

Deepfake Technology and India's Digital Economy: Regulatory Challenges to Financial Stability, Consumer Trust and Cyber Law Enforcement

Ms. Venu Parnami¹, Dr. Nisha Dhanraj Dewani²

¹Research Scholar, Department of Law, Chaudhary Devi Lal University, Haryana, India
Email: venuparnami@gmail.com

²Associate Professor, Department of Law, Maharaja Agrasen Institute of Management Studies
Email: Dhanraj.nisha31@gmail.com

Abstract

This research study adopts an analytical approach to study the legal and economic aspects of deepfake technology in Indian online economy. It examines the relationship between cyber fraud facilitated by deepfakes, digital financial infrastructures, regulatory initiatives and preparedness of institutions. The referred data been collated from various sources such as government reports, publications from RBI, cybercrime statistics, industry studies and global research on AI-led schemes. The report revealed that India's fast-paced digitisation has outstripped the preparedness of rules and made all elements of the country's banking, digital payment, electoral system, e-commerce and social media ecosystems vulnerable. The drawbacks of deepfake technology undermines the consumer trust, increases transaction risks and compliance costs, and decreases the credibility of evidence in cyber investigations. Existing rules such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, Digital Personal Data Protection Act, 2023, and RBI cybersecurity regulations offer piecemeal safeguards but do not create comprehensive governance frameworks tailored specifically for AI. The study explores the policy recommendations including the statutory regulation of synthetic media, mandatory AI watermarking, digital identity verification, public awareness efforts, the creation of specialised cyber forensic infrastructure and mechanisms for international cooperation.

Keywords: : Deepfake technology, digital economy, cybercrime, artificial intelligence, financial fraud, India, cyber law, fintech regulation, consumer trust, digital payments.

I. INTRODUCTION

India is one of the world's fastest growing digital economies. Internet penetration, availability of smart phones, Aadhar linked identity systems and digital payment platforms have completely changed the economic landscape. Government initiatives such as Digital India, Jan Dhan Yojana and fintech innovation frameworks have accelerated financial inclusion and enabled millions of citizens to become a part of the digital economy. The Unified Payments Interface (UPI) has emerged as a global benchmark for real-time digital payments, said the National Payments Corporation of India (NPCI). The number of digital payment transactions has crossed 18,000 crore in 2024-25, as per government data, reflecting an unprecedented dependence on digital financial systems. The rapid digitalisation of financial services has also been a major driver of the growth of India's GDP and the growth of e-commerce. (Mahmud & Sharmin (2021). But India's digital

ecosystem is increasingly under cyber security threats. Deepfake technology is one of the most dangerous emerging technologies that use deep learning algorithms and generative adversarial networks (GANs) to generate fake audio, video and visual content (Dandotiya (2025). Deepfake systems are able to clone human voices, facial features and identities with alarming accuracy (Nguyen et al., 2019). Originally viewed as entertainment or media, deepfakes are now being weaponised for cybercrime, financial fraud, identity theft, misinformation, extortion and political manipulation. In India, deepfake-enabled scams have targeted banking systems, investors, elderly citizens, users of digital payments and corporate institutions. ((Awah Buo, 2020; Popa et al., 2025; Shoaib et al., 2023). The economic impact of deepfake technology is more than individual fraud. Deepfakes erode consumer confidence in digital transactions, raise compliance costs for financial institutions, distort market

information, and diminish the reliability of digital evidence (Duggal (2026)). The lack of regulation for synthetic media could present systemic vulnerabilities that pose threats to the national economic stability as India moves towards an AI economy. (Vatreš (2021)). This paper seeks to analyse the challenges posed by deepfake technology to the regulatory landscape of India's digital economy with a focus on financial stability, consumer trust and cyber law enforcement.

II. RESEARCH OBJECTIVES

The main objectives of this research are to:

- Describe the principles and evolution of deepfake technology. To understand the economic impact of deep fake related frauds on India's digital economy.
- Evaluating potential consequences of deepfakes for economic stability and public trust.
- Examine the efficacy of the existing cyber law regime in India in dealing with deepfake offences.
- To study the challenges faced by regulatory bodies and cybercrime units in compliance.
- To propose policy options to strengthen legal and institutional frameworks.

III. RESEARCH METHODOLOGY

The research is conducted with doctrinal and analytical approach. The main sources are the Legislative framework like IT Act, 2000 with important amendments, the Digital Personal Data Protection Act, 2023, BNS 2023, and RBI cybersecurity standards along with the government's reports and policy papers. Secondary data is also collected from journal articles and industry studies. Further the observation is developed on the basis of publicly available datasets and official statistics on digital frauds, complaints about cybercrimes, financial losses and growth of digital transactions.

IV. UNDERSTANDING DEEPPFAKE TECHNOLOGY

4.1 Deepfakes: Meaning and Nature

The word "deepfake" is a blend of the words "deep learning" and "fake." Deepfake technology is the use of advanced artificial intelligence models to create synthetic media that looks very similar to real people (Ke et al. (2025)). As indicated in figure no. 1, the dominant technology platform is the Generative Adversarial Network (GAN), comprising a neural network that creates synthetic content and another that detects discrepancies. (Misirlis and Munawar (2023)).

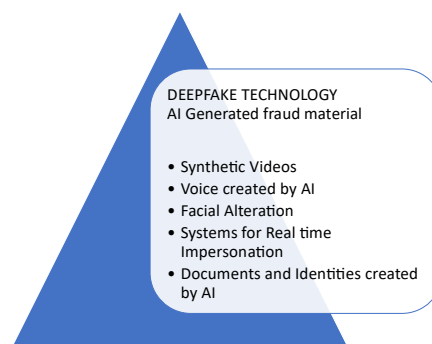


Figure No. 1 AI generated Deepfake content

Modern deepfake technologies have become so sophisticated, fuelled by advances in machine learning, cloud computing and availability of public datasets (Fernando et al. (2025)).

4.2 Evolution of Deepfake Technology

Deepfake technology was originally created for entertainment, gaming and film. However, with the increasing availability of AI tools, cybercriminals have been able to leverage deepfakes for malevolent purposes (Shohel et al. (2022)). The rise of AI software and cheap computing power has made the

production of synthetic media available to a wider audience (Nguyen et al. (2019).

V. INDIA'S DIGITAL ECONOMY AND GROWING VULNERABILITIES

5.1 Expansion of Digital Financial Systems

India's digital transformation is one of the most comprehensive in the developing world. Digital payment systems, mobile banking apps, e-commerce platforms and AI-driven governance mechanisms have greatly enhanced economic efficiency. UPI has become the backbone of India's cashless economy. The post-demonetisation and post-pandemic digitalisation trend has seen a huge spurt in digital financial inclusion. Digital transactions are increasingly relied on by small businesses, casual workers and rural communities. But the fast pace of digital adoption has also increased the vulnerability to cyber threats. In many cases, new Internet users do not have sufficient knowledge of cybersecurity.

5.2 Economic Dependence on Consumer Trust

Digital economies operate fundamentally on the foundation of trust. Users need to have confidence on various financial platforms. Deepfakes pose a significant risk to the foundation of trust by facilitating realistic impersonation and misleading representations (Vecchietti et al. (2025). For example, voice clones created by AI can replicate the voices of bank officials, corporate leaders, or

even family members, thereby deceiving victims into transferring money.

5.3 Digital Fraud in India

As discussed above, the digital frauds are increasing day by day. An analysis of Artificial Intelligence (AI) scams in India, 2025 report reveals that 47 % of Indian adults have either fallen victim to, or are acquainted with someone who has been a victim of, an AI voice-cloning or deepfake scam, which is nearly double the global average of 25 percent. The report states that 83 percent of those in India who were duped by AI voice scams suffered financial losses, with nearly half of these losing more than INR50,000. This underlines the alarming rise of fraud driven by deepfakes in the Indian financial sector (Jainendran, 2026). One trend particularly threatening to the financial sector is the rise and increasing prevalence of deepfakes as tools of cyber-enabled financial crime in the rapidly evolving threat landscape. Artificial intelligence and machine learning have progressed to the point where synthetic content can be produced with such high fidelity that most people can't tell it from real media. These developments have created major opportunities for creativity and increased efficiency but have also created new avenues for fraud, impersonation and large scale deception that pose challenges for existing legal, technical and organisational safeguards. (Kashyap, S. (2025).

Table No.1 Estimated Increase of Cyber and Deepfake-Enabled Financial Fraud in India

Year	Reported Cyber Fraud Complaints	Estimated Financial Losses	Major Trend
2021	2,62,846	₹551 + crore	After the pandemic, digitalization of payment has rapidly increased thus leading to more fraud.
2022	6,94,446	₹2,290+ crore	Growth in UPI and impersonation scams
2023	13,10,357	₹7,465 crore	AI-assisted phishing and rise in the identity fraud.
2024	19,18,835	₹22,845 crore	Massive expansion of AI-enabled deepfake frauds
2025*	24,02,579	₹22,495 crore (all banking frauds, including digital frauds)	Rising synthetic identity and deepfake scams

Source: Compiled from data of the Indian Cyber Crime Coordination Centre (I4C), National Cyber Crime Reporting Portal (NCRP), Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), Ministry of Home Affairs, Government of India, as reported in [The Economic Times](#)

Table No. 2: Cyber Crimes and Monetary losses in India

Indicators	Reported Data	Significance
Cyber fraud losses in 2024	₹22,845 crore	206% increase from previous year (2023)
Fraud complaints in 2024	Approx. 3.6 million	Indicates large-scale digital vulnerability

High-value cyber fraud cases FY2024	29,082 cases	More than a fourfold increase
Losses from high-value frauds	₹1.77 billion+	Reflects increasing sophistication of scams
Fraudulent accounts created daily	Approx. 4,000	Demonstrates organized cybercrime activity
Karnataka digital arrest losses (2023–2026)	₹468 crore+	Growing impact of impersonation scams

Source: Risk Management Association of India Report 2025

RMA India. (2025, July 23). *India's cyber fraud losses soar 206% to ₹22,845 crore from 2024*. Risk Management Association of India. <https://rmaindia.org/indias-cyber-fraud-losses-soar-206-to-%E2%82%B922845-crore-from-2024>

As indicated in table no. 1 and table No. 2, the rate of cybercrimes and monetary losses in India has been increasing drastically and continuously from 2021-2025. The number of cyber fraud complaints witnessed an exponential growth due to the rise in online banking and digital transactions in the country from 2,62,846 in 2021 to 24,02,579 in 2025. The increasing volume and complexity of cybercrime is also reflected in the rising financial losses, from ₹551 crore in 2021 to ₹22,845 crore in 2024. However, as digital transactions have increased post-outbreak, so has the number of various kinds of frauds like UPI frauds, impersonation scams, synthetic identities and phishing attempts using Artificial Intelligence and deepfake technology. Other data released by the government and the RBI only underscore the magnitude of the problem (RMA India (2025)). In 2024, more than 29,000 high-value frauds and more than 3.6 million fraud reports were received. As the cybercrime networks become more complex and structured, the digital arrest scams have been causing a massive loss of over ₹468 crore and nearly 4,000 bogus accounts being opened every day in Karnataka. The numbers speak for themselves India needs a robust legislative framework, awareness programs and enhanced cyber security to combat AI driven financial crime and identity theft (RMA India (2025)).

VI. FINANCIAL FRAUD TECHNIQUES AND DEEPFAKES

Deepfake-enabled financial fraud has become one of the most dangerous cybercrime offenses in the digital economy. Bad actors use sophisticated technology to create convincing fakes of audio, video, images, and identity to exploit human psychology for financial gain and erode systems of

trust. These fraudulent schemes are becoming more complex and are becoming harder to detect.

(a) Voice Cloning Scams

When an AI is used to mimic a human voice, it is engaging in voice cloning fraud. For example, internet criminals frequently take voice samples from interviews, social media or phone calls to develop convincing audio clones. Scammers will often pose as someone you know and trust – such as a family member, your boss, a police officer or a bank official – to make it sound like you need to send money right away. These schemes use the trust and fear that comes with emotions to trick victims into handing up important information or sending money without confirming if it's legitimate (Kumar & Devi, 2026).

(b) Corporate Executive Impersonation

Corporate fraud schemes involve sophisticated tools to impersonate high-ranking personnel, such as CEOs, CFOs or other senior management. Scammers send bogus voice or video instructions that appear to authorise large financial transactions or the release of sensitive information. If the message is authentic, workers might follow the regulations. Such attacks can result in major financial losses, damage to reputations and suspension of activity for financial institutions and organisations.

(c) Counterfeit Investment Platforms

Fraudulent investment schemes are being advanced by cybercriminals with the use of deepfake celebrity endorsements and fake interviews. One way to get a misleading credibility is through the online spread of counterfeit videos featuring notable personalities, corporate executives, or financial gurus. Cryptocurrency scams, Ponzi schemes and fake trading platforms swindle naive investors out of their money. Such dishonesty undermines investor confidence and the validity of online financial markets.

(d) Manipulation of Banking Authentication

Voice and facial recognition among other biometric validation technologies are becoming more and more a part of current banking frameworks. Artificial intelligence-generated face replicas and synthetic identities can circumvent these methods. Criminals can exploit Know Your Customer (KYC) requirements to access financial accounts and commit fraud without authorisation (Kubam, 2026; Ke et al., 2025).

(e) Political and Market Manipulation

Deepfakes could create chaos in the political and financial world due to its usage of fake announcements, speeches or news reports. Politicians, bank officials or business moguls can make misleading assertions that will make investors lose faith in the market and cause price swings. False information can alter market dynamics, erode investor confidence and undermine the security of digital economy finances.

VII. DEEPFAKE TECHNOLOGY'S ECONOMIC EFFECTS

7.1 Financial Stability Risk

Financial stability is the capacity of monetary systems, payment networks, and other economic institutions to continue functioning normally in the face of systemic shocks and crises. Financial stability in a digital economy like India's depends on secure online transactions, consumer trust, and reliable digital communication technologies. Deepfake technology poses a significant danger to this stability since it facilitates complex fraud, identity theft, and disinformation campaigns that might wreak havoc on financial institutions. As artificial intelligence (AI) tools become more accessible and advanced, cybercriminals are utilising deepfakes to attack consumers, investors, fintech companies, and banks.

(a) Increasing Transaction Fraud

There are very clear economic implications of deepfake technology. One is the increase of fraudulent digital transactions. Synthetic identities, false video interactions and AI-generated voice cloning are tools that cybercriminals might use to impersonate real people or groups. The victim is

lured into unlawful payments, transmitting money or giving up important financial information. Such loss erodes public trust in digital payment platforms such as UPI, mobile banking and online wallets (Jainendran (2026). With the rise of cybercrime, the demand is increasing on financial institutions to reimburse the affected customers. Insurers have also experienced a sharp increase in claims connected to digital fraud. The mounting losses are putting the effectiveness of financial risk management systems and the profitability of banks to the test. Continued fear of fraud might see people shunned away from utilising digital financial services, hampering progress towards a cashless economy.

(b) Protective and Compliance Costs

Deepfake technology has forced financial institutions, fintech startups and digital payment providers to drastically boost their spending on cybersecurity and fraud protection solutions. To identify altered audio, video and identity, financial institutions must use advanced detection systems based on artificial intelligence, biometric verification, behavioural analytics and real-time fraud monitoring tactics. It is increasingly costly and essential to comply with legislation on cybersecurity. For example, businesses have to spend money on data security solutions, cyber audits, forensic investigations, employee training, etc. When it comes to financial technology, compliance can be prohibitively expensive for smaller companies. This struggle may limit their ability to compete successfully, and this may lead to a market that progressively favours larger enterprises with superior technologies (Vecchietti et al. (2025).

(c) Operations Dangers

Financial organisations and corporations are particularly vulnerable to deepfake attacks. Internal communication systems, payment processing, and banking activities are all vulnerable to disruption caused by deepfake technology's fraudulent instructions. For example, employees could be led astray by false executive directives and authorise unauthorised financial transactions or the disclosure of sensitive information. As well as, the obvious loss of money, businesses incur additional costs in terms of forensic investigations, litigation and damage to

their brand. Deepfakes are a risk to brand reputation and customer trust when the public learns of fraud. Digital services that can affect business continuity and economic output are also at risk from cyber disasters.

(d) Danger to Innovation in Fintech

India's fintech ecosystem is one of the fastest growing in the world and online lending platforms, digital payments, blockchain and AI are all helping it to grow at a rapid pace. On the other hand, persistent deepfake-related fraud may act as a deterrent for funding of fintech and technological innovation. (Bartoletti & Byler, 2020). Fintech firms may prioritize compliance with security regulations over innovation when developing new digital financial services and products. Increased risk of fraud results in heightened oversight from regulatory bodies. However, it also suggests higher compliance costs, which pose a significant obstacle for startups and entrepreneurs. The implications of this could be significant for India's position as a global leader in digital finance innovation.

(e) Problems Faced by Foreign Investors

Inadequate cyber governance frameworks, coupled with an increase in AI-driven fraud, may undermine international investor confidence in India's digital economy. For a foreign investor, the decision to invest in financial markets or IT enterprises generally hinges on factors such as cybersecurity resilience, regulatory effectiveness, and digital trust. The increase in cyber challenges linked to deepfakes has generated apprehensions regarding data security, financial transparency, and market credibility. Inadequate tools for AI governance can increase the operational and regulatory risks that investors encounter in digital markets. Hence, besides being a cybersecurity issue, deepfake technology is a massive economic hurdle that could impact investor confidence, market integrity, and financial security in India's rapidly growing digital economy. People are hesitant to engage in online transactions when they have concerns about impersonation or identity theft. In the end, digital adoption and economic growth could be slowed down by issues of trust (Popa et al. (2025).

VIII. CONSUMER CONFIDENCE DECLINES

A digital economy is built on the fundamental pillar of consumer trust. Digital financial systems, e-commerce platforms, online banking services and AI-enabled technologies can only function optimally when users trust the security, reliability and fraud-resilience of these systems. Trust is paramount in India's fast-growing digital economy as millions of people are entering digital commerce and online financial services for the first time. The use of deepfake technology poses a considerable threat to this trust through more advanced impersonation, theft of identity and dissemination of disinformation. As people become aware that AI can create realistic fake videos, imitate voices and change identities, they begin to question the genuineness of online interactions. This fear of impersonation and financial fraud makes people hesitant to engage with digital platforms and this breaks the trust in the technology-driven economic systems. Online banking-related anxiety is on the rise. Consumers are worried that bad actors can undermine accounts, evade verification procedures, and disrupt financial transactions using sophisticated deepfake technology. Digital banking and other cashless payment solutions are less likely to be adopted due to these difficulties. As an example, the reliability of video verification systems utilised by banking and fintech for remote authentication and KYC purposes is being undermined by deepfake technology. (Kishwar, S. D. (2025). Moreover, when people relate technology to deception and fraud, they are less likely to trust services driven by AI. "If consumers perceive these systems as dangerous or unpredictable, automated financial advisers, digital assistants and customer assistance powered by AI may be hampered in their adoption." Digital identity systems are also caught up in another fundamental problem of hesitance. The digital economy of India is increasingly supported by digital verification technology and biometric identities. Fears around synthetic identities, loss of personal data and identity fraud could mean that people are less willing to engage in digital governance and financial inclusion projects. Ultimately, a lack of consumer trust in a business can hinder digital adoption, reduce transaction volumes, and negatively impact long-term economic growth.

The rise of deepfake fraud poses a significant challenge to the overarching objectives of Digital India and financial inclusion, as trust serves as the cornerstone of digital transformation.

IX. IMPACT ON DIGITAL MARKETS AND E-COMMERCE

Digital marketplaces and e-commerce platforms face higher risks associated with deepfake technology as they are heavily dependent on visual content, advertisements, and influencer marketing. The credibility of online reviews, endorsements, and transactions is what provides legitimacy to online shopping. Widespread market distortions stem from the deepfake manipulations which impacts credibility. One of the considerable threats is the misleading product endorsements. Criminals may exploit these AI-generated films promote products, investment schemes, or online services, occasionally featuring prominent individuals to mislead the innocent victims who end up purchasing inferior or counterfeit products. Such deceptive behaviour undermines consumer protections and skews the competitive environment in online marketplaces. (Mahashreshty Vishweshwar, 2023).

Furthermore, deepfake technology enables the creation of altered advertising content and fabricated customer reviews misleading the customers regarding the reliability and quality of products. As a result, unscrupulous sellers can engage in unfair competition against legitimate businesses by utilizing manipulated information to draw in customers.

Another significant challenge faced by the digital artists and influencers is with identity theft. Fraudsters may exploit the image or voice of well-known social media personalities to promote fraudulent financial products, counterfeit items, or scams. The credibility of influencers diminishes, leading to the potential for misguiding their fans and consumers.

False information in the market and deceptive advertising represent significant challenges. Deepfake films and AI-generated content can present misleading information, including false claims about discounts, investment opportunities, or governmental clearances that are not actually

available. Fraudulent advertisements disseminated via digital platforms and social media can result in financial losses for consumers who engage with them. The collapse of market integrity can be attributed to the combined effects of these behaviours. Online shoppers lose faith in businesses, businesses lose their edge in the market, and consumers feel unsafe making purchases due to deepfake manipulation. Loss of trust in online marketplaces might stunt e-commerce development and dampen investor enthusiasm for digital markets in the long term.

X. MACROECONOMIC IMPLICATIONS

Businesses aren't the only ones hit by deepfake cyber fraud; individuals are victims as well. Digital fraud is a major threat to national development, financial stability, and growth targets on a macroeconomic scale. Capital moves away from its original location. Massive cyber fraud leads to the illegal transfer of funds from people, businesses and financial institutions. The economic drain from scams, phishing schemes and fraudulent transactions blocks the productive flow of the economy and decreases the capacity for consumer spending (Bhale, S. (2025). Deepfake technology could be used to commit fraud and could hinder the development of digital transactions. If people feel that digital payment systems are not secure, they may revert to the use of cash, or even avoid online financial services altogether. This slowdown has a direct impact on the growth of fintech, adoption of digital banking and aspiration of a cashless economy. A stronger enforcement infrastructure, cyber forensic laboratories, AI surveillance technologies, and fraud detection systems is something that law enforcement, cyber security organisations, and financial regulators should heavily invest into. Government agencies already have a heavy financial load due to these expenses.

Another significant outcome is the rising expense of overseeing financial institutions. Addressing them increasingly relies on data analytics tools, AI detection systems, and sophisticated monitoring systems employed by both public and private sectors. Although these steps are critical for cybersecurity, their concern is for the privacy and data protection of parties and come with hefty price tags.

Productivity drops as a result of deepfake fraud and other cyber security threats. All areas of the economy see a drop in efficiency and production when reputational harm and disruptions to operations occur.

In addition to the obvious financial and productivity loss, deepfake technology has a lot of hidden expenses. It affects consumer confidence, market stability, institutional efficiency, investor confidence and long-term development goals. The proliferation of deepfake technology in cybercrime, if not contained, can be a serious challenge to the sustainable growth of India's digital economy.

XI. DEEPPAKES AND CYBERCRIME IN INDIA

a. Increase in AI-Driven Cybercrimes

The scenario of cybercrime in India has seen a revolution with the advent of artificial intelligence. With the use of AI-powered tools, cybercriminals are now able to execute more sophisticated, targeted and massive attacks than ever before. One of the most obvious examples of AI-driven cybercrime is the use of AI to generate phishing emails that are designed to look like they came from banks, enterprises or government bodies. These scam emails can look legitimate and can fool consumers into giving up important information, leading to widespread financial fraud and data theft. Fraudsters are also increasingly adopting voice cloning technology, with hackers creating AI-generated duplicates of voices to pose as family members, corporate leaders or other trustworthy people and ask for money to be sent urgently. Another rising concern is deepfake video fraud, where people, organisations and the public are deceived by faked films. These films can ruin reputations, propagate disinformation and erode trust in digital media. AI has also enabled synthetic identity fraud where criminals may generate realistic but fake identities that may even pass Know Your Customer (KYC) verification checks, posing severe concerns to banking and fintech security. And the rise of AI-powered automated misinformation campaigns means that false news, propaganda, and deceptive stories may be rapidly disseminated, fuelling social unrest and economic instability. The most disturbing aspect of these technologies is the

scalability, as AI tools allow cybercriminals to automate attacks and target thousands of victims at a very cheap cost, radically boosting the reach and profitability of cybercrime operations. (Shoaib et al., 2023).

11.2. Social Engineering and Psychological Manipulation

The success of social engineering assaults has been increased by deepfake technology by using human emotions and psychological vulnerabilities. Fake emergency calls are a typical approach, with deepfake voices impersonating relatives or friends in trouble, asking for urgent financial help. Victims are often in a hurry to transfer money, acting spontaneously, under pressure of their emotions. Another growing type of fraud is impersonating government or police, when criminals employ AI-generated voices and films to impersonate law enforcement officers, government officials or regulatory bodies. Fraudsters use a threat of arrest, a legal action or financial penalties to scare victims into paying extortion. Cybercriminals also do fake customer support chat, impersonating personnel of banks, e-commerce platforms or service providers to get passwords, one-time passwords (OTPs) and other sensitive financial information. AI-powered romance scams are also gaining in popularity, with scammers using the technology to construct convincing fake identities and form emotional connections with victims online, before either fleecing them for money or blackmailing them. In all these tactics the name of the game is emotional manipulation. Cybercriminals use fear, urgency, trust, affection, and panic to greatly raise the chances of successful fraud. Thus, deepfake-enabled social engineering is one of the deadliest types of modern cybercrime.

11.3 Vulnerable Group

The damage from deepfake-enabled cybercrime does not affect everyone in society equally, with certain groups being more vulnerable than others. Older people are particularly vulnerable, as they are not very tech-savvy and not well-versed in the latest cyber risks. They are therefore regularly targeted by voice cloning scams, banking frauds and impersonation schemes. Rural digital users are

especially more vulnerable because of poor cybersecurity literacy and awareness of online fraud methods. They are often victims of UPI fraud and impersonation scams. Similarly, first-time internet users are often not familiar with digital systems and may have difficulty recognising phishing, false verification requests and fraudulent messages. Small business owners rely more on digital payment systems and online transactions and are susceptible to corporate impersonation assaults, fraudulent payment requests and business email compromise scams. Women and students are often vulnerable to identity theft, deepfake-based harassment, sextortion, and online exploitation due to their heavy use of social media platforms. The digital communication systems, banking applications and internet services are gaining their popularity even among the common customers, who are increasingly susceptible to cyber risks. As deepfake technologies get more sophisticated, the opportunity for deceit across all demographic groups increases, which calls for more public awareness and digital literacy campaigns.

11.4 Issues of Cyber Forensic

The uncontrolled growth of deepfakes and AI-generated content offers significant hurdles to cyber forensic investigation and the administration of justice. Sandoval et al. (2024). One of the biggest challenges is how to verify the authenticity of digital evidence, as investigators often can't explain if content is real or has been fabricated or altered by AI. This ambiguity diminishes the dependability and evidentiary value of digital materials presented to courts and investigative authorities. Another problem is the identification of the perpetrators, as cybercriminals often employ AI techniques, anonymisation technologies and counterfeit digital identities to hide their involvement, which delays the investigations and punishments. Tracing of AI-generated content is also equally challenging since deepfakes are sometimes hard to be attributed to the original creators. This leads to weak attribution procedures and restricted accountability. Enforcement efforts are further complicated by jurisdictional difficulties as servers, platforms and offenders sometimes operate across numerous nation's leading to serious cross-border legal and

enforcement challenges. Moreover, the issues of metadata integrity are raised when the metadata of the manipulated files are modified, deleted or invented, which undermines the forensic verification process. Another major issue is the increase of the so-called "liar's dividend" problem, where anyone can dismiss real evidence by labelling it a deepfake, thereby eroding faith in actual digital evidence and making legal proceedings more difficult. Moreover, the majority of law enforcement agencies and forensic professionals do not have expertise in the use of AI and deepfake detection, which reduces their investigation effectiveness.

The tremendous speed of technological innovation implies AI tools are evolving considerably faster than legal and regulatory frameworks, producing substantial enforcement gaps and challenges to effective policymaking. Collectively, these problems demonstrate the urgent need for improved forensic skills, specialised training, international cooperation, and robust legislative frameworks to combat the rising threat of deepfake-enabled cybercrime in India.

XII. INDIAN LEGAL FRAMEWORK FOR DEEPFAKE FRAUD

India already has cyber law in the form of IT Act, DPDP Act 2023 and DPDP Rules 2025 where intermediary and financial laws cover deep fake related frauds. In IT Act 2000, sections 66C and 66D deal with cheating by personation and identity theft respectively and so provide a way to fight fraud and impersonation using deepfakes. Section 72 is for personal information. The provisions such as sections 67 and 67A are for profound false content that is sexually explicit or filthy. However, the Act does not define or govern deepfakes, synthetic media, or AI-generated identities. Government has recently amended India's IT intermediary rules with the Notification No. G.S.R. 120(E) and signed by Joint Secretary Ajit Kumar and discussed in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, the growing misuse of deepfake technology and remove the flagged unlawful content.

Apart from above, the Bharatiya Nyaya Sanhita, 2023 (BNS) can punish actions employing

deepfakes like as criminal intimidation, forgery, identity fraud, defamation and sexual exploitation. These laws give a legal remedy, but they may not be very enforceable since they are not designed for AI-generated content. The Reserve Bank of India and the banking industry have put in place a number of measures like two-factor authentication, transaction monitoring, fraud detection systems and risk-based limits to prevent digital fraud. These methods help to prevent financial loss but there is no present framework in place to fight deepfake driven financial fraud. India's present legal framework for tackling deepfake-related offences has major gaps because there is no special legislation that governs artificial intelligence-generated content and synthetic media.

XIII. RECOMMENDATIONS

1. Implementation of Specific Legislation Addressing Deepfake Technology

Deepfake and other forms of artificial intelligence-generated synthetic media pose serious problems, and India must immediately enact thorough legislation to deal with them. When it comes to protecting citizens from the ever-evolving threat of cybercrime powered by artificial intelligence, the present legislative frameworks set up by the IT Act, BNS and data protection legislation are incapable. Definitions of synthetic media, AI impersonation, manipulated digital content, and non-consensual digital change should be defined precisely as part of a thorough law tackling deepfakes. Legislation prohibiting the destructive creation, diffusion, and application of deepfakes must be established. This is especially important in cases of sexual exploitation, election manipulation, fraud, identity theft, and extortion. Specific roles must be specified for the digital service providers, artificial intelligence (AI) creators, and social media intermediaries which includes duties such as content moderation, rapid removal procedures, mandatory reporting of dangerous synthetic media, and digital evidence storage for investigations.

2. Enforced watermarking and artificial intelligence tagging

Mandatory digital watermarking and tagging systems for AI-generated content are among the

finest means to fight against the exploitation of deepfakes. We need to be able to identify artificially generated audio, video and images from actual media.

Imposing watermarks would make it easier to spot doctored video. This would be a win for digital platforms, consumers and investigative authorities. Traceability technologies will increase accountability by allowing authorities to trace the origin and propagation of harmful deepfake content. Moreover, obligations to provide transparency, such as specific branding of AI-generated content, would help in the fight against disinformation and will safeguard consumers from being misled by fraudulent films, adverts or financial sponsorships. Such measures – increasingly common across the world – might go a long way in helping India's digital trust framework (Oza et al. (2024).

3. Strengthening the defences of the banking industry against cyberattacks.

The banking and financial sectors are particularly vulnerable to fraud enabled by deepfake technology. That's why today's banks and other financial institutions need modern cybersecurity solutions that can detect advanced AI-based attacks. (Shohel, R. M., et al. (2022). Biometric verification systems can be used by financial institutions and fintech organisations to enhance their security measures by combining elements such as facial recognition, voice authentication, device identification and behavioural analytics. Relying on a single authentication technique increases the vulnerability to deepfakes. Banks and other financial organisations should leverage advanced AI-powered fraud analytics to identify synthetic identity fraud, strange account activity and unexpected transaction patterns. It would be much easier to prevent fraud if computers could look at how users behave, such as their typing patterns, their transaction history and their device usage. Further precautions such as required client alerts, real-time anomaly detection and cooling-off periods for high-risk transactions can considerably reduce monetary losses from impersonation scams. Regular cybersecurity assessments and comprehensive personnel training are important to stay ahead of the growing threat landscape.

4. Initiatives to raise awareness and educate the general residents.

Fighting the intricacy of deepfake fraud involves more public education, greater digital literacy initiatives, and regulatory measures for technology. Public education is vital in decreasing victimisation because a lot of cybercrime involves social engineering and psychological manipulation. To counteract the growing dangers from cyber-attacks, there needs to be cooperation across government agencies, banks, educational institutions and IT corporations to build comprehensive digital literacy projects. Public awareness programs should be targeted at educating individuals of the dangers of phishing attempts, online impersonation, fake videos, voice cloning frauds and the best approaches to assure secure transactions. The priority should be given to individuals who are least likely to have sufficient knowledge of cybersecurity practices. This would cover students, rural residents, the elderly and digital newcomers. Cyber fraud reporting mechanisms should be well known and campaigns should focus on the importance of verification measures and safe online activity. Raising awareness among individuals regarding AI-generated dishonesty will help boost public confidence in digital systems and dramatically lower the effectiveness of social engineering efforts.

5. An Advanced technical Investigating framework

The rise of deepfake technology creates serious problems for cyber forensic investigations as synthetic media can affect the integrity of evidence. Hence, India has to build a world-class forensic infrastructure to identify and verify AI-generated content. The Government should set up National AI Forensic Laboratories with state-of-the-art deepfake detection tools, advanced machine learning analysis systems and technology to authenticate digital evidence. The development of a cybercrime agency with specific sections for the deepfake detection can boost the efficiency of the investigations and the technological knowledge. Thus, India has to roll up common norms for certification of AI-generated evidence to ensure legitimacy and admissibility of digital evidence in court processes. All law enforcement, prosecutors and training in artificial intelligence (AI), cyber forensics (CF) and synthetic

media analysis (SMA) is mandatory for all the judicial officers, lawyers and law enforcements. An increase in the conviction rates, making investigations trustworthy and making sure that there are less problems while dealing with altered digital evidence will be the outcome of the better forensics capabilities of a country.

6. Cooperation on a global scale

The character of this crime is inherently global since the involved offenders, servers, victims and digital platforms in deepfake-facilitated cybercrime crosses over several legal areas. Effective regulatory infrastructure requires strong cross-border enforcement procedures and international cooperations. India should strengthen its Mutual Legal Assistance Treaties and international agreements on cybercrime to facilitate better sharing of information, collection of digital evidence and extradition. International security organisations, cybersecurity response teams and law enforcement agencies around the world could collaborate to ensure timely information sharing and coordinated responses to widespread fraudulent activity.

India should take the lead in international discussions on AI governance to establish uniform standards for the regulation of synthetic media, AI transparency, cybersecurity ethics, and digital evidence management. Better international legal harmonisation would significantly improve enforcement against transnational cybercriminal networks.

7. Algorithm for managing AI research and development

India could develop AI regulatory frameworks that enable innovation while ensuring the ethical development and use of AI technology. Regulatory sandboxes enable decision-makers to test risks and compliance solutions in a controlled setting prior to a larger deployment. Such settings could also benefit research into AI governance frameworks, development of deepfake detection tools, and ethical AI testing. The partnership of government agencies, financial institutions, technology companies, educational institutions and cybersecurity experts can drive innovation and clarity in regulations. Privacy concerns, algorithmic prejudice,

cybersecurity threats, and the abuse of synthetic media are just some of the new AI-related hazards that regulatory sandboxes might help uncover (Bhargava (2025)).

To sum up, aggressive legislative reforms, technological protections, institutional preparation, education, and training are mandatory if artificial intelligence is to benefit rather than hinder India's digital economy.

CONCLUSIONS

The e-commerce sector of India is encountering an increasing threat from deepfake technology. The potential advantages of artificial intelligence (AI) to economies, financial inclusion, governance, and technological advancement are significant; however, the threats posed by financial fraud and cybercrime are considerable. Online trust structures, digital profiles, and amenities fuelled by artificial intelligence are becoming growing essential to the Indian economy as the nation experiences a rapid digital transformation. Due to its ability to create highly convincing impersonations, the dissemination of false information, and the enablement of financial fraud, deepfake technology presents a serious threat to the reliability of trust systems. Cyber fraud losses have skyrocketed, customer trust has dropped, compliance costs have risen, reputation has taken a hit, and digital payment systems have security flaws, all of which have an economic impact.

REFERENCES

1. Adabala, D. S. (2026). *When technology lies: Deepfake and criminal law in India*. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6665081
2. Advisory on Deepfakes and AI-Generated Content. (2023, December 26). *Press Information Bureau*. <https://pib.gov.in/PressReleasePage.aspx?PRID=1989777>
3. Awah Buo, S. (2020). *The emerging threats of deepfake attacks and countermeasures*. arXiv. <https://arxiv.org/abs/2012.07989>
4. Bartoletti, I., Leslie, A., & Millie, S. M. (Eds.). (2020). *The AI book: The artificial intelligence handbook for investors, entrepreneurs and FinTech visionaries*. Wiley. <https://doi.org/10.1002/9781119551928>
5. Bhale, S. (2025). *Deepfake laws in India: The need for legal regulation in the AI era*. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5153296>
6. Bhargava, A. (2025). *Deepfake technology and its legal regulation in India: A doctrinal and comparative study*. Vintage Legal. <https://www.vintagelegalvl.com>
7. CERT-In. (2024). *Deepfake threat advisory*. <https://www.cert-in.org.in>
8. Dandotiya, R. (2025). *Cyber Rakshak*. Mahagatha.
9. Duggal, P. (2026). *Online frauds and law: Legal framework, cyber crime, digital evidence & Indian cyber laws*. Law & Justice Publishing Co.
10. Fernando, T., Katuwal, R., Gammulle, H., Seneviratne, S., & Denman, S. (2025). *Face deepfakes: A comprehensive review*. arXiv. <https://arxiv.org/abs/2501.09692>
11. IndiaAI. (2024). *Revised AI advisory: How AI regulation can impact India*. <https://indiaai.gov.in>
12. Jainendran, P. (2026, January 15). *Deepfakes and financial cybercrime: India's multi-layered response*. Observer Research Foundation. <https://www.orfonline.org>
13. Kashyap, S. (2025). *The digital mirage: India's evolving legal battle against deepfake technology*. SCRIPTed: A Journal of Law, Technology and Society, 22(2). <https://doi.org/10.2218/scrip.22.2.2025.12004>
14. Ke, Z., et al. (2025). *Detection of AI deepfake and fraud in online payments using GAN-based models*. arXiv. <https://arxiv.org>
15. Kishwar, S. D. (2025). *Regulating deep fakes and synthetic media: Privacy, policy and legal challenges*. Journal of Data Protection and Privacy.
16. Kubam, C. S. (2026). *Agentic AI microservice framework for deepfake and document fraud detection in KYC pipelines*. arXiv. <https://arxiv.org>
17. Mahashreshthy Vishweshwar, S. (2023). *Implications of deepfake technology on individual privacy and security*.

18. Mahmud, B. U., & Sharmin, A. (2021). *Deep insights of deepfake technology: A review*. arXiv. <https://arxiv.org/abs/2105.02496>
19. Ministry of Electronics and Information Technology. (n.d.). *Information Technology rules*. <https://www.meity.gov.in>
20. Ministry of Home Affairs. (n.d.). *Cyber crime reporting and management portal*. <https://cybercrime.gov.in>
21. Misirlis, N., & Munawar, H. B. (2023). From deepfake to deep useful: Risks and opportunities through a systematic literature review. *Journal of Content, Community and Communication*, 18(9), 78–95. <https://doi.org/10.31620/JCCC.12.23/06>
22. Mohamed, R. S., et al. (2023). *Deepfakes, misinformation, and disinformation in the era of frontier AI*. arXiv. <https://arxiv.org/abs/2309.12397>
23. National Crime Records Bureau. (2021–2025). *Crime in India reports*. <https://ncrb.gov.in>
24. National Payments Corporation of India. (n.d.). *Annual reports*. <https://www.npci.org.in>
25. Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. (2019). *Deep learning for deepfakes creation and detection: A survey*. arXiv. <https://arxiv.org/abs/1909.11573>
26. Oza, P., Patel, N., & Patel, A. (2024). *Deepfake technology: Overview and emerging trends in social media*. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.4981040>
27. Panda, B. N. P. (2024). *Deepfake technology in India and world: Foreboding and forbidding*. Law and Humanities Quarterly Review.
28. Parliamentary Standing Committee on Information Technology. (n.d.). *Reports on artificial intelligence and cybersecurity*. <https://loksabhadocs.nic.in>
29. Passos, L. A., et al. (2022). A review of deep learning-based approaches for deepfake content detection. *Expert Systems with Applications*, 196, 116736. <https://doi.org/10.1016/j.eswa.2022.116736>
30. Press Information Bureau. (n.d.). *Cyber fraud and digital arrest scam reports*. <https://pib.gov.in>
31. Reserve Bank of India. (2024–2025). *Annual report*. <https://www.rbi.org.in>
32. Reserve Bank of India. (n.d.). *Cyber security framework for banks and payment operators*. <https://www.rbi.org.in>
33. Reserve Bank of India. (n.d.). *Master direction on digital payment security controls*. <https://www.rbi.org.in>
34. Sandoval, M.-P., et al. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *AI and Ethics*. <https://doi.org/10.1007/s43681-024-00668-z>
35. Sangwan, H. (2026). *Deepfakes and the criminal justice system: Legal challenges to consent, privacy, and evidence*. SSRN Electronic Journal. <https://papers.ssrn.com>
36. Shohel, R. M., Ahmed, S. S., Islam, M. M., Uddin, M. S., Mahmud, S., & Karray, F. (2022). Deepfake detection: A systematic literature review. *IEEE Access*, 10, 25494–25513. <https://doi.org/10.1109/ACCESS.2022.3154404>
37. Srikant, M. (2025). *Bharatiya laws against deepfake cybercrime: Opportunities and challenges*. Vivekananda International Foundation. <https://www.vifindia.org>
38. Vatreš, A. (2021). Deepfake phenomenon: An advanced form of fake news and its implications on reliable journalism. *Društvene i Humanističke Studije*, 6(3), 561–576. <https://doi.org/10.51558/2490-3647.2021.6.3.561>
39. Vecchietti, G., Nunes, P., Rodrigues, R., & Casais, B. (2025). Managing deepfakes with artificial intelligence: Introducing business privacy calculus models. *Technological Forecasting and Social Change*, 213, 124042. <https://doi.org/10.1016/j.techfore.2025.124042>