# VISION FOR VISHWA GURU INDIA: INITIATIVES FOR GLOBAL LEADERSHIP BY 2047

*Sponsored by*

Indian Council of Social Science Research (ICSSR)
Ministry of Education, New Delhi

Volume – I

Editors in Chief
Dr. Ahila. D
Dr. N. Bagyalakshmi

Department of Commerce
**NALLAMUTHU GOUNDER MAHALINGAM COLLEGE**
(Autonomous), Pollachi, Tamil Nadu
95th Rank in NIRF
Re-Accredited by NAAC & ISO 9001:2015 Certified
Affiliated to Bharathiar University, Coimbatore
Website: www.ngmc.org Email:ngm@ngmc.org

# CONTENTS

# CYBER CRIME AND DIGITAL PAYMENTS IN INDIA: A COMPREHENSIVE ANALYSIS

**Dr. G. Anitha Rathna**
*Assistant Professor, Department of Commerce with E-Commerce*
*PSG College of Arts & Science, Tamil Nadu, India*

**Dr. M. Sumathy**
*Professor and Head, School of Commerce, Bharathiar University, Tamil Nadu, India*

**Ms. Sneha Jayalakshmi. J**
*Research Scholar, Bharathiar University, Tamil Nadu, India*

## Abstract

*The payment method has changed as a result of financial transaction digital transformation. The use of digital payments has increased significantly and quickly. As more people choose to use digital payments, there is an increasing risk of falling victim to cyberattacks like online fraud, identity theft, and spyware or virus attacks. Cybercrime, or crimes committed online, has increased as a result of transactions taking place in the digital realm. Hacking on websites, web applications, and web browsers is known as cybercrime. For any business that deals with electronic payments and transactions, secured payment is essential. Cybersecurity is one of the most important problems facing participants in the digital payment ecosystem. Numerous factors, including ignorance and a weak digital payment infrastructure, can be blamed for the increase in these cyberattacks. Various cyber security techniques exist to protect against cybercrime's threats. This chapter discusses the causes, dangers, and fixes for cyber-attacks on digital payment systems.*

***Keywords:*** *Cybercrime, Digital Payments, Challenges, Transaction, Cyber Attack.*

## Introduction

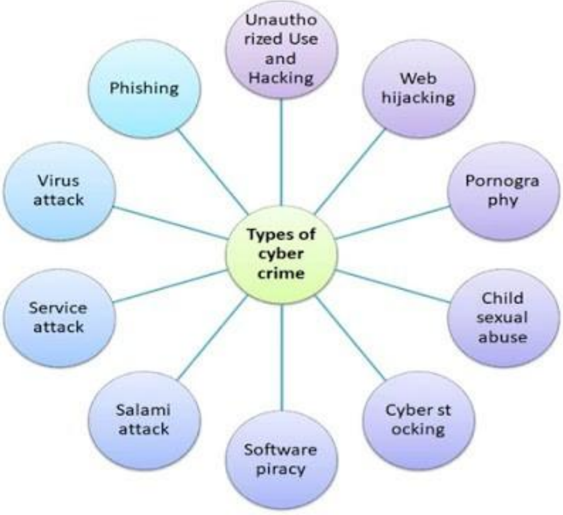
The way people communicate, conduct business, and access information has changed dramatically as a result of the quick development of technology. Cybercrime, as it is commonly known, is one of the newer criminal activities brought on by this digital transformation. India has emerged as a top target for cybercriminals due to its expanding digital landscape and rising internet penetration. In order to effectively combat this threat, it is crucial to comprehend the nature and extent of cybercrime in India as well as the difficulties associated with gathering electronic evidence. the impartial proof in India.This study aims to contribute to the understanding of cybercrime trends in the nation by looking at the most common types of cybercrimes, the legal framework governing cybercrime, and the difficulties and solutions related to electronic evidence collection and preservation. Hacking, identity theft, financial fraud, and online harrassment are just a few of the illegal activities that fall under the umbrella term "cybercrimes," which also includes other related terms. These crimes have serious repercussions for people, businesses, and national security in addition to causing significant financial losses. For the development of successful prevention and response strategies, it is essential to understand the types and patterns of cybercrimes that are common in India.

The Information Technology Act of 2000 serves as the cornerstone of India's legal framework for combating cybercrime (IT Act). The IT Act establishes the legal framework for combating cybercrimes and lays out the punishments for infractions like unauthorised access, data theft, and computer-related offences. But in order to effectively address new threats, the legal system needs to keep up with how quickly technology is developing. In cybercrime investigations, gathering and preserving electronic evidence is a significant challenge. The rapid spread of cybercrime and the dynamic nature of digital data make the timely identification and retrieval of
j electronic evidence crucial .The gathering and preservation of electronic evidence is further complicated by legal and procedural requirements, such as ensuring chain of custody, admissibility, and privacy concerns. Law enforcement organisations must adopt strong strategies and make use of digital forensics methods and equipment to get past these obstacles. In order to improve cybercrime investigation capabilities and create a secure framework for handling electronic evidence, cooperation between the government, law enforcement organisations, and the private sector is essential. This research paper aims to highlight the practical implications of current approaches and pinpoint areas for development by looking at notable cybercrime cases and their related electronic evidence management. Additionally, it will offer suggestions for enhancing cooperation, promoting awareness and education about cybersecurity best practises, and strengthening legislation against cybercrime. It is crucial to comprehend the nature of cybercrime and the difficulties posed by electronic evidence if we are to protect India's digital infrastructure. This research paper aims to contribute to ongoing efforts to combat cybercrime and safeguard people and organisations from digital threats by looking at the common types of cybercrimes, the legal system, and the strategies for efficient electronic evidence management.

**Cyber-Crime**

One of the most important inventions of the twenty-first century is the Internet. Currently, the internet has eliminated all barriers and changed how we interact with one another, play games, work, shop, meet new people, watch movies, order food, pay bills, and greet loved ones on special occasions like birthdays (Al-Zahrani, 2022). Cybersecurity is the most urgent concern as cyber threats and attacks are on the rise.

Fraudsters are now attacking the systems with more sophisticated methods. People, small businesses, and large corporations are all impacted. Because of this, all businesses—IT and non–IT alike—have realised the importance of cyber security and are working to put all available defences in place. Cybercrime is explained in depth in some definitions. Cybercrime is defined by the Oxford Dictionary as "Criminal activities conducted using computers or the Internet." "Cybercrime may be said to be those species, of which a genus is a conventional crime, and where either a computer is an object or subject of the conduct constituting crime," says the definition of the term. There are various ways to commit a cybercrime and some of them are mentioned below in Figure (1).



**Hacking**

It cracks personal security and finds personal data.

- **Unauthorized access to systems or networks:** It is a form of hacking, an unlawful act, or a crime. Here, the attacker intentionally uses another person's account to access a system without the victim's consent.
- **Virus/worm:** Hinders the proper operation of the programs or harms the system and software. • Email bombing: This practice involves the hacker sending the victims phoney or fraudulent emails. The hackers do this by flooding the mailbox with a large number of emails. As a result, the server crashes, disrupting the operation of web portals.
- •**Dos Attack:** harms the hardware and software, or prevents the programmes from operating as intended.
- **Email bombing Attack:** This hacker technique involves sending victims phoney or fraudulent emails. In order to overtax the mailbox, the hackers send an enormous number of emails. The server crashes as a result, disrupting the operation of web portals.

- **Salami attack:** It has to do with money laundering. In doing so, the hackers steal money incrementally or in small steps. Here, they create duplicate bank accounts and transfer a small sum of money from a variety of accounts to one that she can access later.
- **Trojan attack:** In doing so, the hacker seizes command over the computers of others. A Trojan horse virus infiltrates a system and deceives willing users.
- **Web jacking Attack:** The hacker gains control of and access to another legitimate website.

## Authorized Framework for Cybercrime in India

Addressing cybercrime in India requires a robust legal framework that defines offenses, prescribes penalties, and establishes mechanisms for investigation, prosecution, and prevention. The primary legislation governing cybercrime in India is the Information Technology Act, 2000 (IT Act)

1) **The Information Technology Act, 2000:**
   The IT Act is the cornerstone of India's legislation against cybercrime. It offers a thorough framework to address a variety of cybercrimes, such as hacking, unauthorised access, data theft, and computer-related crimes. The Act establishes guidelines for the search and seizure of electronic evidence and gives law enforcement agencies the authority to look into cybercrimes. It also creates the Cyber Appellate Tribunal to hear appeals against the decisions made by the Act's adjudicating officer.
2) **Amendments to the IT Act:**
   The IT Act was strengthened and its provisions were updated to address new issues in light of the evolving nature of cybercrimes. Significant changes were made by the Information Technology (Amendment) Act of 2008 to address new types of cybercrimes and strengthen the penalties for offences like cyberterrorism, identity theft, and confidentiality breaches. The amendment also included provisions for data protection, electronic communication monitoring, and interception.
3) **Other Relevant Laws and Regulations:**
   The legal framework for cybercrime in India is supplemented by other laws and regulations in addition to the IT Act. The Indian Penal Code, 1860, contains provisions that can be used to prosecute online crimes like fraud, libel, and stalking. The investigation and prosecution of cybercrime cases are governed by the Criminal Procedure Code, 1973. Regulations pertaining to financial cybercrimes and electronic payment systems are provided by the Reserve Bank of India Act of 1934 and the Payment and Settlement Systems Act of 2007.

## Jurisdictional Challenges in Prosecuting Cybercriminals

In India, in addition to the IT Act, there are additional laws and regulations that support the legal framework for cybercrime. Online crimes like fraud, libel, and stalking can be prosecuted under provisions in the Indian Penal Code, 1860. The Criminal Procedure Code of 1973 governs the investigation and prosecution of cybercrime cases. The Reserve Bank of India Act of 1934 and the Payment and Settlement Systems Act of 2007 both contain regulations pertaining to financial cybercrimes and electronic payment systems.

## Approaches of Cyber Security

Any illegal activity that makes use of a system, piece of technology, or network is considered a cybercrime. Cybercrime can be divided into two categories: that which targets systems and that which systems unintentionally assist in (Li & Liu, 2021).

## Network Security

The hardware and software safeguards that guard against disruptions, unauthorised access, and other abuses of the infrastructure and network are referred to as network security. With the aid of strong network security, company assets are guarded against a variety of attacks from both inside and outside the organisation. Monitoring cyberthreats and risks related to web browsers, websites, online services, and networks is a crucial part of network security. Thanks to companies like Cisco, Palo Alto, Symantec, Fortinet, Okta, and Z scaler that provide complete network security solutions, our information is secure.

## Firewall

The term "network security" refers to the hardware and software measures that safeguard the network's infrastructure against disruptions, unauthorised access, and other abuses. Effective network security safeguards company assets against a range of attacks coming from both inside and outside the organisation. Monitoring of online risks and threats involving web browsers, websites, online services, and networks is crucial for network security. Businesses offer network security.

## Multi-Factor Authentications

Only after positively presenting more forms of identification to anverification device can a user access websites or software programmes with multi-factor authentication (MFA). A mobile number can be used in addition to a fingerprint, password, or two or more pieces of information (OTP).

**Passwords**

The likelihood of fraud or cybercrime has increased as a result of the popularity of online shopping through various e-commerce websites or applications. In order to protect applications from threats like unauthorised access and modification, security measures must be developed, incorporated, and tested into the applications. To find, fix, and ideally prevent security flaws in applications, the ultimate goal is to enhance security procedures..

**Application Security**

A user can only access websites or software programs with multi-factor authentication (MFA) if they successfully authenticate with identification at an authentication device. A mobile number can be accessed with the information, a fingerprint, a password, or both (OTP). Allowing MFA diminishes the risk of cybercrime because hackers won't be able to admission the computer and does not get the code that your mobile or other devices received.

**Digital Signature**

A digital signature, which functions as a biometric or an addition to a digital document, attests to its legitimacy and integrity. A digital certificate is a document that confirms the bearer's identity and offers security. The three guiding principles of cyber security for the organisation are CIA (Confidentiality, Integrity, and Availability) among all these methods for preventing cybercrimes .It is also referred to as the security triangle. The availability principle implies that the information must be made available based on predetermined criteria, while the confidentiality principle and integrity principle imply that only authorised individuals may access and modify the information .All information must be original and reliable, according to authentication, authorization only grants access to information to those who have been given permission, and accounting mandates regular tracking of all data and events (Wang et al., 2015).

**Conclusion**

Cybercrime and fraud in digital payment systems are covered in this chapter. All financial transactions now take place online as a result of digitization. This situation has increased awareness of cybercrime. The chapter discusses various cybercrimes as well as cyber security measures to prevent or stop them. It draws attention to the transition from traditional to digital payment gateways. The chapter provides a list of the various regulatory bodies in charge of monitoring online transactions and domestic and international cybercrime. CERT-In and NCSP are just two of the organisations that have worked to track down and stop these cyberfrauds. A web-based economy was created as a result of the development of fintech. The cash-based society was replaced by a cashless society thanks to digital payments. An increase in cyber attacks is attributed to the use of computers or other electronic devices for financial transactions. The chapter discusses the main causes of these attacks as well as preventative measures.

**References**

1. Aggarwal, S. (2023). Online Transactions and Digital Fraud: A Bibliometric Analysis. *IUP Journal of Information Technology*, *19*(2), 21-40.
2. Darmawansyah, A., Djunaedi, D., &Kristiawanto, K. (2023). Legal Protection of Cryptocurrency Users Against Cybercrime Attacks. *Journal of Social Research*, *2*(7), 2393-2401.
3. Despotović, A., Parmaković, A., &Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In *Digital Transformation of the Financial Industry: Approaches and Applications* (pp. 255-272). Cham: Springer International Publishing.
4. Makam, G. (2023). Cybercrime and Electronic Evidence in India: a Comprehensive Analysis. *Available at SSRN 4475784*.
5. Napate, S., Dey, A., &Prajapat, S. RISKS ASSOCIATED WITH DIGITAL PAYMENTS. *Enhancing Productivity in Hybrid Mode: The Beginning of a New Era*, 71.
6. Rathna, G. A., &Sumathy, D. Predicting Consumer Intention And Behaviour Towards Organic Food Products-A Consumer Style Inventory (Csi) Approach.
7. Sumathy, M., & Rathna, G. A. (2018). A Study on Marketing Strategies and Awareness About Organic Products in Coimbatore. *ZENITH International Journal of Business Economics & Management Research*, *8*(3), 139-147.
8. Verma, S., Sharma, J., Kaushik, K., & Vyas, V. (2023). Mounting Cases of Cyber-Attacks and Digital Payment. In *Cybersecurity Issues, Challenges, and Solutions in the Business World* (pp. 59-80). IGI Global.