cryptocurrencies, online monetary extortion has reached an untapped stage. Blockchain technology has been misused for scams like ponzi schemes and cryptocurrency wallet hacks, despite the assurance of safe and simple transactions. Because cryptocurrencies are pseudonymous, it is difficult to track exchangers, recover stolen funds, and deter attackers. For example, one of the largest cryptocurrency scams in history was the one coin hoax, which defrauded investors of over ₹33,000 crore, or roughly $4 billion.

• **social building attacks:** social designing attacks, such as emotional manipulations and business mail compromise, have also significantly increased. These strategies rely on psychological manipulation to trick victims into exchanging money or revealing sensitive information. Advances in artificial intelligence have enabled fraudsters to create convincing deepfake audio and video samples, making these attacks more difficult to identify.

Recognizing and reducing the effect

Given their increasing frequency, it is essential to take into account the tools, effects, and moderating techniques associated with online trickery and budgetary extortion. The common types of tricks, the mental and specialized factors that enable them, and the societal consequences of these crimes are the main topics of this essay.

Effects and reduction

• **covid-19:** during the global covid-19 pandemic, money-related extortion and internet scams became much more common. Cybercriminals took advantage of weaknesses in unprotected systems and the increase in online activity as businesses and individuals moved to more remote locations. Pandemic-related scams including phony boost checks, phony charity offerings, and phony vaccine sales were common during this time.

• **financial accidents:** these frauds have a significant impact on one's finances and mental health. Casualties often have financial catastrophes, emotional distress, and damaged credit. Businesses may face reputational damage, legal liabilities, and operational disruptions. Additionally, the sheer number and complexity of these transgressions put a strain on cybersecurity and legal requirements, highlighting the urgent need for preventive measures.

• **identifying and keeping a strategic separation from tricks:** managing the increase in online and budgetary extortion calls for a thorough, multifaceted strategy. While open mindfulness exercises could help people identify and keep an effective distance from tricks, businesses need to strengthen their cybersecurity strategy. Governments and administrative organizations must order forceful enactment and encourage global engagement in order to curb cross-border extortion. The early detection and prevention of such threats can be greatly enhanced by developing innovations, particularly ai-driven extortion location frameworks.

An increase in inexpensive counterfeits and internet scams

The rising dependence on social networks and the growing integration if the internet into everyday life have led to a surge in financial extortion and online deceit. As more people and businesses conduct business online, cybercriminals have seized the opportunity to take advantage of flaws in computers and human behavior. The fast growth of digital wallets, internet banking, and e-commerce has led to an increase in empowered extortion. The scope and complexity of these threats are illustrated by a few recognized bank scams and online frauds. These are a few of the more outstanding instances.

Ponzi and triangle tricks: the key distinction between the two types of extortion is that ponzi schemes typically ask victims to make financial contributions with promised profits expected at a later time. Unlike ponzi schemes, pyramid

Journal of Research and Development
A Multidisciplinary International Level Referred and Double Blind Peer Reviewed, Open Access
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-18, Issue-5| May-2026

schemes typically offer a victim the opportunity to "make" money by recruiting additional victims. Millions of people have been duped by internet ponzi schemes that promise larger returns on speculation with no risk. The saradha chit finance scam, which defrauded thousands of speculators mostly in the west bengal state and odisha of approximately ₹2,500 crore, is a notable example of how computerized communication may accelerate the spread of scams. Using its chit support programs, the firm enticed casualties with promises of large profits. Numerous captures, political debates, and widespread financial specialists' elimination were all part of the aftermath. In a different instance, the indian police arrested two people after filing a complaint against hawk pay reducing. The business purported to connect financial experts with businesses including amazon (amzn.o), britannia (brit.ns), and others, and had advertised returns of up to 22%.

Ransomware attacks: attacks that restrict access to data or computer systems and demand payment to unlock them have becoming more frequent. Cybercriminals use ransomware to jumble victims' data and demand payment, usually in bitcoin, to restore access. Unmistakable events that target governments, corporations, and clinics, like the ransomware and revil ransomware attacks, have caused extensive damage. Examples include the 2017 ransomware ransomware infection that compromised several systems, including state-run initiatives like the state of gujarat wide region organization (gswan), exposing weaknesses in fundamental government infrastructure.

Romanticism tricks: also referred to as "catfishing" or "dear tricks," fraudsters create fictitious online personas to create intense connections with victims, ultimately tricking them into paying money or divulging personal information. In order to obtain reserves, scammers frequently fabricate tales about financial difficulties, family emergencies, or trip expenses. These tactics frequently begin on social media platforms or dating apps. Sentiment fraudsters manipulate victims into trading money by creating fictitious internet connections and taking advantage of their emotional weaknesses. According to studies, these tactics brought in millions of dollars annually, with the majority of victims being targeted by dating sites and social media. Cases include deceptive individual stories, phony messenger services, hint movement techniques, and more. In one instance, a woman from delhi lost ₹50 lakhs to a man posing as a uk expert who promised endowments. The man then added a fictitious traditions officer who asked for clearance costs. Additionally, a man posing as an armed force official seeking money for a fictitious issue conned a woman in pune out of ₹12 lakha woman in mumbai lost ₹5 lakh to a whatsapp friend who pretended to have been a uk engineer.

Business email compromise (bec): in the nation of india, scammers use phony emails to trick employees into transferring money or revealing personal information. Business email compromise (bec) is the name given to this tactic. These attacks frequently rely on social building techniques to get over security barriers by impersonating reputable retailers or senior administrators. By posing as administrators or suppliers, bec strategies aim to prevent businesses from making unapproved payments. In a significant cyber theft case in 2018, a group of indian fraudsters pretended to be beat the administrators of a universal company and used fictitious emails and created archives to trick a backup of an italian company, tecnimont limited pvt. Ltd., in pune into transferring ₹200 crore (roughly $27 million) to open a bank account accounts in hong kong. In order to authorize assistance exchanges via various exchanges, the aggressors used business email compromise (bec) tactics that mirrored top officials and created a sense of direness. The extortion was just found.

Tech back tricks: end the call right away if someone says there's a problem with your machine. In fact, a surprising tech return call is probably a scam if the number appears to be genuine or local. By manipulating caller id data, these scammers frequently pose as reliable or local companies. Any pop-ups urging you to get in touch with tech support should be ignored. In order to trick victims into paying for unnecessary services or granting more access to their devices, scammers pose as legitimate blue tech support operators. These scams frequently target the elderly because thieves take advantage of their limited awareness through technology.

These well-researched incidents demonstrate the adaptability and creativity of cybercriminals. The various approaches, locations, and tactics used in each instance highlight how important it is to continue being cautious and making constant efforts to fight internet scams and budgetary extortion. A mediawiki location's recent changes page that was impacted by skilled back fraudsters pushing fictitious "offer assistance lines"

Important perspectives on money threats (2023–2025) an overview picturein india, banking extortion is on the rise, primarily due to technological trickery. Open division banks cause more significant financial losses, but private banks report more cases. The most common types of fraud are tied to cards and the internet, with donkey accounts emerging as a hidden but real threat. To combat this growing issue, experts are increasing open announcements and pushing permission initiatives.

Journal of Research and Development
A Multidisciplinary International Level Referred and Double Blind Peer Reviewed, Open Access
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-18, Issue-5| May-2026

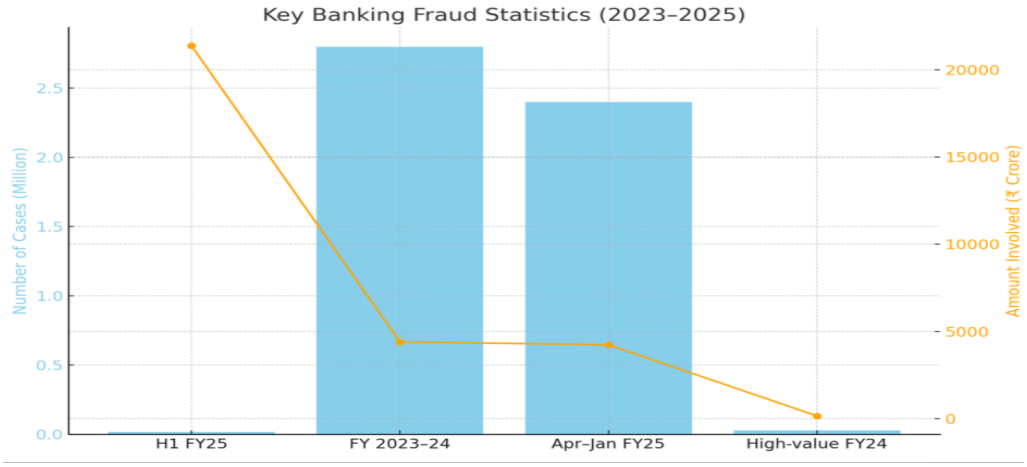

Image 2: sophisticated budgetary frauds

In fy25, banking fraud in india increased dramatically, with losses exceeding ₹21,000 crore in just six months. The major factors behind this increase are computerized schemes, particularly those involving card fraud, network building, and donkey accounts. The scope and progression of these fakes highlight the urgent need for more grounded preventative actions and more notable open awareness, despite administrative actions and advanced detection frameworks.

Crucial remedies for fighting financial fraud and online tricks:

Combating money-related extortion and internet tricks requires a multimodal approach that includes administrative structures, open training, and mechanical advancements. A detailed explanation of several practical security methods is provided in table 1.

Table 1: measures to prevent fraud

Strategies	Technique
Improved verification	By forcing users to confirm their identity using a variety of techniques, like biometrics, password or one-time codes, multi-factor authentication (mfa) improves security. Furthermore, by identifying anomalous user behavior, behavioral biometrics like keyboard dynamics and mouse movements enhance security even more.
Intelligent fraud identification	By examining trends in online transactions, machine instruction and artificial intelligence systems can promptly identify questionable conduct. By employing anomaly detection to spot departures from typical user behavior, these systems enable proactive reactions to possible threats.
Safe data security	End-to-end encryption protects sensitive data during transmission, including login credentials and financial information. The risk of data acquisition by attackers is greatly decreased by using secure technologies like https and secured email services.
Vigilance and training of users	People can learn about popular fraud schemes, warning signals, and safe internet practices through public awareness initiatives. By routinely providing cybersecurity training to employees, employers can help avoid human blunders like falling for phishing emails.
International cooperation & policy	Strict data protection laws must be enforced by governments and regulatory bodies, and businesses must be held responsible for putting strong cybersecurity measures in place. The identification and capture of cybercriminals working worldwide can be greatly improved by cross-border cooperation between law enforcement organizations.
Payment systems protected against fraud	Unauthorized transactions can be detected and stopped by payment gateways with incorporated fraud detection systems. One such method that reduces the possibility of data theft is tokenization, which substitutes unique identifiers for critical payment information during transactions.
Blockchain-powered security	Blockchain technology can increase the security and openness of financial transactions, making it more difficult for thieves to manipulate data. Smart contracts can automate and safeguard contractual agreements, reducing the likelihood of human error and tampering.
Management of cyber incidents	Organizations should establish clear incident response protocols, such as identifying and notifying users and isolating compromised systems, to lessen damage during cyberattacks. Regular backups of critical data can ensure prompt recovery in the case of attacks by ransomware or other security breaches.
Collaborative cybersecurity initiatives	Collaboration between governments, corporations, and nonprofits can expand the reach and effectiveness of anti-fraud initiatives. Cooperation might focus on improving reporting systems, standardizing cybersecurity practices, and funding the creation of innovative solutions.

Journal of Research and Development
A Multidisciplinary International Level Referred and Double Blind Peer Reviewed, Open Access
ISSN : 2230-9578 | Website: https://jrdrvb.org Volume-18, Issue-5| May-2026

By incorporating these agreements, the sophisticated ecosystem's defenses against online scams and budgetary extortion can be strengthened, preventing actual harm to people and companies.

Problems with existing solutions

The development of comprehensive security measures has lagged behind the increase in financial fraud and online scams, creating a problematic situation for individuals, companies, and governments. Table 2 provides a detailed analysis of the issues with the safety arrangements available today.

Table 2: problems with existing fixes

Challenge	Explanation
Latency of response	Fraudulent transactions may go undetected until the funds has been stolen since many existing systems are unable to respond to data in real time. The real-time verification procedure is frequently circumvented by skilled attackers.
Restricted resources	Smaller companies sometimes lack the resources to implement robust security measures. Additionally, a shortage of cybersecurity specialists hinders efficient threat tracking, analysis, and response.
Cyberthreats of the future	Broad use poses a significant security risk. They are a great target for cybercriminals looking to break into networks and commit harmful acts because of their intrinsic vulnerability.
Risks to internal security	Security procedures can frequently be circumvented by malicious insiders or employees with insufficient training. Insider threats are the most challenging kind of fraud to identify and prevent.
A changing threat environment	An continuous "arms race" in the cybersecurity space is shown in the ongoing innovation of fraudulent practices in response to sophisticated security protocols. The long-term efficacy of static defensive systems is intrinsically challenged by this shifting threat scenario.

The rapid expansion of the computer scene and the steady development of cybercriminal tactics present a challenging and dynamic threat to financial security. Current defenses are struggling to keep up with increasingly sophisticated threats and the expanding attack surface. Customers and businesses will remain helpless against financial crime until security measures find a balance between robust assurance and customer satisfaction, and global standards are firmly established.

Conclusion

In conclusion, the increase in sophisticated online tactics and financial extortion emphasizes the urgent need for more clever, adaptable security measures. As attackers increasingly abuse innovations like artificial intelligence, blockchain technology and social building, traditional defenses are no longer adequate. The main types of internet scams and financial frauds that are common in the modern era are compiled in this audit. Critical inadequacies in real-time detection, multi-platform coordination, and client training are revealed by the ongoing battle between attackers and defenders. Additionally, the widespread use of iot devices and the emergence of social design techniques highlight the need for a cohesive, all-encompassing approach to cybersecurity. In order to stay ahead of emerging threats, future efforts must prioritize proactive processes that make use of real-time data and privacy-focused advancements. Future research should focus on developing extortion avoidance systems that are capable of identifying and mitigating threats as soon as they arise. This includes protective devices, real-time analytics, and saddling machine learning. Open and commercial divisions will need to work together to set up flexible security methods and global regulations. The ongoing development of the sophisticated environment must coincide with the advancement of cybersecurity. To ensure a safe, adaptable, and reliable advanced budgetary environment, supported engagement, advancement, and a forward-thinking approach will be essential.

References

1. Vivek kumar sindhi, ritika maini, dr. Harsimran kaur, (2025), “e-banking frauds: insights from literature and security innovations”, international journal of commerce and management studies, vol 10, no 2, 53-69.
2. Gill, s. S., wu, h., patros, p., ottaviani, c., arora, p., pujol, v. C., ... & buyya, r. (2024). Modern computing: vision and challenges. Telematics and informatics reports, 13, 100116.
3. Sergeyev, a. Y., & shirokova, o. V. (2023). Fraud in a digital society in the context of social change. Цифровая социология/digital sociology, 60.
4. Yanamala, a. K. Y. (2024). Emerging challenges in cloud computing security: a comprehensive review. International journal of advanced engineering technologies and innovations, 1(4), 448-479.
5. Nosál, j. (2023). Crime in the digital age: a new frontier. In the implications of emerging technologies in the euro-atlantic space: views from the younger generation leaders network (pp. 177-193). Cham: springer international publishing.
6. Ahmed, m., ansar, k., muckley, c. B., khan, a., anjum, a., & talha, m. (2021). A semantic rule based digital fraud detection. Peerj computer science, 7, e649.

7. Bensaid, a., & draoui, h. (2024). Proving cyber-crime using modern technology: artificial intelligence as a model (doctoral dissertation, ibn khaldoun university-tiaret).
8. Agarwal, u., rishiwal, v., tanwar, s., & yadav, m. (2024). Blockchain and crypto forensics: investigating crypto frauds. International journal of network management, 34(2), e2255.
9. Latha, s. B., dastagiraiah, c., kiran, a., asif, s., elangovan, d., & reddy, p. C. S. (2023, august). An adaptive machine learning model for walmart sales prediction. In 2023 international conference on circuit power and computing technologies (iccpct) (pp. 988-992). Ieee.
10. Modise, j. M. (2023). Community policing strategies include community patrols, neighborhood watch and community policing. International journal of innovative science and research technology, 8(7), 3458-3476.
11. Guo, h., & yu, x. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067.
12. Patel, b., vasa, j., & mewada, h. (2024). E-prime-advances in electrical engineering, electronics and energy.
13. Saha, s., hasan, a. R., mahmud, a., ahmed, n., parvin, n., & karmakar, h. (2024). Cryptocurrency and financial crimes: a bibliometric analysis and future research agenda. Multidisciplinary reviews, 7(8), 2024168-2024168.
14. Roosenboom, p., van der kolk, t., & de jong, a. (2020). What determines success in initial coin offerings?. Venture capital, 22(2), 161-183.
15. Chiu, t., chiu, v., wang, t., & wang, y. (2022). Using textual analysis to detect initial coin offering frauds. Journal of forensic accounting research, 7(1), 165-183.
16. Maji, s. K., & laha, a. (2023). Role of financial and digital literacy in determining digital transaction behaviour: evidence from student level survey in west bengal (india).
17. Lallie, h. S., shepherd, l. A., nurse, j. R., erola, a., epiphaniou, g., maple, c., & bellekens, x. (2021). Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248.
18. Thakur, k., ali, m. L., obaidat, m. A., & kamruzzaman, a. (2023). A systematic review on deep-learning-based phishing email detection. Electronics, 12(21), 4545.
19. Patel, k. (2023). Credit card analytics: a review of fraud detection and risk assessment techniques. International journal of computer trends and technology, 71(10), 69-79.
20. Luo, j., luo, j., nan, g., & li, d. (2023). Fake review detection system for online e-commerce platforms: a supervised general mixed probability approach. Decision support systems, 175, 114045.
21. Bachmann, n., tripathi, s., brunner, m., & jodlbauer, h. (2022). The contribution of data-driven technologies in achieving the sustainable development goals. Sustainability, 14(5), 2497.