

AN ANALYTICAL STUDY OF A CASHLESS CRUSADE VS CYBERSECURITY

Mrs. Gurpreet Kaur Ghattode, Dr. Hariom J. Puniyani

Research Scholar, Hislop College, Nagpur,
RashtrasantTukadoji Maharaj Nagpur University, Nagpur India
gurpreetghattode@gmail.com

Professor & Head, Department of Commerce, Hislop College, Nagpur,
RashtrasantTukadoji Maharaj Nagpur University, Nagpur India
hariompuniyani80@gmail.com

Abstract

"Cashless Transactions" is an intensely used term of this era, every person in society is using this term and getting an advantage from it by using various digital payment methods. Today, we indeed depend upon technology-savvy procedures to fulfill any of our tasks and duties, but the question arises: Are they safe? In 2016, the government of India, with a vision to make this country digitalized, took a revolutionary move through the introduction of the 'Digital India Campaign' to reduce the unnecessary lengthy procedures, documentation, bankruptcy, corruption, and bureaucracy. The government made an effective move through overnight demonetization, which put everybody in a complex situation. There were many difficulties in handling paper currency, currency exchange, banking procedures, limitations on withdrawals, etc. From then to now, banks have played a crucial role as facilitators between governance and the public. It also pushed people towards cashless transactions, but it took time to adopt such a shift.

While moving toward digitalization, the major drawbacks are the lack of digital public infrastructure and digital literacy. So, to make people digitally literate, the government started campaigns and awareness programs. Despite that, most people are unaware of digital/cashless gadgets, procedures, apps, etc. Whereas the people who know about it need to use it very carefully as there is a lot of risk in doing digital transitions. According to the latest data, the rate of cybercrimes and financial frauds is increasing rapidly. The government has set up the 'National Cyber Security Agency' (NCSA) to deal with cybercrimes and using different fraud detection techniques through AI. Through this paper, efforts are made to know the volume of people using cashless transactions, the current status of cybercrime in the country, various mechanisms set up by the government to deal with cybercrimes, and the role of AI in it.

Keywords: Cashless, Cybercrimes, AI, Cybersecurity, Digitalization, Fraud.

INTRODUCTION

A new era of revolution started in India in the year 2016 when we experienced demonetization and digitalization and started accomplishing the aim of a cashless economy. From 2016 to 2025, the Indian economy has seen a leap toward growth and advancement. A remarkable change has been seen in every sector, whether it is commercial, technological, political, etc. The Government of India is trying to bring digitalization to every sector. A lot of stress has been given to the financial sector by introducing the concept of a cashless economy in which the maximum number of transactions are done with the help of electronic/digital gadgets. With the help of E-Governance, the Government is trying to connect with the public directly by reforming governance through technology, which results in more transparency, reduction in corruption, reduction in red-tapism, reduction in unnecessary documentation, etc. But all this is impossible without technological advancement, so the need for advancement in the IT sector is aroused, for which the government started many new projects and made 'IT for jobs'. Despite this, the Government has set eight more pillars under the 'Digital India Initiative', which needs digital public infrastructure with its high cost of implementation. To achieve this goal, banks are playing the major role of facilitator of financial transactions through digital banking instruments and e-banking. With the help of banks, financial inclusion provides lots of benefits to the administration for the implementation of various schemes and making a sound digital public infrastructure in the country. The ultimate aim is to provide digital infrastructure and internet access in every part of the nation, to spread awareness about online procedures, to spread digital literacy, etc.

At present, we can see the change in our environment, whether it is internal or external, business or personal, everything has changed. It took almost a decade to bring this dynamic change. Now, most people depend upon cashless transactions, the Government has launched UPI app to make transactions easy; it also provides other payment methods like ATM, Micro ATM, NEFT, RTGS, Aadhar-based payment, etc. The acceptance of cashless transactions becomes fruitful as financial inclusion emerges as an effective tool for generating revenue for govt.

With this acceptance, we have accepted risk, too. There is a lot of risk in doing Cashless transactions. The redressal machinery has been set up to deal with cybercrime grievances. The Cybersecurity Cell at the local level, the 'National Cyber Security Agency' (NCSA) at the national level, the National Cybercrime Reporting Portal (online), etc., are set up by the Government. Despite these agencies, fraudsters always have the forefront plan, and the police and the other authorities need to stay ahead of them.

OBJECTIVES

1. To know the volume of People using Cashless transactions.
2. To understand various mechanisms set up by the government to deal with cybercrimes and the role of AI in them.
3. To evaluate the impact of the above mechanisms on cybercrimes.
4. To spread awareness among the people of different ways to deal with cybercrimes.

RESEARCH METHODOLOGY

The author has gathered the data for this research paper through the secondary data collection method. The secondary data has been collected through government websites, news articles, newspapers, periodicals, research papers, etc.

LITERATURE REVIEW

The Ministry of Home Affairs has set up machinery to deal with cybercrimes at different levels, not only this there are so many campaigns to spread awareness among the citizens about various cybercrimes and financial frauds. Many researchers have done research on cybercrimes, financial fraud, Digitalization, and cashless transactions. As cybercrimes have become a crucial topic of concern, newspapers, e-papers, and periodicals have also published many articles, some of which are listed here:

Newspaper Articles: Times of India, Hindustan Times, The Hindu, Business Standards, Indian Express.

Official Websites: Cyber Crime Portal, Ministry of Home Affairs, National Portal of India, National Cybercrime Reporting Portal

Research Articles: National Strategy for Financial Inclusion by RBI.

Dr. Poonam Wani and Dr. Veena P Bhosale Published an article on 'Cybersecurity and Fraud Prevention in India's Financial Sector: A Comprehensive Review' examines recent cyber security incidents and the various sorts of cyber threats that different sectors have encountered.

I: A Cashless Crusade and its New Reforms:

With a vision to make the economy cashless, the government of India started a regime in which demonetization took a significant place. After demonetization the need for cashless transactions arose, just before demonetization, the UPI app was introduced for seamless Online transactions. It is not easy to achieve this goal of a cashless economy as it requires a sound digital infrastructure, availability of digital gadgets, digital literacy, and Internet access throughout the nation. To fulfil all these requirements More stress is placed on the 'Digital India' and 'Make in India' initiatives. It has given a boost to the IT sector as well as electronic manufacturing, but in the initial stage, it was not easy to shift towards cashless transactions as people indulged in the habit of using physical cash. Slowly the Indian economy is transforming towards cashless, then we experienced the breakthrough of pandemic covid 19 pandemic due to which most of the population started using cashless transactions as the use of physical currency may cause virus. This has been shown in the swift change in the Indian economy, this will also help the government through financial inclusion.

Now we can see the change, that most of the people in our surroundings depend upon digital gadgets for making cashless transactions, there are so many apps that are Providing us with online payment facilities. Before we used RTGS and NEFT to fund transfers but now we have so many other ways of making online transfers e.g. UPI apps, Debit Cards, Credit Card, Aadhar-based payment systems, money orders and book mail by Post office, mobile wallets, etc. The advancement in these modes of payment shows the dependency of the citizens towards cashless transactions. The volume of cashless transactions has increased from Rs. 1962 lakh crore to Rs. 3659 lakh crore at a CAGR (Compounded annual growth rate) of 11% additionally in the last five months from (April to August) of the current F.Y 2024- 25 the total transactions volume has raised to Rs 1669 lakh crore. In digital transactions, the UPI has shown remarkable success as UPI transactions have risen from 92 Crore, in the F.Y 2017- 18 to 13,016 Crores in the F.Y 2023-24 at a CAGR of 129%, according to current data of the last 5 months from April to August of current F.Y 24-25 the transaction volume has reached 7,062 Crore. Whether it is business, employment, profession, or any other field we can see that most of the funds were managed through online modes, which leads to financial inclusion which is one of the sustainable goals for the Economic growth of the nation

II: Types of Cybercrimes and Financial Frauds:

Several cybercrimes are happening around us, some of them we're aware of but some of them are not known to us. On average there are 100 to 150 cybercrimes happening in an individual city daily. Indian banks reported over 23,000 cybercrime incidents in 2023, Near about one million financial fraud crimes were registered in the year 2023. From the year 2021 to 2024 there is a 900% jump in cybercrimes in India.

There are so many types of cybercrimes and financial frauds. Some common examples are fraud through fake calls, SMS, WhatsApp messages, website Links, Fake Facebook IDs, Identity theft, Online shopping, Cyber extortion, and Fraud through Debit and credit cards.

Some of the Recent Frauds are:

- **Digital Arrest:** In this cybercrime, there is an international racket involved in it. Here someone unsuspecting person calls your phone number, impersonating someone and saying that he's calling from the CBI or ED or any tax authority be income tax department, or the general GST department, they make you believe that you are accused in the case of being part of a conspiracy of defrauding the tax authorities or duping their tax department or there is an ongoing criminal investigation by the CBI or the ED which scares the people and these people who are impersonating as police scare the people by saying that if they do not cooperate with us and tell the details, then they will be arrested. Now that is enough for a common citizen to be scared and cooperate, now once the cooperation happens, they are seeking an Aadhaar card, Bank card details, your phone number, and so on. With bank account details they will scam money out of your bank account. Example: a case in Karnataka involved an 11-crore cybercrime cheating case.

- **AI Voice Cloning:** Here the cyber fraudsters impersonate the voice of the people by calling them and then deceive victims by using this voice through AI. Here the fraudsters send a recorded message of the victim's children's voices, making them speak to someone with having similar voice with the use of AI and threaten the parents by asking them to pay immediately or they will not find their kids. Parents also respond to these fraudsters very quickly as they are afraid of their kids' lives, there have been so many cases happening recently.

- **Website Cloning:** Website cloning is a type of fraud in which the fraudsters clone the website itself, which shows the exact information and everything about the original website, through they convince other people to share their details, which can be misused by the fraudsters. Like this there are many more frauds and the fraudsters are finding more and more ways and techniques to make people fool.

III: Various mechanisms set up by the government to detect cybercrimes with the help of AI:

Cybercrimes and financial fraud are becoming a matter of worry in every part of the Nation. It becomes necessary to make a strengthened mechanism to deal with these culprits. Govt. of India has set various mechanisms as redressal machinery for cybercrimes & financial frauds. Everything starts from our smartphones and also ends on it so we should be aware of whatever we are doing in it. Here are some machines that are trying to detect cybercrime risk and taking action on it:

- The 'National Cyber Security Agency' has launched the 'National Cybercrime Reporting Portal' as a part of 14C to enable the public to report incidents about all types of cyber-crimes.
- A toll-free Helpline number is also provided to the public i.e. **1930**. If one should call this helpline number within a 'Golden Hour', Then there is a 90-100% chance of getting their money back. ('Golden Hour'- Complaint registered within one hour of Crime occurred)
- The Indian Computer Emergency Response Team (CERT-In), A national agency that coordinates cybersecurity efforts and responds to incidents and issues alerts and advisories.
- Cybercrime cells are specialized cells within police departments across India dedicated to investigating and prosecuting cybercrimes.
- Cyber forensic labs are specialized laboratories that provide forensic analysis and support to law enforcement agencies in investigating cybercrimes.

IV: Impact of these mechanisms on cybercrimes and the precautions to be taken:

To report financial fraud 'The Indian Cyber Crime Coordination Center' (14C) under the Ministry of Home Affairs has set up a 'Citizen Financial Cyber Fraud Reporting and Management System'. It is time to strengthen mechanisms dealing with cybercrimes as it is not easy to clutch the grip on fraudsters because they are not working at any particular place, they are performing these tasks from all over the world. It's difficult to trace their location as they are scattered and using fake identities. They are also exploiting our country's digital growth that's why the regulatory framework should be sharper and stricter.

All the above-stated agencies are working their best in putting every effort to clutch the grips of the culprits. Police are also working actively to address any of the complaints they received and taking immediate action. As the citizens were already headed towards cashless Transactions and the growth and advancement of our nation are also at their peak, we cannot lose hope. Whenever the police track any fraudster or stop any kind of Cybercrime, the culprits find another way of doing the crime. It doesn't mean that we stop taking action, many

times it happens that the victims cannot take the step to complain about the cybercrime or they may get too late but if we take quick action against them then we can grab them. Another thing that we can do is not answer or reply to unknown calls, messages, WhatsApp chats, online links, etc. We should always use only authentic apps for payments and always do two-step verification. Never share personal details or bank details with anybody else. Banks always alert us by sending messages that they never ask for our bank account details, despite that people get fooled so easily, we should stop believing in others if we want to protect ourselves. The Government through the Department of Telecommunications has implemented a cybercrime awareness 'Caller Tune campaign' to spread awareness among the citizens. This campaign is scheduled for three months, this Caller tune has been spreading awareness messages at least 8 to 10 times per day with a toll-free helpline number.

CONCLUSION

The inevitable change has been brought to the Indian Economy through Cashless Transactions, here is what the author has concluded from the research in the area of Cashless Transactions, Cybercrimes, Financial frauds, and AI.

As we say 'to win a battle we need to lose something', it seems that accomplishing the Goal of a Cashless or no Cash Economy is not only a win-win game. By heading towards cashless transactions, cybersecurity is a matter of great concern that we cannot avoid. According to data that was published in various newspapers and websites, cybercrimes are increasing day by day.

The Ministry of Home Affairs is taking every possible measure to control these cybercrimes, AI is also playing a major role in detecting cyber cons, Suspecting the risk in financial transactions, Alerting people about the latest incidents, etc. Despite all the precautions, awareness programs, and prompt action, the fraudsters find a way to escape. As per the data examined not only the authorities or cyber cops are responsible for increasing cybercrimes but also people themselves are responsible to some extent. Lack of digital Knowledge, complete information about authentic applications and websites, illiteracy, avoidance of verification, response to every call and link, trust in the Unknown, hasty decisions, greed to earn money using shortcuts, etc are some of the reasons for culprits to make people blockhead and get advantage of it. So does this concluded that the administration and the general public have to put their efforts parallelly to avoid the risk. By following such measures, we can think of a sustainable cashless economy.

REFERENCES

- [1] <https://timesofindia.indiatimes.com/city/gurgaon/your-call-to-helpline-in-golden-hour-is-key-to-get-money-back-from-cyber-cons/articleshow/108925847.cms>
- [2] Indian banks reported over 23,000 cyber security incidents in 2023. Article of cnbctv18, <https://www.cnbctv18.com/technology/indian-banks-reported-over-23000-cybersecurity-incidents-in-2023-government-to-parliament-19526257.htm>
- [3] India saw 129 cybercrimes per lakh population in 2023. Article from Times Of India. <https://timesofindia.indiatimes.com/india/india-saw-129-cybercrimes-per-lakh-population-in-2023/articleshow/106524847.cms>
- [4] https://www.business-standard.com/india-news/around-1-1-million-financial-fraud-cases-registered-in-2023-shows-data-124020601528_1.html
- [5] Cyber frauds jump 900% in four years. Article From Indian Express, <https://indianexpress.com/article/india/cybercrime-sharp-rise-complaints-2024-govt-data-9816845/>
- [6] Cyber frauds in vacant transactions surges in FY 24, <https://www.thehindu.com/data/cyber-fraud-in-banking-transactions-surges-in-fy24-data/article68813626.ece>
- [7] Cyber Security for a Safer Financial System (Keynote address by Shri M K Jain, Deputy Governor, Reserve Bank of India at 'Cyber Security Exercise for Banking Sector' an international event under India's G 20 Presidency on June 5, 2023, in Mumbai)
- [8] Wani, Dr. P. and Bhosale, Dr. V. P. (May 2024) 'Cybersecurity and Fraud Prevention in India's Financial Sector: A Comprehensive Review' International Journal of creative research thoughts (IJCRT)12(5) ISSN: 2320-2882 [IJCRT%20Fin%20inclusion%20&%20cyber%20Security.pdf](https://www.ijcrt.com/Fin%20inclusion%20&%20cyber%20Security.pdf)
- [9] [CYBERSECURITYFINANCIALSYSTEM2D39A8754117488EB7A1550711E4B0A4.pdf](https://www.ijcrt.com/CYBERSECURITYFINANCIALSYSTEM2D39A8754117488EB7A1550711E4B0A4.pdf)
- [10] <https://fiaglobal.com/ai-in-financial-inclusion/>
- [11] Brochures from the Ministry of Home Affairs, India

Official Websites:

- [1] Cyber Crime Portal: <https://cybercrime.gov.in>
- [2] Ministry of Home Affairs: <https://cybervolunteer.mha.gov.in>
- [3] National portal of India: <https://services.india.gov.in>
- [4] National Cybercrime reporting portal: <https://i4c.mha.gov.in>