Journal of Intellectual Property Rights
Vol 30, September 2025, pp 583-590
DOI: 10.56042/jipr.v30i5.15633

Combating AI-Enabled Identity Theft: Strengthening Legal Frameworks in India

Saima Jan† and Anna Bashir
School of Law, University of Kashmir, Hazratbal – 190 006, India

Received: 10th December 2024; revised: 7th May 2025

The rapid advancement of Artificial Intelligence (AI) is reshaping the digital landscape. This offers both opportunities and challenges across multiple sectors, with cyber security emerging as a vulnerable domain. One growing concern is the rise of AI-enabled identity theft, which threatens the privacy and security of both individuals and institutions. India's laws on AI-enabled identity theft lack comprehensive coverage and enforcement. As a result, cybercriminals are often able to exploit these legal loopholes. This paper examines the current legal frameworks in India pertaining to identity theft. It also suggests practical steps to augment the legal frameworks to the effect of combating AI-enabled identity theft. By examining existing laws, regulations, and international best practices, this paper provides insights into the necessary legal reforms and technological interventions needed to strengthen India's capacity to address the evolving risks associated with AI-enabled identity theft.

Keywords: Artificial Intelligence, Identity Theft, Data Protection, IT Act, Digital Personal Data Protection Act, India

In today's digital age, the growth of Artificial Intelligence (AI) technology has revolutionized various aspects of our lives, including how we manage and protect our identities. AI-enabled identity theft refers to the malicious use of AI algorithms and techniques to steal, manipulate, or impersonate individual's personal information, credentials, and digital identities for fraudulent purposes. Unlike traditional identity theft methods, which rely heavily on manual processes and social engineering tactics, AI-enabled identity theft uses advanced algorithms to automate and scale attacks, making them more sophisticated, targeted, and difficult to detect. For example, an individual receives an email that looks identical to one from their bank logos, language, and even the signature match perfectly. Within hours of clicking a link, their personal data is compromised, financial accounts are drained, and their digital identity is hijacked. But behind this deception is not just a skilled fraudster, it's an algorithm. This is the reality of AI-enabled identity theft that the victims have to grapple with.This form of identity theft encompasses various techniques, including deep fake technology to create highly convincing fake identities, machine learning algorithms to analyze and exploit vulnerabilities in authentication systems, and natural language processing algorithms to generate convincing phishing emails and social engineering message.[1] India, with its expanding digital infrastructure and growing reliance on biometric and digital identity systems like Aadhaar, faces a unique and urgent challenge. The implications of AI-enabled identity theft are deepened far-reaching which affect individuals, businesses, and society at large. Victims may suffer financial losses, reputational damage, and emotional distress, while businesses may face regulatory penalties, loss of customer trust, and legal liabilities. Some measures to address cyber threats including the Information Technology Act, 2000, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and the more recent Digital Personal Data Protection Act, 2023 do exist in India. These laws have not been designed with AI-driven threats in mind. Consequently, they fall short in addressing the specific risks posed by synthetic identities, algorithmically generated attacks, and AI-based deception. The enforcement mechanisms often lack the technical capacity to keep up with the pace of AI innovation. Since AI continues to advance, the need to address AI enabled identity theft becomes imminent.

This paper seeks to analyze the current legal landscape surrounding AI-enabled identity theft in India. It evaluates existing frameworks, identifies gaps in their ability to address AI-driven crimes, and offers recommendations to strengthen these laws. By focusing on the intersection of emerging AI technologies and legal protections, this paper aims to provide actionable insights that will help India build a robust legal

†Corresponding author: Email: syedsaima144@gmail.com

infrastructure that can combat AI-enabled identity theft and ensure the security of its digital ecosystem.[2]

Techniques of AI-Enabled Identity Theft

Traditional identity theft began with methods like mail theft, dumpster diving, and simple phishing scams. Thieves would physically steal documents or trick individuals into revealing personal information through deceptive communications. As technology progressed, the tactics also changed. Cybercriminals started hacking databases and using malware to access vast personal data, leading to more efficient and large-scale identity theft operations. Social engineering also evolved, becoming more complicated with targeted attacks, often exploiting human psychology to manipulate victims.

The introduction of artificial intelligence (AI) has transformed identity theft into a more complicated andalarming threat. AI enables the automation and enhancement of traditional techniques, while also introducing new methods. One prominent technique is the creation of deepfakes and synthetic identities. AI can generate realistic video and audio mimicking real people, which can bypass biometric security and deceive individuals into believing they are interacting with a trusted person. Synthetic identities, crafted from both real and fabricated data, present significant challenges for detection.

AI has also revolutionized phishing and spear-phishing. Using machine learning and data analytics, AI can craft highly personalized and convincing phishing emails by analyzing social media profiles and other available data. This automation allows for large-scale dissemination of these tailored attacks that significantly increases their success rate. AI's data-mining capabilities feed directly into this process. It can delve deep into vast amounts of public and breached data to build detailed profiles- answering security questions, mimicking speech patterns to the level of predicting behaviors.[3] This capability enhances social engineering efforts by providing detailed knowledge to answer security questions and exploit specific vulnerabilities.

Password cracking also stands enhanced by AI. Traditional methods relied on forceful methods or simple methods, but AI can utilize deep learning system to predict passwords based on patterns and previously leaked data, reducing the time and effort needed to break into accounts. AI-powered chat bots further extend the capabilities of social engineering, engaging individuals in realistic conversations to extract sensitive information by posing as legitimate customer service representatives or other trusted entities.

Artificial Intelligence knows both when to be an offensive and when to hide. By studying what normal activity looks like on a system or network, AI can copy that behavior and blend in, making it difficult to detect. Its harmful actions are hidden within patterns that most cyber security tools are designed to trust, which makes spotting anything unusual much more challenging. This shift in tactics doesn't just make things more serious, it calls for a complete rethink of our legal and security systems. As AI starts playing a bigger role in identity theft, our ways of tackling it must be smarter and more robust.

Impacts of AI Enabled Identity Theft in India

The impact of AI-enabled identity theft in India is profound and multifaceted, affecting individuals, businesses, and the overall economy. As one of the world's fastest-growing digital economies, India is highly susceptible to cyber threats, including sophisticated AI-driven identity theft. The widespread adoption of digital services, accelerated by initiatives like Digital India, has created a vast pool of personal and financial data, making it an attractive target for cybercriminals.[4] The increased digital footprint spanning Aadhaar-linked services, mobile banking, UPI transactions, and e-governance has created a storehouse of personal data ripe for exploitation. When artificial intelligence gets weapon zed in this environment, the scale and precision of identity theft reaches alarming levels.

For individuals, the repercussions are severe. Victims of identity theft often face significant financial losses, damage to their credit ratings, and a long, difficult process of restoring their identities. The emotional toll, including stress and anxiety, is also considerable. AI-powered techniques such as deep fakes and automated phishing have made it easier for criminals to deceive individuals and gain unauthorized access to their personal information.[5] In another instance, *The Hindu* reported in 2023 that elderly pensioners in Kerala were targeted using deep fake videos of pension department officials. The videos instructed them to "verify" their identities via biometric inputs, which were then harvested and misused. These are not isolated cases they reflect a disturbing trend where AI is being used not just to impersonate, but to manipulate and deceive. The rapid growth of synthetic identities, which blend real and fictitious data, complicates the detection and resolution of such frauds.

Businesses, particularly small and medium enterprises (SMEs), are equally vulnerable. With limited budgets and expertise in cyber security, they struggle to keep up with increasingly sophisticated attacks. According to a 2022 report by the Data Security Council of India (DSCI), more than 60% of cyber-attacks on Indian Small and Medium Enterprises involved identity theft, many using AI-powered phishing or data-mining techniques.[6] In Bengaluru, a fake fintech website equipped with an AI chatbot managed to impersonate a customer support system so convincingly that it tricked users into sharing OTPs and KYC details. Losses exceeded ₹2 crore before the site was taken down.[7]

Even large corporations having dedicated IT security teams aren't immune to such phishing attacks.[8] In 2021, a major telecom company faced a breach after its employees fell for emails generated through AI-driven spear-phishing campaigns. These emails mimicked internal communication styles and included tailored references to ongoing projects, making them nearly indistinguishable from genuine messages. The breach led to exposure of customer data and sparked a formal investigation by The Indian Computer Emergency Response Team(CERT-In).

At the national scale, the economic and social ramifications are immense. A joint report by Nasscom and McKinsey (2023)[9] estimates that cybercrime which involves mostly identity theft could cost the Indian economy up to $18 billion annually by 2026. But the greater loss may be trust.If citizens begin to doubt the safety of using platforms like UPI, DigiLocker, or AarogyaSetu, the momentum India has built toward digital inclusion could slow dramatically, especially in rural and semi-urban areas.

Government programs are no exception either. The Aadhaar ecosystem is increasingly being exploited through AI-generated synthetic identities. In 2022, UIDAI acknowledged weaknesses in its system after reports surfaced of fraudulent Aadhaar numbers being used to open bank accounts and obtain loans. These were not simple forgeries but sophisticated identities built using a mix of real and fabricated data often indistinguishable from legitimate profiles.[10]

Efforts like *Cyber Surakshit Bharat* and the *Indian Cyber Crime Coordination Centre (I4C)* show that the government is aware of these threats. These initiatives need constant upgrading, as AI-based attacks evolve rapidly. Public-private collaboration, regular audits, and real-time threat monitoring must become the norm, not the exception.[11]

The impact of AI-enabled identity theft in India is significant, affecting various facets of the society and the economy. It necessitates a concerted effort from individuals, businesses, and the government to enhance cyber security measures so as to promote awareness and develops resilient systems to safeguard against these sophisticated threats.

Recent Cases of AI-Enabled Identity Theft in India

The rise of artificial intelligence has undoubtedly opened new frontiers in technology but it has also armed cybercriminals with powerful tools to deceive, manipulate, and exploit. Recent incidents across India paint a stark picture of how AI-enabled identity theft is becoming more personal, more convincing, and far more dangerous than ever before. Some of the cases are as mentioned below:

A high-profile case surfaced in Mumbai, where the city police registered a complaint against the Maharashtra Youth Congress and 16 others for circulating deep fake video of Union Home Minister Amit Shah. The video, engineered with AI to make Shah appear to say something he never did, falsely suggested that he planned to reduce reservation rights for Scheduled Castes, Scheduled Tribes, and Other Backward Classes. In reality, the original footage had Shah discussing a completely different issue the removal of Muslim reservations in Telangana. The manipulated clip sparked outrage and was widely shared online, threatening to stoke caste-based tensions. A BJP functionary, Pratik Karpe, filed the complaint, and the case is now being pursued under multiple sections of the IPC and the Information Technology Act. This incident underscores how deep fakes are no longer limited to personal scams they are entering the political arena and threatening public harmony.[12]

Sachin Tendulkar recently fell victim to a deep fake video scam, where a manipulated video featuring his likeness was circulated online. The video, which appeared to be genuine, falsely depicted Tendulkar endorsing a product. Tendulkar expressed his concern and distress over the misuse of his image, calling the incident "disturbing" and emphasizing the need for stronger regulations and public awareness to combat the growing threat of deep fakes. This incident highlights the increasing prevalence of such scams, where advanced AI technology is used to create realistic yet fake videos, potentially damaging reputations and misleading the public.[13]

A recent incident in Kerala has shed light on the increasing threat of AI-enabled scams. A 73-year-old

man from Kozhikode was tricked into transferring ₹40,000 by a deep fake fraudster. The scammer used an AI-generated video and voice to impersonate the victim's former colleague and convinced him that the money was needed for an urgent medical procedure. The funds were traced to an account in Maharashtra, and the local police are now investigating the matter.[14]

Similarly, a 59 year-old woman lost ₹1.4 lakh after receiving a distress call from what she believed was her nephew in Canada. The caller's voice distressed and familiar begged for financial help due to an accident and pending legal troubles. The caller convinced woman as it was her nephew, and the woman transferred the money without hesitation. Only later did she came to known that the voice had been synthesized using AI, part of a growing trend in voice cloning scams. Experts warn that such cons are particularly effective against older individuals or families with members abroad, playing on emotions and urgency.[15]

In other notable incident reported in December 2024, cybercriminals exploited artificial intelligence (AI)-based voice cloning technology to defraud a senior railway official's friend of ₹2 lakh. The perpetrators successfully mimicked the voice of M.L. Meena, the Director General of Railways, and contacted his friend, claiming an urgent medical emergency. The impersonation was so convincing that the victim, without suspecting foul play, transferred the funds across multiple transactions. The fraud came to light only when the recipient's phone number was verified and found not to belong to Meena. Experts, including representatives from the Cyber Peace Foundation, have expressed concern over the increasing frequency and sophistication of such AI-driven scams in India.[16]

These cases demonstrate the evolving nature of identity theft, where Artificial Intelligence technologies are exploited to create realistic, fraudulent representations, thereby deceiving individuals and the public at large. The growing prevalence of these scams calls for enhanced cyber security measures and public awareness to mitigate the risks associated with AI-enabled identity theft.

International Best Practices Combating AI- Enabled Identity Theft

Addressing AI-driven identity theft involves integrating legal, technological, and social measures that prioritize individual rights, dignity, and wellbeing. Countries such as those in the European Union, under the General Data Protection Regulation (GDPR), and Canada through the Personal Information Protection and Electronic Documents Act (PIPEDA), have set global benchmarks in data protection, granting individuals control over their personal information including rights like data portability and erasure.[17]Complementing these are AI-specific regulations such as the EU AI Act (2024), which targets high-risk AI systems by mandating human oversight, algorithmic transparency, and avenues for redress, ensuring that decisions impacting identity are never left solely to machines.[18] On the technological front, nations like Estonia have pioneered encrypted biometric e-identification systems, carefully designed with opt-out options and user consent at their core. Meanwhile, AI detection tools are being employed globally to flag fraudulent behavior like deep fakes or synthetic identity use, with jurisdictions like Singapore requiring auditability and fairness to prevent discrimination.[19] Equally important is the human-centric promotion of digital literacy. The United Kingdom's National Cyber Security Centre and Australia's eSafety Commissioner have made notable progress in educating citizens, offering multilingual, inclusive content that bridges digital divides for vulnerable groups, including the elderly and children.[20] International cooperation also plays a crucial role, with organizations like International Criminal Police Organization (INTERPOL) and European Union Agency for Law Enforcement Cooperation(Europol) forming cross-border task forces to dismantle global fraud networks, while standard-setting bodies such as International Organisation for Standardisation (ISO) emphasize privacy-by-design principles.[21] Notably, the United States contributes through institutions like the Federal Trade Commission (FTC), which provides victims of identity theft with comprehensive support offering recovery steps that are easy to follow which are emotionally supportive, and legally empowering.[22] Some European Union countries provide state funded compensation for those who suffer identity theft losses they cannot recover from acknowledging the psychological as well as financial harm involved.[23] These practices, when viewed collectively, reflect a global move toward not just technical resilience, but a compassionate and ethical response to identity theft in the age of AI.

Overview of Existing Legal Frameworks and Regulations on AI-Enabled Identity Theft in India and their Limitations

As India steps into an era increasingly shaped by artificial intelligence, the legal infrastructure meant to

protect citizens from AI-enabled identity theft remains at best, a fragmented patchwork. Instead of a unified law targeting this menace, what currently exists is a series of overlapping, sometimes outdated, statutes each trying in its own way to respond to a problem that is evolving faster than the law can keep up.[24]

At the heart of India's cyber security law is the Information Technology (IT) Act, 2000, a statute originally designed to recognize electronic transactions and facilitate digital governance. Over the years, it has been amended to address the growing spectrum of cybercrimes. Provisions like Sections 43, 66, and 66C cover unauthorized access, identity theft, and penalties for data breaches. While these provisions provide a base for prosecuting AI-driven impersonation and misuse of identity, they fall short in specificity. The Act was never crafted with AI in mind, and as a result, its language lacks the nuance to tackle sophisticated techniques like deep fakes, AI-generated synthetic identities, or voice cloning. Law enforcement agencies often try to fit modern crimes into outdated legal boxes, which can delay investigations or result in weak prosecutions. The penalties remain relatively light when compared to the severe consequences AI-fueled identity theft can impose.[25]

Another cornerstone of India's identity infrastructure is the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 which governs the use of biometric and demographic data for public services. While Aadhaar offers a seemingly robust verification system, it has often come under fire for vulnerabilities.[26]Several data breaches and cases of unauthorized access have raised concerns, especially given that AI technologies are now capable of generating fake fingerprints or spoofing iris scans. Despite strict clauses like Section 29, which prohibits the unauthorized sharing of Aadhaar data the law has struggled to keep up with the innovation of those intending to exploiting it. The rise in bank frauds linked to Aadhaar-verified accounts, often aided by AI algorithms, underscores the need for the system's continuous technological and legal strengthening.[27]

In a significant step forward, the Digital Personal Data Protection Act (DPDPA), 2023 was introduced to provide a rights-based approach to data protection.[28] While it doesn't mention AI explicitly, its emphasis on consent, data minimization, and transparency lays a foundation for reducing AI-driven misuse of personal data. Laws related to the correction of personal information and mandatory security safeguards offer a degree of control to individuals. The DPDPA still leaves open questions about government access to data, especially in the name of national security, raising concerns about unchecked surveillance capabilities. And like the IT Act, it may not yet have the teeth or the foresight to adequately grapple with the pace at which AI threats are emerging. The DPDPA has limitations, including exemptions for government use due to national security reasons, potentially creating a loophole for AI surveillance misuse. The Act may not fully anticipate the future capabilities of AI-enabled identity theft, necessitating regular reviews and updates to remain effective.[29] Overall, while the DPDPA represents progress in safeguarding data privacy in India, its efficacy depends on robust enforcement and adaptation to evolving technological landscapes.

The financial sector, too, is grappling with the implications of AI in fraud. The Reserve Bank of India (RBI), through its Cyber Security Framework and know your customer(KYC) norms, has urged banks to adopt stringent identity verification and cyber security protocols. AI has been both a threat and a tool here used by fraudsters to clone voices or documents, and by banks to detect anomalies in transactions.[30] But the regulatory rigidity can sometimes backfire. Strict compliance rules can stifle innovation or delay the deployment of newer, more secure AI-powered solutions. The limited data-sharing between institutions meant to protect privacy can ironically hamper the development of effective fraud detection models.[31]

The Payment and Settlement Systems Act of 2007 mandates robust security measures for electronic transactions, encompassing protections against AI-enabled fraud and identity theft. Banks are required to adhere to guidelines issued by the Indian Computer Emergency Response Team (CERT-In), ensuring prompt reporting and coordinated responses to cyber security incidents, including those involving AI. Collectively, these regulations aim to foster a secure banking ecosystem capable of effectively combating AI-enabled identity theft and other cyber threats.

The Banking Regulations in India, while essential for ensuring security and consumer protection, have certain disadvantages when it comes to addressing AI-enabled identity theft. Strict regulatory frameworks

can slow down the adoption of new AI technologies, causing Indian banks to fall behind global competitors. Overly prescriptive rules may stifle innovation by limiting the ability of banks to experiment with different AI-based identity solutions. Regulations that restrict data sharing between banks can hinder the development of robust AI models, which rely on large, diverse datasets to improve accuracy and effectiveness in preventing identity theft. Balancing these regulatory constraints with the need for innovation is crucial for effectively combating AI-enabled identity theft.

Even consumer rights frameworks like the Consumer Protection Act, 2019,[32] offer some recourse for victims of AI-driven scams, particularly under provisions for unfair trade practices. But these laws tend to focus more on the outcome of the fraud than the advanced techniques used to carry it out. Filing a complaint about a deep fake based scam, for instance, may not fall neatly within the law's current scope especially if the scam doesn't involve a traditional transaction or service provider.[33] While the Act may not explicitly mention AI, its provisions offer a framework for consumers to seek remedies and protection against various forms of fraud and unfair practices, including those facilitated by advanced technologies.

The existing legal frameworks in India provide some protection against identity theft but are not well equipped to handle the sophisticated methods used in AI-enabled identity theft. The absence of explicit definitions and classifications for AI-enabled identity theft in Indian law makes it difficult for law enforcement and judicial bodies to effectively prosecute such crimes.[34] Current laws were established before the widespread adoption of AI technologies, leaving gaps in addressing techniques like deep fakes and synthetic identities. Enforcement is further complicated by jurisdictional issues, a lack of technical expertise, and limited resources among law enforcement agencies.[35] The challenge is not just legislative it is also structural. Many of the agencies tasked with enforcement face a shortage of technical expertise. Cybercrime units themselves often lack access to advanced forensic tools or AI capabilities themselves, making investigations slow and patchy. The jurisdictional overlaps especially in a federal system like India's only add to the complexity, particularly in cases that cross state or even national boundaries.

What's needed is not just a revision of the laws but a reimagining of laws that are anticipatory rather than reactive, frameworks that are dynamic enough to evolve alongside technology, and enforcement mechanisms that are resourced and empowered to take on crimes that are invisible, borderless, and increasingly automated.[36]

Recommendations to Address AI-Enabled Identity Theft in India

AI-enabled identity theft poses a growing threat to individuals and organizations worldwide, with India being no exception. The rapid advancements in artificial intelligence have given rise to sophisticated methods of identity theft, such as deep fakes and synthetic identities, which current legal and regulatory frameworks are ill-equipped to handle.[37] Addressing this challenge requires a multifaceted approach encompasses legislative reforms, enhanced enforcement mechanisms, technological innovations, and increased public awareness.[38] The following recommendations are aimed to fortify India's defenses against AI-enabled identity theft, which shall help protect personal data and prosecute offenders. By implementing these measures, India can bolster its cyber security infrastructure and safeguard its citizens from the evolving risks associated with digital identity fraud.

Short Term Measures

(i) Updating of existing laws in India to recognize AI-Based identity theft. First, there is a need to amend key legislations like IT Act to include and define AI-enabled identity theft. It will help law enforcement agencies to respond effectively and tackle the menace.

(ii) Strengthen the Digital Personal Data Protection Act, 2023 by integrating provisions focused specifically on AI-related risks. This includes mandatory encryption, strict data access protocols, and stronger accountability for data handlers.

(iii) Mandate incident reporting for identity theft cases by providing requirements for organizations to report AI-driven identity theft incidents to authorities within a defined time frame. The quick reporting of the incidents can help contain damage, assist investigations and ensure transparency for those affected.

(iv) Awareness campaigns should be launched to educate individuals and organizations on how to recognize and prevent identity theft. Schools, workplaces and community groups to undertake

to recourses to make cyber security part of everyday literacy.

(v) The empowering of specialized cybercrime units, building capacity within law enforcement by equipping cybercrime cells with the right tools and training to investigate AI-related offences should be worked out. Collaborations with tech firms and academic researchers can fast-track capability-building.

(vi) Encourage immediate adoption of AI-Powered security tools by promoting the use of existing AI driven authentication systems like biometric and behavioral analytics within high-risk sectors such as banking, telecom, and healthcare.

Long Term Measures

(vii) Specific laws on Artificial intelligence crimes should be introduced that can comprehensively addresses AI misuses, including identity theft, deep fake abuse, and synthetic fraud. A standalone law will be better positioned to evolve alongside emerging threats.

(viii) Develop homegrown AI threat intelligence platforms. Invest in indigenous systems capable of detecting emerging patterns of AI-enabled fraud. These platforms could be run in collaboration with public-private stakeholders and support national threat monitoring.

(ix) Enhancing International Legal Cooperation and strengthening bilateral and multilateral cybercrime agreements to deal with cross-border cases. There should be greater cooperation with agencies like International Criminal Police Organization (INTERPOL), United Nations office on Drugs and Crime (UNODC), and data protection authorities in countries like the United States and European Union can close jurisdictional gaps.

(x) Public-Private partnerships and Innovation should be encouraged. Deeper collaboration between the government, tech companies, and academic institutions should be developed. These partnerships can support Research & Development in AI-powered identity verification tools, as well as generate shared threat intelligence.

(xi) India can draw on the experiences of countries like the United States (The California Consumer Privacy Act of 2018), European Union (General Data Protection Regulation), and Canada, where more mature frameworks exist to regulate data use and protect identities. Adopting successful global strategies to local realities will be key.[39]

(xii) Technology companies and research institutions around the world are actively working on innovative solutions to tackle identity theft. From AI-powered authentication systems to advanced biometrics and behavioral analytics, these tools are being designed to stay one step ahead of cybercriminals. In parallel, public-private partnerships, industry alliances, and cyber security forums are proving invaluable by enabling the sharing of threat intelligence and best practices.For India, there's a valuable opportunity to learn from international regulatory frameworks like the General Data Protection Regulation in the EU or The California Consumer Privacy Act of 2018 in the US. Strengthening our own data protection laws with these lessons in mind could help bridge current gaps. At the same time, collaboration with global organizations and tech industries will be not just for exchanging information, but also for developing a unified approach to combating AI-enabled threats.

(xiii) India should invest in homegrown cyber security solutions that are tailored to its unique challenges. Encouraging innovation in AI technology, supporting startups, and building research ecosystems can go a long way. No strategy is complete without empowering citizens. Promoting digital literacy and raising awareness about cyber security must be a national priority so that individuals, too, can play an active role in protecting their identities in the digital age.

Conclusion

AI-enabled identity theft is a significant and evolving threat in India, exploiting advanced technologies to steal personal information and commit fraud. Current legal frameworks are insufficient to address the complexities of AI-enabled identity theft, and enforcement mechanisms and cyber security capabilities are inadequate, resulting in low detection and conviction rates. Technological solutions like biometrics block chain and AI-driven authentication offer promising avenues for enhancing identity theft prevention and detection. To combat this threat, it is crucial to introduce specific legal provisions for AI-enabled identity theft, enact new legislation for

emerging cyber threats, impose stricter penalties, and enhance enforcement capabilities through specialized cybercrime units and international collaboration. Policymakers, law enforcement agencies, and technology stakeholders must collaborate to strengthen legal frameworks, increase funding, and invest in AI-driven technologies. Public awareness campaigns and cyber security training are essential to educate individuals and organizations about the risks and preventive measures thereof. By taking collective action and implementing these measures, India can enhance its cyber security resilience, protect individual's identities, and build a secure digital ecosystem.

References

1 Mathew A, Cybercrime as a service & AI-enabled threats, *International Journal of Computer Science and Mobile Computing*, 12 (1) (2023) 28.
2 Chakraborty A, Biswas A & Khan A K, *Artificial Intelligence for Cybersecurity,* (Edited by ChakrabortyA), 2023, 231.
3 Ateefa Rehan S, A Study of AIoT in Detecting Social Engineering Attacks: Phishing and Identity Theft*, International Journal of Data Science and Advanced Analytics*, 4 (1) (2022).
4 Ishaq Azhar M, the Impact of AI on identity and access management: An empirical analysis, *International Journal of Creative Research Thoughts*, 3 (1) (2015) 668.
5 Ibrahim Suleiman Al Qatawneh *et al*., Artificial intelligence crimes, *Academic Journal of Interdisciplinary Studies,* 12 (2023) 143.
6 Data Security Council of India (DSCI) Report, (2022).
7 Cyber Safe India Case Brief, (2022).
8 Arunachalam P, Economic impact of identity theft in India: Lessons from western countries, *3rd International Conference on Information and Financial Engineering,* 12 (2011).
9 Nasscom-McKinsey Cyber security Outlook (2023).
10 UIDAI Annual Report, (2022).
11 Suzie D, Identity manipulation: Responding to advances in artificial intelligence and robotics, (2020).
12 https://economictimes.indiatimes.com/news/elections/lok-sabha/maharashtra/amit-shah-deepfake-video-case-registered-against-maharashtra-youth-congs social-media-handle/article-show/109722406.cms (accessed on 6 May 2025).
13 https://www.ndtv.com/india-news/sachin-tendulkar-deepfake-video-disturbing-to-see-sachin-tendulkar latest-victim-of-deepfake-4866196 (accessed on 6 May 2025).
14 https://www.hindustantimes.com/indianews/deepfake-scammers-trick-indian-man-into-transferring money-police-investigating-multi-million-rupee-scam-101689622291654.html (accessed on 28 June 2023).
15 https://www.indiatoday.in/technology/news/story/he-sounded-exactly-like-my-nephew-woman-loses-rs-14-lakh-in-ai-voice-scam-2463939-2023-11-17 (accessed on 6 May 2025).
16 https://timesofindia.indiatimes.com/city/ranchi/ai-voice-cloning-scam-railway-dgs-friend-loses-2-lakh-to-cybercriminals/ article show/116661144.cms (accessed on 6May2025).
17 Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016, (General Data Protection Regulation), Official Journal of the European Union, 2016.
18 Proposal for European Parliament and Council of EU laying down rules(Artificial Intelligence Act), 2024.
19 Infocomm Media Development Authority, Singapore, (Model AI Governance Framework Updated 2020).
20 National Cyber Security Centre (UK), Cyber Aware and eSafety Commissioner (Australia), Digital Literacy Resources.
21 INTERPOL & Europol Joint Reports, Tackling Identity Crime in the Digital Age, 2022.
22 Federal Trade Commission (FTC), Identity Theft gov.
23 Germany's Victim Compensation Act allows for compensation when identity theft results in personal harm beyond financial loss.
24 Annappa N, Cybercrime regulation through laws and strategies: A glimpse into the Indian experience, *International Journal of Digital Law*, 53 (1) (2020).
25 Government of India, *The Information Technology Act, 2000,* Ministry of Law Justice and Company Affairs, Legislative Department, *The Gazette of India*, 2000.
26 Ministry of Law and Justice (Legislative Department), *TheAadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*, THE GAZETTE OF INDIA (2016).
27 Vijayaprasad G, Ethical challenges of digital health technologies: Aadhaar, India, *Bull World Health Organisation,* 98 (2020) 277.
28 Ministry of Law and Justice (Legislative Department), *The Digital Personal Data Protection Act, 202*3, The Gazette of India (2023).
29 Chanlang Ki B, Reviewing the privacy implications of India's Digital Personal Data Protection Act, *DESIDOC Journal of Library & Information Technology,* 44 (1) (2024) 50.
30 Manvi G & Ayush G, Cyber security frameworks in India, *Journal of Bussiness Management and Information Systems,* 12(1) (2025).
31 Geethanjali N & Ashwani, Banking sector regulation in India: Overview, challenges and way forward, *Indian Journal of Public Administration*, 64 (2018).
32 The Consumer Protection Act, 2019, (The Gazette of India).
33 Ramesh S, A Comparative analysis of Consumer Protection Act 1986 and Consumer Protection Act 2019 in India: Strengthening consumer rights and redressal, *Journal of Legal Subjects,* (2023).
34 Deepti M, Comparative analysis of cyber security laws of India United States and United Kingdom, *International Journal of Law,*9 (6) (2023) 88.
35 Manjula R &Sanjana Sharma M, Indian legal framework on the right to privacy in cyberspace-issues and challenges, *Fiat Justisia; Jurnal Ilmu Hukum*, 17 (1) (2023) 1.
36 Animesh S, Roshmi S &AmlanJyoti B, A brief study on cyber crime and cyber laws of India, *International Research Journal of Engineering and Technology*, 4 (6) (2017) 1633.
37 Sonia Grewal M, Identity theft as the most pervasive form of cyber crime: Its socio-legal implications on the Indian society, *Webology,* 18 (3) (2021) 562.
38 Widya Setiabudi S, Cybercrime and global security threats: A challenge in international law, *Russian Law Journal,* 11 (3) (2023).
39 Saleem M, Board of Advisors, Honorary Member, Member Supreme Court of Fiji Bihar Human Rights Commission Registrar, IAMC Hyderabad, *Journal of Unique Laws and Students,* 2 (2022).