International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 02, 2024
www.ijirse.com
ISSN: 2454-9665

Virtual Crime: A Big Threat to Urban Cooperative Banking in India

Garima Dahiya,

*Research Scholar (Pursuing **Ph. D.** in Deptt. of Management*
Studies from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonipat)
under the guidance/ supervision of Prof. Rajbir Singh

Abstract

Urban Cooperative Bank incorporates the notion of "Financial Inclusion" into its framework. Urban cooperative banks operate primarily in rural and semi-urban areas. These play a crucial role in the banking sector and contribute to national progress. A cooperative is a voluntary association of individuals who share economic, social, and cultural goals through a democratically governed enterprise. Financial inclusion efforts will empower individuals and create business opportunities for financial market participants. Cooperative banking is crucial for mainstreaming this section of the economy, as evidenced by experiences in developing countries. In order to keep pace with technological advancements, cooperative banks also started using IT for day-to-day transactions which made them more susceptible to cyber attacks. This paper explores the aspects and trends of such attacks. Moreover, the paper also highlights the areas which make these banks vulnerable to virtual fraud more than other commercial banks. Finally, the study concludes with the measures which should be adopted to make UCBs safe and resilient for its customer.

Introduction

Urban cooperative banks play a key role in the country's financial system. Despite the sector's continuous 3-4% share of the entire banking market, its importance should not be overlooked. In terms of pure numbers, UCBs outweigh commercial banks by approximately 1,500. Their outreach extends across a broad range of society, serving ordinary residents, marginalised groups, small and medium-sized businesses, agriculture, and related activities. UCBs have historically played an important role in expanding financial inclusion, long before commercial banks became involved. Their contribution to financial inclusion is firmly interwoven in their path, as they seek out to previously neglected and underrepresented segments. This pioneering position has firmly established UCBs as advocates for diversity and community welfare.

The Indian Cooperative Movement has a long history, having its roots in south India. Kanchipuram registered the first Urban Cooperative Credit Society on October 2, 19041. Since then, India's cooperative movement has generated some spectacular success stories, which have had a profound impact on various sectors of the economy. Many urban banks began as cooperative credit associations before becoming banks. When a cooperative society becomes a cooperative bank, it faces many key obstacles inherent in the banking industry. Banks have the ability to raise large amounts of uncollateralized deposits, which are their principal source of funding for lending and investing operations. As a result, co-operative banks are outliers in the cooperative sector, with resources for

ISSN: 2454-9665

lending and investment coming from the public rather than its members. This increased leverage and maturity gap between assets and liabilities can only be sustained with the continuous trust of depositors. As a result, bank governance procedures and practices must prioritise the protection of depositors' interests and the maintenance of confidence.

Some may claim that UCBs are not systemically relevant due to their size and turnover. However, when we consider the interconnectedness that exists throughout the full spectrum of financial firms, it is clear that any weak link has the potential to damage public trust and confidence. In today's highly interconnected financial ecosystem, even seemingly little disruptions can have far-reaching consequences. The fall of a Gujarat-based UCB in 2001, followed by that of a Mumbai-based UCB in 2019, demonstrates the contagion risks presented by even relatively small banks. As such, it becomes necessary for the UCBs to continue being watchful and proactive in maintaining the sector's resilience. Protecting the individual entities is not the only reason for adhering to strict governance guidelines, effective risk control procedures, and proactive supervision. Rather, it is intricately linked to the overarching objective of maintaining public confidence in the soundness of country’s financial system. Three key challenges confronting the sector are Governance and professionalism, Adoption and upscaling of technology, Capacity building in various operational areas with a view to enhancing efficiency.

However, the focus of this paper remains on the issue of adoption and upscaling of technology given the UCBs walk on digital path is in jeopardy due to lingering danger of ever increasing and ever evolving cybercrime. In today's quickly changing financial market, harnessing technology has become a strategic imperative for maintaining competitiveness. Adopting innovative solutions can lead to increased efficiency, better customer experiences, and more simplified processes. By being proactive in implementing technology, UCBs may position themselves as modern and forward-thinking institutions, garnering a larger customer base and remaining relevant in the digital age. UCBs will continue to capitalise on member loyalty. However, this can fade with time, demographic shifts, and, of course, competition. As UCBs incorporate technology into their operations, they must be acutely aware of the potential cyber dangers that accompany it. The digital arena introduces new vulnerabilities, making strong cybersecurity measures non-negotiable. To effectively reduce cyber threats, invest in cybersecurity solutions, undertake frequent risk assessments, and execute extensive staff training programmes. UCBs should also increase their operational resilience by reducing downtime. They should have appropriate business continuity and catastrophe recovery policies in place that have been thoroughly tested.

Cooperative Movement in India

The Indian cooperative movement, like its counterparts in other countries throughout the world, has been mostly a product of misery. Based on the proposals of Sir Frederick Nicholson (1899) and Sir Edward Law (1901), the Cooperative Credit organisations Act was approved in 1904, clearing the way for the founding of cooperative credit organisations in both rural and urban parts of the country. The Cooperative Societies Act of 1912 recognised the formation of non-credit societies as well as central cooperative organizations/federations. Even after India gained independence in 1947, the state continued to support the cooperative movement. Independent India accepted the concept of planned economy, and cooperative organisations were given a prominent role.

The Government's attitude towards the cooperative movement was influenced by the Saraiya Committee's recommendations, which indicated that cooperative societies play a key role in democratising economic planning.

Various expert groups that have since reviewed the topic of rural lending have unanimously concluded that, in the Indian context, there is no structurally appropriate alternative to village cooperatives. The Rural Credit Survey Committee (1954), the first comprehensive inquiry into rural credit problems, summed up its findings in the celebrated dictum "cooperation has failed, but cooperation must succeed" after a thorough examination of all issues, including the social ethos of rural society.

Since the 1950s, cooperatives in India have made significant development in numerous sectors of the Indian economy, including banking. The cooperative bank is an essential component of the Indian financial system, as evidenced by the role allocated to it, the expectations the cooperative is expected to meet, its size, and the number of offices it operates. Though the cooperative movement began in the West, the significance of such banks in India is rarely matched anywhere else in the world.

Cooperative Banks

Cooperative banks in India are governed by the Cooperative Societies Act. The RBI also regulates cooperative banks. They are governed by the Banking Regulations Act 1949 and the Banking Laws (Cooperative Societies) Act of 1965. The cooperative banking sector in India plays a significant role in expanding institutional credit's geographical and social reach. In fact, the cooperative banking industry has grown as an important component of the country's financial system, with branches reaching even the most rural areas. The cooperative movement in India is one of the largest in the world.

The structure of India's cooperative banking sector is complex. Different parts of the cooperative banking business provide loans to distinct groups of individuals based on their location and tenor. While urban cooperative banks have a one-tier organisation, rural cooperative banks have two unique sets of institutions that provide short-term and long-term lending. In terms of short-term loan co-operatives, there are around 97,224 Primary Agricultural loan Societies (PACS) that deal directly with individual borrowers. District Central Co-operative Banks (DCCBs) serve as a link between primary societies and State Cooperative Banks. State cooperative banks, often known as Apex Banks, are at the pinnacle of a state's credit hierarchy. It serves as a top-level supervisory body and coordinates the spread of the cooperative movement. It serves as the final link in the chain connecting individual members of small distributed primary societies to the broader money market, as well as the Reserve Bank of India and the country's central banking authority.

Virtual crime in Banks

One of the major challenges that researchers confront is agreeing on a definition of cybercrime, as they each approach the issue from their own unique perspective based on their best knowledge and expertise. As a result, in order to describe cybercrime, it is necessary to explain the terms cyber and crime. The term "cyber" is intended to be a catch-all for anything linked to virtual reality, the internet, information technology, and computers, whereas "crime" refers to anything illegal. As a result, cybercrime can be defined simply as any offence involving computers, the internet, or virtual reality.

Cybercrimes have been classified into four categories by Wall. They are cyber-deceptions, cyber-violence, cyber-pornography and cyber-trespass (Wall, 2001). The frauds in e-banking sector are covered under cyber-deception

which is defined as fraud that involves the use of computers to obtain personal or financial information from unsuspecting victims to gain access to funds or assets and includes theft, credit card fraud, and intellectual property violations. Mostly frauds are committed because of two goals, one, to gain access to the user's account and steal his personal information and transfer funds from one account to another. Second is to undermine the image of the bank and block the bank server because so that the customer is unable to access his account (Raghavan, A. R. & Parthiban, L., 2015).

As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 1,59,761; 2,46,514 and 2,90,445 cyber security incidents pertaining to digital banking were reported during 2018, 2019 and 2020, respectively ("Over 2.9 lakh cyber security incidents related to digital banking reported in 2020",2021). As per PwC's Global Economic Crime Survey, cybercrime has jumped to the second position as the most reported economic crime and financial institutions are prime targets (Rivera K. and Rohn C., 2020).

Financial frauds accounted for 75% of cyber-crime in India from Jan 2020 to Jun 2023, with nearly 50 per cent cases related to UPI and internet banking, according to a study by an IIT Kanpur-incubated start-up. RBI has defined bank fraud has as, 'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank' (Reserve Bank of India, 1997).

Co-operative Banks (dark side of the moon)

While technology has provided company continuity, it has also opened a Pandora's Box of sorts. At one end, it has resulted in speedier adoption of digital banking and other technology; at the other, it has rendered us more exposed to cyber-attacks and online fraud. As India embraces internet banking, its citizens' digital literacy has not kept up. According to a research provided by Subex, a Bengaluru-based analytics firm, for April, May, and June 2019, India faced the most cyber-attacks in the world, while the United States was the most cyber-targeted nation in 2019. In fact, an assessment of the main cyber attacks on India's computer networks since 2010 reveals that the banking industry has been struck the most by unauthorised access and data breaches. India ranks fourth in the world for cyber attacks, a trend that has only grown in recent years.

Most UCBs in the country are susceptible as they try to become digital to stay up with the quickly changing landscape, but have not been able to sufficiently safeguard digital infrastructure. Pointing out that most UCBs are ill-prepared to deal with cyber crooks, D Janakiram, Director of Apex Banking Technology Research Organisation, Institute of Development and Research in Banking Technology (IDRBT) said in many cases the bank servers are just connected to the internet and most of the ports are left open, making these banks vulnerable ("Co-operative Banks In India Walk Digital Path, But Vulnerable To Cyber Attacks," 2022).

All cooperative banks are using a cheap software that is made in Mumbai and is priced at Rs 12 lakh whereas nationalised and leading private banks have gone in for an impregnable automated security banking software developed by Infosys and TCS that costs around Rs 6.70 crore ("Hackersprey on Coop Banks with cheap security software: Police," 2022).Banks' use of information technology has increased significantly, and it is now a key

component of their operational strategies. The number, frequency, and severity of cyber incidents/attacks have increased dramatically in recent years, particularly in the financial industry, which includes banks. There is an urgent need for UCBs to implement strong cyber security/resilience architecture to assure the ongoing protection of their assets. As a result, it has become critical to improve the security of UCBs against cyber threats by upgrading present defences for tackling cyber risks.

Recent cases of attacks on cooperative banks in India:

Cyber attack on Cosmos Bank, Pune: In a massive cyber attack that shocked the financial ecosystem of India, the Pune-headquartered Cosmos Bank, one of the oldest cooperative banks in the country, lost a whopping Rs 94 crore to cybercriminals in just three days in August 2018.A probe by the city police revealed it was a "malware attack" in which several cloned debit cards of Cosmos Bank were used for thousands of ATM transactions from India and 28 other countries in seven hours on August 11, 2018.

While around Rs 78 crore was withdrawn in more than 12,000 ATM transactions outside India, another 2,800 transactions of Rs 2.5 crore were made at different places within India. Further, on August 13, 2018, Rs 13.92 crore was transferred to a Hong Kong-based entity using the Society for Worldwide Interbank Telecommunications (SWIFT) facility. The transactions outside India were done through Visa cards, and those in India through RuPay cards, a probe found ("Pune Crime Files: Cyber attack on Cosmos Bank that funnelled Rs 94 crore in just 3 days," 2024).

Kolhapur Urban Cooperative Bank, Maharashtra: Cooperative banks are turning out to be the weak link in the cybersecurity framework of the financial system. Another Maharashtra-based urban cooperative bank's main server was hacked remotely and its account with a large private bank was cleaned of Rs 68 lakh in April, 2019.

According to banking sources, the fraudsters, after gaining access to the cooperative bank's systems, used electronic transfer systems, including Immediate Payment System and National Electronic Fund Transfer for sending funds to a benami account. The money was understood to have been transferred in 34 accounts in different states ("Another Maharashtra cooperative bank's server hacked, Rs 68 lakh siphoned off," 2019).

Sharmrao Vitthal Cooperative Bank, Thane: The Sharmrao Vitthal Co-operative (SVC) Bank has registered a case of criminal breach of trust and data leak against two current and one former employees. The bank, which has 198 branches around the country, has alleged that the accused stole data of 447 customers and some officials, causing it losses of 29 crore. The Srinagar police in Thane are investigating the case ("Breach of data led to loss of Rs 29 cr, says top co-op bank," 2019).

Kangra Cooperative Bank, Himachal Pradesh: In a stunning case, cyber frauds have allegedly siphoned off Rs 7.79 crore from the Kangra Co-operative Bank's current account maintained by Reserve Bank of India (RBI), according to the police complaint filed by the bank. The fraud took place in three separate transactions on as many consecutive days, the first being on April 19, 2023.

They have not been able to ascertain the person who has withdrawn the amount through fraudulent transactions, even though Kangra Bank officials said they have been able to identify accounts in which the money has been transferred ("Kangra Cooperative Banks account with RBI loses Rs7.79croreincyberfraudcase," 2023).

AP Mahesh Cooperative Bank, Hyderabad: RBI imposed fine of Rs 65 lakh on the AP Mahesh Cooperative Urban Bank ltd for failing to provide cyber infrastructure and efficient firewalls as a result of which a loss to the tune of Rs 12.48 crore was caused due to a fraud committed by Nigerian in January 2022.

The act was carried out by the fraudster by sending the employees of the bank a series of phishing emails. Upon opening the emails, system was compromised, provided the fraudster full access to the bank's network ("RBI slaps Rs 65 lakh fine on Mahesh Bank failing to boost cyber security," 2023).

Chembur Nagarik Sahakari Bank: This Bank, which has only 10 branches and serves customers located in the Chembur sub-urb of Mumbai has reported hackers trying to attack its servers, Tamil Nadu State Cooperative Bank fraud of Rs 2.5 crore in 2023, hacking attempt of Rs 145 crore on UP Cooperative Bank. This appears to be only the tip of the iceberg, since many occurrences go unreported, either because banks are unaware of a data breach or are concerned about reputational damage, according to industry players.

RBI and NABARD Data

The Department of Financial Services released frightening numbers on Monday (July 31) regarding fraudulent actions in the cooperative banking industry. According to their data, cooperative banks across the country recorded a startling 4,135 frauds over the last five years, totalling Rs 10,856.7 crore. The data, obtained from the Reserve Bank of India (RBI) and the National Bank for Agriculture and Rural Development (NABARD), emphasises the major issue of fraud that has afflicted the cooperative banking.

As of June 14, 2023, the country's total number of cooperative banks is 1,886, with 1,500 urban cooperative banks and 386 rural cooperative banks. These cooperative institutions play an important role in meeting the financial requirements of many communities around the country.

The data supplied by the Department of Financial Services provides a breakdown of the scams recorded during each fiscal year, giving a worrying picture of the rising problem:

Financial Year	Number of Frauds	Amount involved in Frauds (in crore)
2018-19	**1,285**	**703.75**
2019-20	**719**	**6,839.18**
2020-21	**438**	**1,985.79**
2021-22	**729**	**536.59**
2022-23	**964**	**791.4**
Total:	**4,135**	**10,856.70**

Source: RBI and NABARD

What makes Co-operative Banks more Vulnerable?

- **Ill- equipped:** Even the majority of UCBs are woefully unprepared to deal with cybercriminals. In many situations, bank servers are only connected to the Internet, with most ports left open, making them more

vulnerable. The situation is significantly worse when it comes to rural cooperative banks. In Hindi, the scenario appears to be an open invitation by these banks to cybercriminals. Cybercrime police of the city identified 53 urban cooperative banks that are yet to update their cybersecurity software, increasing their susceptibility to a cyberattack and causing loss to thousands of customers ("Public money vulnerable in 53banks having poor cybersecurity," 2023).

- **No designated Chief Information Security Officer:** The majority of these cooperative banks, including the large UCBs, do not have appointed CISOs to establish their cybersecurity strategy and roadmap. Instead, IT administrators frequently function as CISOs, and there is a complete absence of competent labour resources. As a result, there is a broad lack of understanding of the rapidly changing danger situation. Instead, there is excessive reliance on suppliers or third-party solution providers.
- **Sophisticated attacks:** For the majority of UCB IT managers, cybersecurity begins and stops with anti-virus. Things may be much more rudimentary in rural cooperative banks. Today's cyberattacks are far more sophisticated than viral ones. Unfortunately for individuals serving as cybersecurity custodians for these cooperative banks, the emergence of ransomware assaults, malware attacks, RAT (Remote Access Trojan) attacks, advanced persistent threat (APT) attacks, and zero-day attacks, among others, would sound like Greek and Hebrew.
- **Budget constraint:** With budget constraints, these banks frequently strive to secure themselves with low-cost solutions such as anti-virus. Though this may have worked in an ideal world, in today's real-world competitive environment, all cooperative banks require advanced protection tools such as Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions.
- **Insider threat:** Another major source of concern for cooperative banks is the threat from insiders and unhappy staff. During the pandemic, bank staff asked hackers to recover money from frozen accounts. The only option is for cooperative banks to implement appropriate Data Loss Prevention (DLP) systems, which allow banks to govern the data that users can access and transmit.
- **Non-reporting:** As early as December 2019, the RBI mandated cybersecurity in banks and established a standard for security installation and attack reporting. However, fear of reputational harm sometimes inhibits small cooperative banks from disclosing cyberattacks to the appropriate authorities. In fact, there are several examples where cooperative banks fall victim to cyberattacks and lose money and data, but such incidents are seldom made public due to a lack of a solid legislative framework that requires such disclosures.
- **Non-compliance:** Cooperative banks are often found non-complying with the RBI guidelines and directives for maintaining cyber hygiene. The Reserve Bank imposed a monetary penalty of ₹4.00 lakh on Jijamata Mahila Sahakari Bank Limited, Pune for non-compliance with RBI directions on 'Reserve Bank of India - Know Your Customer (KYC) Direction, 2016' and 'Frauds in UCBs: Changes in Monitoring and Reporting Mechanism'. The RBI said the Jijamata Mahila Sahakari Bank had not conducted periodic review of risk categorisation of accounts; and had not reported a fraud to RBI within the stipulated timeline ("RBI imposes monetary penalty on four co-operative banks. Details here," 2023).

ISSN: 2454-9665

Suggestive Measures:

At times supervisory medicines may taste bitter. However, prevention is always better than cure. With the best interests of the sector in mind and to safeguard the interests of depositors while fostering a resilient, sound, and stable financial system that contribute to the nation's development a few measures should be taken by UCBs:

- **Need for a Board approved Cyber Security Policy:** All UCBs should immediately implement a Cyber Security policy, properly approved by their Board/Administrator, that provides a structure and strategy for detecting cyber threats based on the complexity of the company and acceptable levels of risk. Once the Board has completed the policy development process, a confirmation email must be provided to the Department of Co-operative Bank Supervision within three months of the circular's date. It must be assured that the cyber security strategy addresses the following broad issues, taking into account the amount of technology adoption and digital products provided to customers.
- **Cyber Security Policy to be distinct from the IT policy of the UCB:** The Cyber Security Policy should be unique from the UCB's IT/IS policy in order to highlight the risks associated with cyber threats as well as the steps to address/reduce these risks. While identifying and assessing inherent risks, UCBs should consider the technologies1 used, distribution channels2, digital products3 offered, internal4 and external5 threats, and classify each risk as Low, Medium, High, or Very High.
- **IT Architecture/Framework should be security compliant:** The IT architecture/framework, which comprises network, server, database, and application, end user systems, and so on, should always consider security measures, and it should be evaluated by the Board or its IT Sub-committee on a regular basis. To accomplish this, UCBs may take the following steps:

i. Identify weak/vulnerable areas in IT systems and processes.
ii. Allow restricted access to networks, databases, and applications through well-defined processes and approvals.
iii. Assess the cost of impact in case of breaches/failures.
iv. Implement a suitable Cyber Security System to address these areas.
v. Clearly specify and document responsibility for each of the above steps.

- **Cyber Crisis Management Plan:** Because cyber risk differs from many other hazards, typical BCP/DR (Business Continuity Plan/Disaster Recovery) arrangements may be insufficient and should be reviewed in light of the nature of cyber risk. CERT-In (Computer Emergency Response Team - India, a Government entity) is a Government of India organisation that has taken significant steps to strengthen cyber security by providing proactive/reactive services and guidelines, threat intelligence, and assessments of various agencies' preparedness in various sectors, including finance. CERT-In has also released the National Cyber Crisis Management Plan and Cyber Security Assessment Framework. UCBs may use the CERT-In/NCIIPC/RBI/IDRBT recommendations as reference material for their instruction.

  UCBs must rapidly detect any cyber incursions (unauthorised entry) in order to respond, recover, and mitigate the consequences of cyber-attacks. Among other things, UCBs, especially those offering services such as internet banking, mobile banking, mobile wallet, RTGS/NEFT/IMPS, SWIFT, debit cards, credit cards, etc., should take the necessary detective and corrective measures/steps to address various types of cyber threats6

viz. Denial of Service (DoS), Distributed Denial of Services (DDoS), ransomware/ cryptoware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing etc.

- **Organisational Arrangements:** UCBs should evaluate organisational arrangements to ensure that security risks are brought to the attention of appropriate/concerned officials, allowing for prompt action.
- **Cyber Security awareness among Top Management/Board/other concerned parties:** To manage cyber risk, the entire organisation must commit to creating a cyber-safe environment. This will necessitate a high degree of awareness/familiarization among employees at all levels, including the Board and Top Management. UCBs should actively raise awareness of their cyber security objectives among their customers, vendors, service providers, and other stakeholders. Customers, employees, vendors, service providers, and others are more aware of the potential effects of cyber-attacks, which helps UCBs plan for cyber security threats.
- **Ensuring protection of customer information:** UCBs, as owners of customer sensitive data, should take appropriate steps to ensure its confidentiality, integrity, and availability, regardless of whether the data is stored in transit within themselves or with third-party vendors; the confidentiality of such custodial information should not be jeopardised in any situation. To achieve this, UCBs must implement appropriate systems and processes throughout the data/information lifecycle. UCBs may educate and raise customer knowledge about cyber security threats.
- **Supervisory reporting framework:** UCBs should immediately report any anomalous cyber security incidents (whether successful or unsuccessful) to the Department of Co-operative Bank Supervision by email, providing complete details of the incident. In the event that there are no cyber security events, a 'NIL' report will be filed quarterly.

Conclusion

The synergistic benefits of the merger of the cooperative movement and banking, as outlined in the UCB framework, can only be realised with strong governance and skilled management. When governed by strong governance, UCBs can promote financial inclusion, benefiting both the community and the institution. The measures we are making today to secure the UCB sector will not only protect these institutions, but will also serve as a barrier against possible attacks and vulnerabilities to the financial system. By creating a culture of prudence and foresight, we can ensure that the UCBs continue to grow as pillars of trust, contributing to our country's strong and secure financial future.

References

- Another Maharashtra cooperative bank's server hacked, Rs 68 lakh siphoned off (2019, May 9). *The Times of India.*
- Breach of data led to loss of Rs 29 cr, says top co-op bank (2019, Dec 17). *Mumbai Mirror.*
- Co-operative Banks In India Walk Digital Path, But Vulnerable To Cyber Attacks (2022, April, 20). *The Times of India.*
- Hackers prey on Coop Banks with cheap security software: Police (2022, May 6). *Deccan Chronicle.*

ISSN: 2454-9665

- Kangra Cooperative Banks account with RBI loses Rs7.79 crore in cyber fraud case (2023, May 24). *Economic Times.*
- Over 2.9 lakh cyber security incidents related to digital banking reported in 2020 (2021, Feb 4). *Hindustan Times.*
- Public money vulnerable in 53 banks having poor cyber security (2023, July 3). *Deccan Chronicle*.
- Pune Crime Files: Cyber attack on Cosmos Bank that funnelled Rs 94 crore in just 3 days (2024, Feb 19). *Indian Express*.
- Raghavan, A. R. & Parthiban, L. (2015). *Effect of Cyber Crime on Bank's Finances*, Vol. 2(2).
- RBI imposes monetary penalty on four co-operative banks. Details here (2023, Dec 4). *Livemint.*
- RBI slaps Rs 65 lakh fine on Mahesh Bank failing to boost cyber security (2023, July 2). *Indian Express*.
- Reserve Bank of India (1997). *Report of the Study Group on Large Value Bank Frauds*.
- Rivera, K. and Rohn, C. (2021). Fighting fraud: A never-ending battle. *PwC's Global Economic Crime and Fraud Survey 2020.*
- Wall. (2001*). Cybercrimes and the Internet*.