International Journal of Civil Law and Legal Research

E-ISSN: 2789-8830
P-ISSN: 2789-8822
Impact Factor (RJIF): 5.62
IJCLLR 2026; 6(1): 23-28
www.civillawjournal.com
Received: 14-11-2025
Accepted: 16-12-2025

Subhashis Chakrabartty
Research Scholar, School of Legal Studies, Seacom Skills University, Kendradangal, Bolpur, Birbhum, West Bengal, India

Kishwar Parween
Research Supervisor, School of Legal Studies, Seacom Skills University, Kendradangal, Bolpur, Birbhum, West Bengal, India

Correspondence
Subhashis Chakrabartty
Research Scholar, School of Legal Studies, Seacom Skills University, Kendradangal, Bolpur, Birbhum, West Bengal, India

Regulating digital banking and data privacy in India: A comparative legal analysis with international standards

Subhashis Chakrabartty and Kishwar Parween

DOI: https://www.doi.org/10.22271/civillaw.2026.v6.i1a.181

Abstract
With the fast-growing digitization of all sectors, digital banking quickly changed the face of traditional banking in India by providing easier, faster and cost-effective financial services. Banks are increasingly providing services 24x7 to customers through electronic means (such as net banking, mobiles banks, ATM network and electronic fund transfer systems) which are available across time zones in both rural and urban areas. Even as digital banking has delivered tremendous benefits to customers, by driving financial inclusion and efficiencies, it has also escalated fears about data privacy, cybersecurity and growing incidence of digital fraud. The growing reliance on digital banking services has left both consumers and banks vulnerable to a gamut of cyber threats such as ATM fraud, NEFT frauds, social engineering attacks, insider-enabled scams and epic corporate banking heists. Such threats do not only lead to money loss but also create the problem of trust and leak sensitive personal and financial data.
Under such circumstances, providing strong legal protection on data privacy and digital transactions has emerged as an important challenge for regulators and policy makers. Methodology: The research follows the doctrine method of social scientific research comprising primary data (judgment of Supreme Court and High Courts, gazette notification of Reserve Bank of India, reports published by government) as well as secondary sources (journals). The research uses famous banking-crime cases as examples to critique weaknesses in supervision, internal control, and corporate governance systems. It also analyses the schemes of Indian Penal Code, banking laws and corporate legislation vis-à-vis digital banking frauds and finally it examines the efficacy of the extant penal measures against such abuses. The study finds that while India has achieved significant success in digitising its banking system, the legal and regulatory infrastructure needs further strengthening to effectively deal with cyber threats. The study highlights the necessity for further data security initiatives and progress in institutional governance, public understanding and more safety-oriented technospace to make digital banking in India suitable and reliable.

Keywords: Banking regulation, digital banking, cybercrime, data protection, comparative law

1. Introduction
The word "bank" is used and circulated widely. "Bank" has the same meaning in Bengali and English. The phrase has historically been connected to banks and financial institutions [1, 2]. Due to the competitive environment with new technology, the bank has been completely automated for the last four years. Through e-banking, a bank intends to launch a fundamental concept of information technology enabled services. This percentage was just 47% before to the pandemic, but by the third quarter of 2020, it had risen to 55%. Banks are starting to realise that their clients are fixated on maintaining their trust and safeguarding their privacy. The nature of banking has changed over the years, from day bricks and mortar to digital screens (laptops, mobile) bricks. When it was made impossible to transfer any money for foreign trade, a technological experts and a bank, then developed a practice that could be used by us in the electronic commercial temple-prayer hall. Net banking or e-payments are the names used for online financial transactions. The system would require all banks with branches to participate [3, 4]. Mobile banking has penetrated far beyond cities to villages/semi-urban areas encouraged by the increasing affordability of smartphones and better internet access. This growth has helped to drive financial inclusion by bringing the unbanked and underbanked into the formal financial system. With digital payments, the risk of counterfeiting for physical cash transactions are removed and instead replaced with high-level security in which debit card transaction can be reported instantly as lost or stolen and blocked [4].

"PHISHING" is the term used by fraudsters to describe the theft of an individual's electronic personality. It might be a very profitable enterprise [1]. Approximately one crore personality robberies occur per year in the United States alone. The Web has contributed to the problem's measurements. Many people have died (mostly the shippers that give things to the cheat of electronic character) [2]. Despite these advantages, the rapid digitization of banking services has also given rise to new forms of financial fraud and data privacy concerns. The increasing reliance on electronic platforms exposes customers and banks to cyber threats, including unauthorized access, identity theft, data breaches, phishing attacks, and social engineering frauds. As digital banking systems process vast volumes of sensitive personal and financial data, ensuring the confidentiality, integrity, and security of such data has become a critical legal and regulatory challenge [3, 5].

The advent of digital banking has therefore required that a legal infrastructure address issues concerning data protection, cybersecurity, consumer protection and institutional responsibility. The Indian legal response to these threats is a mix of the general criminal law, sectoral banking regulations and nascent data protection laws. Nevertheless, legislations' impacts on the prevention and intervention of digital banking frauds are still under the spotlight [3, 5].

This paper attempts to carry out a comprehensive review of the trend, concept and phenomenon of digital banking in India, by examining the nature and extent of digital banking frauds in relativity with legal and regulatory response which is made towards data privacy and cybersecurity aspect. Through reviewing country-specific case studies, jurisprudential accounts and policy directives, the research seeks to unveil shortfalls within the governance of digital banking to recommend underpinning legal and policy reforms that will buttress consumer protection and trust over banking systems online.

2. Digital Banking

Digital banking is the provision of financial services like loans, deposits and cards which a bank offers to customers through electronic channels/online banking in an effort not to impose customers to bank, digital banking mechanizes all the products of banking. Digital banking enables customers to access their bank 24/7 which doesn't depend on whether you are a night person or not. "Customers can also schedule regular payments, e.g. to pay phone or gas bills, and work in advance which dates to use," he says on the bank's online banking platform. Digital banking operations too are running in the rural areas that is also on inexpensive mobiles as yes there actually IS decent internet connection almost anywhere. Risk of fraudulent transfer-of-funds will probably be negligible now that digital banking transfers have come into their own. For internet banking, lost ATM cards can be reported and canceled online right away [4].

With digital banking, all transactions are performed whenever you need them. One of the key benefits is that banking can be provided 24×7, providing customers with access to their finances when they want it and not just during office hours or business days. In a similar fashion, the internet banking facilities can allow setting up automated and regular payments for utilities like electricity, gas and telecommunication etc., so as to limit reliance on manual processes that cause delays in the transactions [4].

2.1 Different type of digital banking:

- **Banking cards:** Cards support other digital payment solutions beyond cash withdrawal. It can be used on Point of Sale (PoS) machines and for online transactions. Prepaid cards, which are not linked to a bank account and consumed according to the loaded funds, can be offered by banks as well. There were various banking cards such as Visa Debit Card, Credit Card, ATM Card and Prepaid Card. Attached to a customer's bank account; when used for purchases or cash withdrawal from ATM, the money is deducted immediately [6, 7].
- **Unstructured Supplementary Service Data (USSD):** You can transact on your mobile by simply dialing 99#. The high ratio promoting the establishment of local finance is a comprehensive policy. All of these are visible on a mobile screen by the time it gets to its destination. It is the latter Works on pure GSM systems [6, 7].
- **PoS terminals:** Card not-present is used where the card holder does not have his or her card physically with him or her at the time of transaction. It is a process also used by gas stations and supermarkets. Nowadays, virtual and mobile PoS terminals exist and use web-based apps as well as NFC-enabled phones to enable payment [6, 7].
- **Internet and Mobile Banking:** Reaching services opening accounts, transferring funds or closing accounts via the Internet, called e-banking. It is considered a type of digital banking as it contains some but not all online features. On a related note, mobile banking gives you access to your banking needs through phone apps. Mobile banking is also contributing to a rise in banks without brick-and-mortar branches [6].

3. Digital banking and the problem of data privacy

The rapid expansion of digital banking has significantly transformed the banking sector by enabling customers to access financial services through electronic platforms such as internet banking, mobile applications, automated teller machines, and electronic fund transfer systems. Digital banking enhances efficiency, convenience, and financial inclusion by reducing dependence on physical bank branches and allowing round-the-clock access to services [4]. However, this technological transformation has also intensified concerns relating to data privacy and protection of personal information.

Digital banking systems involve the continuous collection, storage, and processing of large volumes of sensitive personal and financial data, including identity details, account information, transaction histories, biometric data, and behavioral patterns. Such data is often shared across a complex ecosystem comprising banks, payment service providers, fintech companies, cloud service providers, and third-party vendors. This interconnected structure increases the vulnerability of customer data to unauthorized access, misuse, and cyberattacks [8]. One of the primary data privacy challenges in digital banking is the rising incidence of cyber frauds such as phishing, ATM skimming, identity theft,

unauthorized electronic fund transfers, and social engineering attacks. These frauds frequently exploit weaknesses in data security systems or manipulate customers into disclosing confidential information. Low levels of digital literacy and inadequate awareness among users further aggravate the problem, making customers easy targets for cybercriminals [6].

Moreover, the increasing use of modern technologies, such as big data analytics, artificial intelligence or automated decision-making tools in banking gives rise to new privacy challenges. They depend heavily on customer data to, for example, score creditworthiness, detect fraud and provide personalised financial services. Without clear consent mechanisms and meaningful oversight, these practices could introduce harmful levels of surveillance, profiling and even discrimination [9, 10]. In India, the problem pertaining to data privacy challenges also stem from lack of uniformity in the preparedness concerning cybersecurity law among banks, specifically cooperative and regional rural banks and technology digital banking law. Though specific guidelines for sectors released by the Reserve Bank of India and forthcoming data protection legislation aim to tackle these issues, enforcement mechanisms, accountability and a consumer redress mechanism are current challenges [10-13].

4. Methodology

4.1 Sources and Analytical Framework: The study employs the Doctrinal Research Method and heavily relies on (inter alia) decisions of the Apex court in India, i.e, the Hon'ble Supreme Court along with various state courts. It also mentions the Cyber Appellate Tribunals and international bodies and their advisories on cyber security with a spotlight on digital banking [13].

4.2 Data collection

- **Primary Data**: Gather information that has never been used before and relates to a new subject. In our case, this means news on cyber frauds. Questionnaires given out to bank employees, RBI notifications like among others will provide primary data [13].
- **Secondary Data:** It is the prior collected and utilized data. In our research we will use periodicals, journals, books extensively as secondary data [13].

4.3 Tools and Techniques: Statistical tools such as statutory materials, case reports, periodicals, government publications, national & international journals e-resources etc. were used. Case laws across different Courts, including the Supreme Court of India, Cyber Appellate Tribunal and applicable international tribunals to ascertain as to how courts have adjudicated on matters concerning internet banking frauds, data protection, privacy rights or IPR protections/applicability etc. [13].

Software: Ms. Excel is one crucial piece of software and equipment: used primarily to explore putative correlations between variables in Microsoft Excel [13].

5. Results and Discussion

5.1 Different type of Digital Fraud

- **ATM Fraud:** Charge cards and ATM cards are similar. An ATM card can be used for any fraud that is carried out using a credit or charge card. A former army guy had gone to an ATM to take out cash in a different instance. He found it intriguing because new money is rarely given out via an ATM. In response, the bank where the ATM was located said he had been tricked by a counterfeit note. They also questioned whether the Treasury Department, which put the notes in ATMs, had set up a trap or if the consumer was being abducted. The number of reported frauds involving ATMs and other devices rose by more than 65% in 2022 compared to 2021, and the total amount involved nearly doubled, according to the Finance Ministry's report to a Parliamentary Committee. Meanwhile, the National Payment Corporation of India stated that an average of 2,000 consumers are impacted by cyber fraud every month [14].
- **NEFT Fraud:** EFT is referred to as NEFT (National Electronic Fund Transfer) in India. No transaction is identified by RBI. Assume that there aren't many EFT (or NEFT) transactions overall. However, they do produce close to 85% of cash flow. Millions of rupees may soon be lost to the nation due to EFT fraud, in which thieves steal money directly. The Wire Exchange After being released from prison, Mr. Moore enroped Taylor, a bank employee. He joined forces with another employee to serve as a representative for the EFT department of the current National Bank in Chicago. The next prepared a little spade work: three bank accounts were opened in Vienna, Austria, and only those few missing individuals were identified as casualties with Taylor's help. Indeed, he was now prepared to kill [14].
- **ICICI Bank Loan Scam:** A dispute involving a 3,250-crore ($437 million) advance to the Videocon Bunch in 2012 involves Chanda Kochhar, the former CEO and Overseeing Executive of ICICI Bank. Illustration and How It Occurred: In a quid pro quo arrangement, Videocon Gather was given credit, while Deepak Kochhar, Kochhar's spouse, allegedly received kickbacks from NuPower Renewables. The Central Bureau of Examination (CBI) confirmed that Chanda Kochhar mismanaged her position to grant the loan, causing ICICI Bank to suffer an unfair loss. Escape clauses: With senior bank officials mistreating their experts for individual pick-up, the case brought attention to the challenge of fascinated and vulnerable corporate administration within the Indian account management framework [15].
- **The PMC Fraud:** The RBI was in charge of the PMC bank's operational management for six months after the Save Bank of India took over in September 2019. The financial expert starts to freeze and contact the nearest branches. At that time, the RBI increased the withdrawal limit to 10,000 and 25,000. By hiding the faulty advance records of ₹6,500 crores, Bliss Thomas, the former supervisory chief of PMC Bank, deceived the bank sheets, the assessors, the government, and the Save Bank of India for many years. Lodging Advancement and Foundation Limited (HDIL), a legitimate bequest company, took these ₹6,500 crores [14, 15].

  The executive was apprehended in February of 2022. When the Reserve Bank of India found that PMC Bank had hundreds of fictitious accounts to conceal over 4,300 crore bank loans to its parent company—which was then in risk of having to file for bankruptcy—the fraud case came to light. The bank regulator claims that

fraudulent loans involving HDIL on PMC's balance sheet were twisted out of shape [14, 15].

- **The Kingfisher Vijay Mallya Scam:** In India, Kingfisher tycoon Vijay Mallya is accused of extortion and money laundering totalling ninety billion rupees. The ostentatious Indian businessman, widely regarded as India's response to Richard Branson, expanded his newly acquired territory, formed Breweries Bunch, whose valuable assets included its refreshments division and Kingfisher Carriers, and led an extravagant lifestyle by purchasing Equation One, cricket teams, islands, and vintage cars. However, the demise of Kingfisher Carriers, which had accumulated US$1 billion in debt and ceased operations in 2012, freed him from inconvenience [15].
- **Social Engineering Frauds:** Social engineering is the hacking of people's minds to trick them into divulging personal information (such as email addresses, computer passwords, bank account numbers, and personal details). This technique, also known as their virtual personality, allows hackers to access our bank accounts and gain access to our computers, tablets, and mobile phones. In order to extort money and support other detrimental initiatives, they can modify and misuse the data [14, 15].

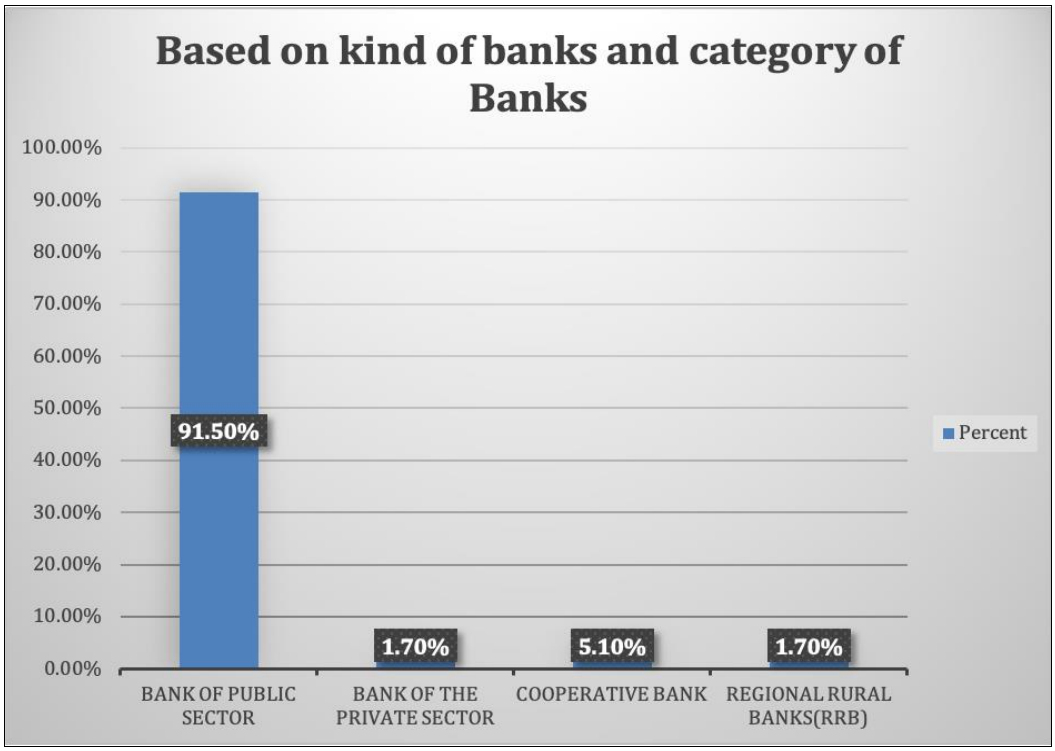
5.2 Data Analysis

Table 1 shows that the distribution of cases across various categories of banks indicates marked predominance of the public sector banks. Public Sector Banks among the 59 cases, the public sector banks constituted 54 cases (91.5%), which reflects that they are more prone to this issue under consideration. This high ratio is primarily due to their larger customer base, geographic footprint and turnover volume. Similarly, the customer base of public sector banks is also diverse with a fair share of rural and non-digital-savvy customers who might turn out to be more vulnerable to operational and security risks.

In the private sector banks, as opposed from the public sector, only one case is (1.7%) is a significant reduction and may show good powers of internal control, modernize technology base and risk management systems. Cooperative banks, of which there are three (5.1%), introduced cases also having just low medium exposure because of limited technological infrastructure and weaker supervision than scheduled commercial banks. Regional Rural Banks (RRBs) register a single case (1.7%). However, low though it is, this one instance brings to focus the risk of rural credits and lower digital proficiency.

Table 1: Based on kind of banks and category of banks, the data following is given [16]

Category of Bank	No of Cases	Percent
Bank of Public Sector	54	91.5
Bank of the Private Sector	1	1.7
Cooperative Bank	3	5.1
Regional Rural Banks (RRB)	1	1.7



Sources: Computed by researcher 2025

Fig 1: Based on kind of banks and category of Banks

The aforementioned result highlights the extent to which public sector banks have failed to stop or manage internet banking fraud. The secret to social engineering fraud is a trusting environment. Before violating their victims' trust, fraudsters use well-known or authoritative identities to reassure them. One such instance is the notorious "Jamtara

scam" from India. Here, residents of the Jamtara neighbourhood would pretend to be bank staff and call credulous victims. They would use coercive or frightening tactics to persuade victims to reveal their banking credentials, resulting in significant financial losses for the targeted persons.

In general, and present study suggest high account of cases in public sector banks demand better cybersecurity for the banking system as a whole along with good regulation (more so for PSBs) and customer awareness particularly with reference to public sector banks and cooperative banks.

6. Indian legal and regulatory framework

6.1 Provisions of the Indian Penal Code

- **Section 378, Theft:** Theft occurs when someone takes something that is movable without the owner's consent with the intention of stealing it.
- **Section 415:** Deception Cheating: Fraud is the deliberate deception of another person to get them to do something or not do something that they otherwise wouldn't. This act or omission must cause harm to someone's body, mind, reputation, or property, or it must be likely to do so.
- **Section 472:** Producing or Having a Fake Seal, etc. A life sentence or a maximum seven-year prison sentence, along with a possible fine, is imposed on anyone who makes or fakes a seal, plate, or other impression-producing tool with the intent to use it in a forgery covered by Section 467 of this Code, or who knowingly keeps such a counterfeit tool.
- **Section 464:** Creating a False Document, when someone fabricates an electronic file or record, they are initially charged with: (a) Prepare, sign, stamp, or complete a document or portion of a document. (b) Generates an electronic document or a portion of it. (c) Enhances any electronic document with an electronic signature.

6.2 The negotiable instruments act, 1881:

- **Sec 45A-Holder's right to duplicate of lost Bill:** If a bill of swap is lost before it is due, the person holding it may ask the drawer to give him another bill of the same kind, providing the drawer with security if necessary to protect him from anyone should the allegedly lost bill be discovered.
- **Sec 87-Effect of Material:** Effect of Material: Any substantial modification to a negotiable agreement renders it unenforceable against any party involved at the time of the modification who did not consent to it. The only exception is when the modification is made to carry out the parties' original, shared intention when they created the instrument.

6.3 Punishment for fraud

Since the penalty for fraud includes both a fine and a sentence of jail, it cannot be compounded. Technology improvements have led to an increase in online fraud, which is now considered a major criminal offence.

Fraud is punishable under Section 447 of the Companies Act of 2013. Additional elements of the Act are designed to reveal frauds perpetrated by corporate authorities, directors, and/or senior management.

If someone is found guilty of fraud under Section 447, their penalty might range from six months to ten years in prison.

7. Conclusion

Effective internal controls and information analytics can help identify frauds more quickly, which will help banks limit the losses. Extortion hazard management is becoming an increasingly important component of interior review groups. The failure of inner review groups to identify anomalies like shameful credit examinations, dispensing without adhering to the terms of authorisation, failing to establish proper post-disbursement supervision, and hiding information about unauthorised abundance withdrawals is noted in an RBI circular on review and review frameworks in banks.

E-banking is essential for progress since it allows online transactions with a single click and resolves the worldwide issues with traditional banking. Accuracy and efficiency are the cornerstones of the contemporary e-banking system. In the era of e-banking, hitherto underutilised transaction mechanisms including NEFT, RTGS, ECS, and EFT (electronic funds transfer) have gained popularity, facilitating both local and international transactions. E-banking frauds are, in fact, unprecedented and massive on a worldwide scale. Their research is quite difficult. Crimes targeting banking schemes that concentrate on banks, bank accounts, and e-banking from the viewpoint of a computer (e.g., items theft, damages, replacements, or destruction) follow the investigation methods for general property crimes and do not present novel analytical obstacles.

Every transaction is authenticated by the consumer using the same OTP. The OTP expires after it is used. The customer cannot be tricked, even if a malicious person manages to obtain the lone-key password and use it. OTPs can also be sent to users via SMS. The bank server generates a random number and sends it via SMS to the customer's mobile device as an OTP (One Time Password). The online banking software user enters the transaction-specific OTP, which is then sent to the bank's server. The bank confirms the transaction if the OTP matches the one the customer submitted. An attacker cannot alter this OTP, making it useless for abuse.

Banks around the world are using these innovations. In order to translate multidimensional information, such as recurrence, time, and connections, into an intuitive picture, this device offers a visual depiction of information designs and exceptions. The premise is that people are more accustomed to visual data arrangements than numerical ones. This could be helpful in monitoring the evolution of cash, particularly in hostile to-cash washing investigations and borrower preoccupation with reserves; revealing complex systems with many layers and/or a few middlemen; and discovering hidden and/or indirect links. Information that can be spoken to geospatially and appear intelligent includes budgetary transactions, resource data, customer information and contracts, references to locations, names, and addresses.

Digital financial fraud is widespread and constantly growing. To avoid hacking and financial loss, the general public needs to be taught how to utilise digital banking properly and cautiously. Additionally, it is argued that the complaint system is not the best or most user-friendly for the average person. To guarantee safe, transparent, and reliable digital banking in India, a thorough regulatory framework, improved institutional capacity, increased consumer awareness, and ongoing technology innovation are crucial.

Conflict of Interest

There is no conflict of interest disclosed by the author.

Reference

1. Kapoor A. Digital payments and the rise of UPI in India. J Payments Strategy Syst. 2020;14(3):215-228.
2. Thakur S. Electronic banking fraud in India: effects and controls. Int J Sci Res. 2019;8(10):823-829.
3. Sharma R. Digital banking and IT-enabled financial services: a conceptual overview. J Bank Finance Stud. 2021;9(2):45-52.
4. Bhargavi C, Sravanthi M. Significant role of digital technology in detecting banking frauds in India. Int J Adv Multidiscip Res Stud. 2023;3(3):1124-1127.
5. Aljudaibi SA, Amuda YJ. Legal framework governing consumers' protection in digital banking in Saudi Arabia. J Infrastruct Policy Dev. 2024;8(8):1-18.
6. Kirti K. Analytical study of e-banking frauds and its impact on Indian economy. Int J Legal Res Analys. 2023;2(7):5-20.
7. Rysman M, Wright J. The economics of payment cards. Rev Netw Econ. 2015;14(1):57-79.
8. Dospinescu O, Dospinescu N, Agheorghiesei DT. Fintech services and factors determining the expected benefits of users: evidence in Romania for millennials and generation Z. E&M Econ Manag. 2021;24(2):101-118.
9. Rysman M, Wright J. The economics of payment cards. Rev Netw Econ. 2014;13(3):303-353.
10. Basu S. Security and privacy concerns in e-banking: an empirical study. Int J Bank Finance. 2008;5(1):1-22.
11. Ahmad I, Khan S, Iqbal S. Guardians of the vault: unmasking online threats and fortifying e-banking security, a systematic review. J Financ Crime. 2024;1:1-18.
12. Ali MA, *et al*. E-banking fraud detection: a short review. Int J Innov Creat Change. 2019;6(8):67-87.
13. Kothari CR. Research methodology: methods and techniques. 2nd rev ed. New Delhi: New Age International Publishers; 2004.
14. Johri N. E-banking frauds and safety solutions: analysis. Indian J Integr Res Law. 2021;2(6):1-12.
15. Vanini P, Rossi S, Zvizdic E, *et al*. Online payment fraud: from anomaly detection to risk management. Financ Innov. 2023;9:66:1-25.
16. Gupta R, Gupta S, Ajekwe CC. Electronic banking frauds: the case of India. Theory Pract Illegit Finance. 2023;1:166-183.