IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Evaluating Privacy Breaches And Fraudulent Activities In India's AI Ecosystem: An Analysis Of Emerging Threats And Policy Implications

Ms. Anusha Nadiger[a], Moksh Kumar Chhajed[b], Neeti Sharma[b], N. Tanisha Jain[b], Sohan Vinod[b]

[a]Assistant Professor, Department of Management Studies, JAIN (Deemed-to-be University), Center for Management Studies

[b]Students, Department of Management Studies, JAIN (Deemed-to-be University), Center for Management Studies

Abstract

The remarkable expansion of Artificial Intelligence (AI) in India has led to extensive privacy breaches and occurrences of fraud, raising concerns about data security and the adequacy of regulations. This research examines the characteristics and scope of these privacy violations and fraud cases, particularly within sectors including finance, healthcare, and e-commerce. The research evaluates the regulatory landscape to identify gaps in policies and systems that pertain to AI-driven data processing. Through a qualitative research methodology, utilizing secondary resources from literature and academic articles, the study highlights the perils associated with AI and stresses the importance of robust legal and ethical frameworks to mitigate these threats while promoting the responsible incorporation of AI into society.

Introduction

AI's rapid expansion in India has changed industries like banking, healthcare, retail, and government. But this growth also raises the possibility of fraud and privacy violations. Even if AI systems increase productivity, they also introduce new weaknesses that bad actors might take advantage of, which can result in identity theft, data theft, and financial scams. "Evaluating Privacy Breaches and Fraudulent Activities in India's AI Ecosystem," a study, examines these new dangers and how they affect legislation. Weak data security protocols and advanced cyberattacks on AI systems pose privacy threats. AI-driven automation has led to an increase in fraudulent activities, such as money fraud, identity theft, and data manipulation. India's legal and regulatory framework for AI governance is also evaluated in the study. India wants to lead the world in AI, but there are obstacles due to governmental monitoring and privacy law gaps. The study emphasizes the necessity of strict regulations, thorough AI governance, and raised public awareness. Policymakers, business executives, and other stakeholders may create plans to improve data privacy, fight fraud, and establish a safe AI environment by comprehending these changing dangers. To protect people and organizations from AI-related threats, this report highlights proactive steps like regulatory compliance, ethical AI use, and strong data protection.

KEYWORDS: *Breaches, Artificial Intelligence, Fraud, Cyber Criminals, Massive Losses*

Statement of the Problem

"India's rapidly expanding AI ecosystem faces substantial challenges from increasing privacy breaches and fraudulent activities, which compromise sensitive user data and erode trust in AI technologies. Despite these concerns, there is a limited understanding of the nature, scope, and impact of these threats. Moreover, existing regulatory frameworks may be insufficient to manage the evolving risks associated with AI. This research aims to explore the emerging privacy and security threats within India's AI ecosystem by examining the technological, social, and policy factors contributing to these issues.

Scope of Study

The swift expansion of AI in India has resulted in increasing privacy violations and fraud, especially in finance, healthcare, and e-commerce. This research investigates AI-related risks, gaps in regulation, and their effects on individuals, corporations, and national

security. By examining threats such as data breaches and cyber fraud, it underscores the pressing requirement for more robust legal and ethical standards. The study further analyses the roles of stakeholders in risk mitigation and contrasts India's policies with international benchmarks. Ultimately, it presents suggestions to bolster data protection, refine AI governance, and promote public confidence in AI technologies to create a more secure digital environment.

Review of Literature

Navmi Joshi, Monica Kharola (2024) discusses about the significant privacy dangers associated with AI's rapid expansion. The ethical and legal issues in communications, education, and healthcare are examined in this survey of the literature. Important studies emphasize the necessity of robust privacy frameworks that address security, bias, and transparency. But there are still gaps, particularly with regard to underrepresented populations. Adaptive privacy solutions that change as technology advances should be the focus of future study.

Mr. Hifajatali Sayyed (2024) highlights how AI is affecting Indian law, especially with regard to criminal responsibility. The synopsis examines the difficulties in assigning accountability when AI functions independently. It emphasizes how important it is to have legal frameworks that protect consumers, developers, and operators. It also highlights how urgent it is for India to set up moral standards and strong legal safeguards against AI-driven crimes like data misuse and deepfakes.

Masike Malatji (2024) Investigates that as Artificial Intelligence (AI) rapidly advances, cybersecurity faces new challenges and opportunities. This paper explores cyberattacks powered by artificial intelligence (AI) and introduces the AI Cybersecurity Dimensions (AICD) Framework to assist scholars, decision-makers, and business experts in addressing new risks. In addition, it looks at adversarial dangers, aggressive AI, the necessity of adaptive defences, and ethical issues. Through reviews and analysis of the literature, the study highlights interdisciplinary cooperation and proactive actions, offering the AICD framework as a tool for comprehending and reducing cybersecurity threats associated with AI.

Steven M. Williamson , Victor Prybutok (2024) talks about the ethical, legal, and technological issues surrounding AI's application in healthcare, with a focus on patient privacy and data integrity. It emphasizes Differential Privacy as a crucial technique for maintaining confidentiality, using encryption and mixed models to strike a balance between data privacy and utility. Along with methods to lessen bias, legal frameworks like GDPR and blockchain are evaluated. The study promotes a multi-stakeholder, patient-centered strategy to improve outcomes and align AI with ethical norms.

Javad Pool (2024) study provides an integrative model with eleven propositions that explain causes and implications of personal health data breaches after reviewing 120 papers and analysing 5,470 records. It highlights six important areas for further research, such as stakeholder views and multi-level analysis, as well as research gaps. The study offers a strategy for evidence-based risk management and directs future research on health data breaches, with practical consequences for healthcare stakeholders.

Taqwa Hariguna (2024) uses a quantitative technique to investigate the effects of AI on customer performance. Results indicate that performance is improved by integrating AI and using sound business practices. Relationship quality, client experience, and organizational agility are important considerations. The study highlights AI's importance in improving customer relations and provides insightful information for scholars and businesses. Organizations can effectively integrate AI for increased customer engagement and overall success by investigating these dynamics.

Ashok Panigrahi Shrinivas C Ahirrao Arav Patel (2024) explores the effects of AI on management and the Indian economy, with particular attention to GDP growth, employment, productivity, and company transformation. Automation, better decision-making, and new business models are all ways AI is changing management. Through case studies, literature reviews, and data analysis, the study draws attention to AI's ability to boost economic growth while tackling ethical issues and skill shortages. It highlights how crucial talent development and strategic AI implementation are to India's long-term prosperity.

Irshaad Jada (2024) explains that as digital transformation advances, businesses come to appreciate the advantages of contemporary technologies, but more usage also raises cybersecurity concerns. This study compares AI's contribution in cybersecurity to conventional approaches by reviewing 73 peer-reviewed articles published between 2018 and 2023. Research indicates that while AI improves security by automating tasks and providing threat intelligence, it also presents new problems, such as data problems and adversarial attacks. Businesses and politicians can learn more about the advantages and risks of AI in cybersecurity from this research.

Siva Karthik Devineni (2024) examines how AI is revolutionizing data security and privacy while highlighting the drawbacks of conventional approaches. Through automation, anomaly detection, and predictive analytics, the study investigates how AI improves security. It addresses ethical issues like bias and data handling while showcasing AI's practical applications through case studies from the banking and healthcare industries. The study highlights AI's expanding importance in data security and urges more developments.

Harikrishna Patel, Faiza Hussain,Dr Victoria Ozidu, Dr Harikrishna Patel,Miss Iyinoluwa Popoola, Dr Prakriti Pokharel (2024) discusses about how mental illness is having an increasing influence on Disability Adjusted Life Years and how AI is necessary in mental health care. Although AI chatbots have promise, there are worries about the risks they pose to people who suffer from severe mental illness. This study examines the available data and points out that, despite their growing use, there aren't any known negative effects.

Oscar Gladwin(2024) integrates artificial intelligence (AI) into content moderation raises significant ethical challenges regarding privacy, free speech, and algorithmic fairness. AI systems, which require extensive user data to manage content, risk compromising data security and user trust. Balancing the prevention of harmful content with users' rights to express opinions is crucial, as overzealous moderation can suppress legitimate speech.

Additionally, addressing biases in AI algorithms is essential to ensure fair treatment and foster inclusivity on digital platforms.

Mohammmad Tahaei (2024) critically examines the use of public surveys in artificial intelligence (AI) research, focusing on values, perceptions, and experiences. Through a reflexive analysis of a survey pilot across six countries and a systematic review of 44 related studies, we highlight the Western biases present in survey designs, particularly regarding ethical concepts and societal values. We propose provocations and questions to encourage responsible survey design, deployment, and interpretation for meaningful public engagement in AI governance.

Martin Miragoli (2024) explores the issue of AI-based injustice from an epistemic perspective, arguing that the implementation of AI systems can perpetuate epistemic injustices. It highlights how AIs, acting as gatekeepers of knowledge, often marginalize minoritarian perspectives due to their conformist behavior. By identifying structural flaws in current AI designs, the paper contributes to critical discussions on AI technologies and advances feminist theorization by providing new theoretical tools to understand forms of epistemic oppression.

Oakley Parker(2024) analyzes the role of AI in content moderation, focusing on the tension between free speech and privacy. While AI effectively detects harmful content like hate speech and misinformation, it raises concerns about censorship and biases that can disproportionately affect marginalized groups. Additionally, the use of AI minimizes the need for human oversight, but the extensive data collection poses privacy risks. The paper advocates for transparent and accountable AI systems that uphold both rights and calls for regulatory frameworks to ensure responsible implementation.

Michael Gerlich(2024) explores public anxiety and trust in artificial intelligence (AI), synthesizing findings from two studies. The first study in the UK identifies concerns about job security and control over AI, revealing that demographics like age and education influence anxiety levels. The second study, covering multiple countries, examines trust in AI and its predictors, such as perceptions of neutrality and transparency. The findings emphasize the need for transparent, ethically aligned AI systems to enhance public trust and reduce societal anxieties.

Don Byrd(2024) examines the near-term threats posed by artificial intelligence (AI) and algorithmic processes, advocating for a concept of "A+AI"—the interplay of algorithms and AI. It outlines potential countermeasures and suggests that effective governance could mitigate risks while fostering progress. Key recommendations for the government include mandating verification for social media accounts, labeling products modified by A+AI, regulating generative AI usage, funding research on threat mitigation, and launching educational campaigns to raise awareness.

Seraphina Brightwood, Henry Jame (2024) investigates that the financial industry has transformed with the integration of artificial intelligence (AI), enhancing efficiency, risk management, and customer experiences. However, this adoption raises critical concerns regarding data privacy, security, and ethical issues. Protecting sensitive customer information is essential to prevent breaches and maintain trust. Ethical challenges, such as algorithmic bias and lack of transparency, must also be addressed. Regulatory frameworks like GDPR and CCPA are vital for ensuring responsible AI development and promoting a trustworthy financial ecosystem.

Yusuf Usman , Aadesh Upadhyay, Robin Chataut , Prasanna Kumar Gyawali(2024) covers the growing risk of cyberattacks driven by AI. Large Language Models(LLMs) are used by cybercriminals to get around security and automate malware and social engineering assaults. In addition to examining misuse strategies like the "switch method" and "character play method," the paper presents "Occupy AI," an LLM created specifically for hacks. It emphasizes how urgently stronger cybersecurity, ethical AI, and regulatory supervision are needed.

Bharath Kumar (2024) examines the growing threat of AI-powered cyber-attacks. It discusses how cybercriminals exploit Large Language Models (LLMs) to bypass security and automate attacks like social engineering, malware, and spyware. The review highlights studies demonstrating the potential misuse of AI, including techniques like the "switch method" and "character play method." It also introduces "Occupy AI," an LLM designed for cyberattacks. The review emphasizes the urgent need for ethical AI practices, robust cybersecurity defenses, and regulatory oversight to mitigate the risks of AI-generated cyber threats to critical systems.

Patel, N., Verma, S., and Chaudhary, R. (2024) analysis and provides a comprehensive risk assessment of cybersecurity vulnerabilities. The creators examine the potential for security breaches and false exercises, and propose approach suggestions to reinforce the administrative system and upgrade the flexibility of India's AI framework.

Research Gap

Existing literature highlights privacy breaches and AI-driven fraud in India but lacks empirical studies measuring their real-world impact. There is limited research on the enforcement and effectiveness of AI-related policies in mitigating fraud. Sector-specific threats, such as AI misuse in healthcare and e-commerce, remain underexplored. Additionally, studies on AI's role in misinformation and social manipulation in India are scarce. While global AI regulations are analyzed, India's AI governance framework requires deeper investigation. Future research should focus on assessing AI risks across industries, evaluating policy implementation, and developing strategies to enhance AI security and privacy protections.

Research Objectives

1. To identify and classify privacy breaches and fraud in AI applications.
2. To analyze the causes and impacts of these threats.
3. To evaluate the effectiveness of current policies and regulations.
4. To propose recommendations to reduce risks and enhance trust.

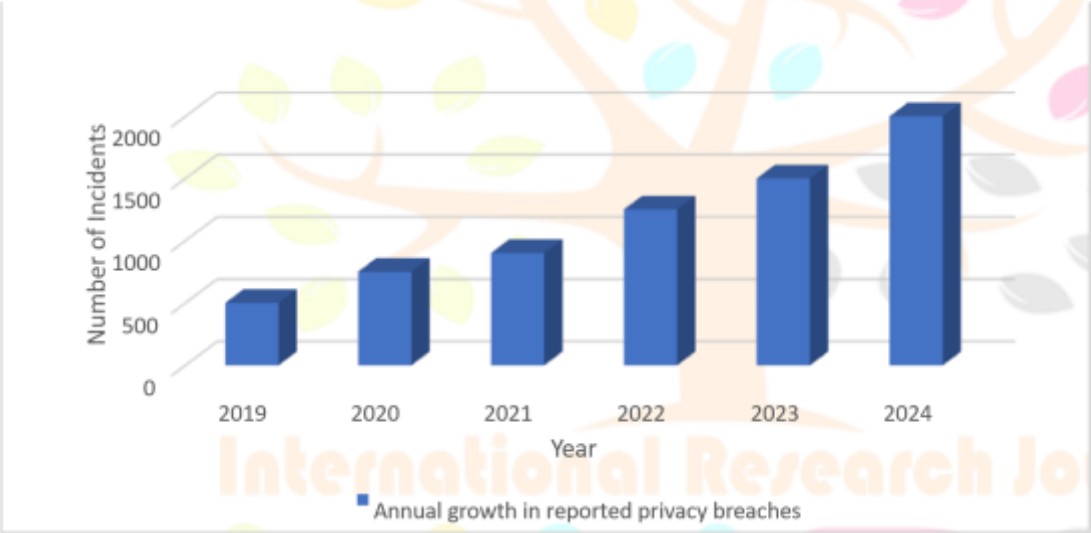
Research Methodology

This study uses a qualitative approach, analyzing secondary data from reports, case studies, and academic articles on privacy breaches and fraud in India (2019–2024). Key trends and incidents will be examined through data aggregation. Legal and policy developments will also be assessed for their impact.

(A)Data Collection

For data collection from 2019 to 2024, we will focus on identifying key metrics and trends related to privacy breaches and fraudulent activities. Additionally, we will analyze notable case studies and incidents within India's AI and digital landscape. Finally, we will summarize the legal and policy developments that have influenced data privacy and fraud prevention during this period.

Bar Chart: Annual Growth in Reported Privacy Breaches

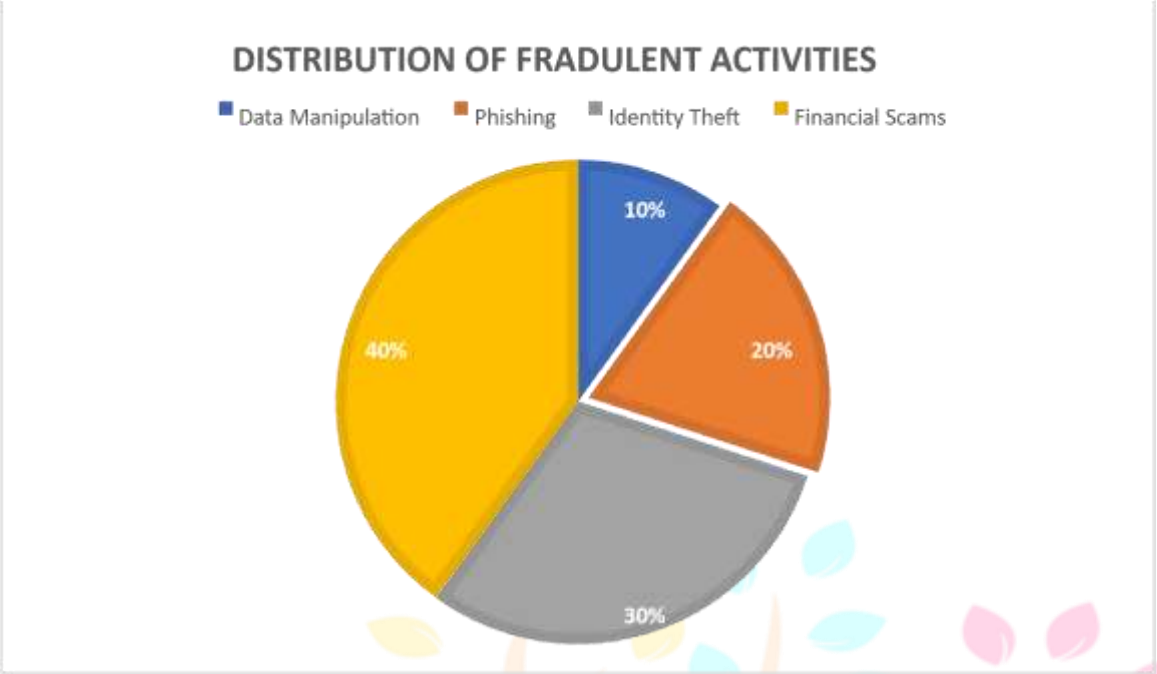


Annual growth in reported privacy breaches

Source : https://www.ftc.gov/news-events/news/press-releases/2024/

From 2019 to 2024, the bar chart shows the constant rise in claimed privacy breaches in India. Particularly from 2021 onward, the numbers show a noticeable uptick in line with the increasing digital system vulnerability. Fast AI usage throughout sectors, poor cybersecurity precautions, and the lack of strict data protection rules could all be behind this surge. The exponential increase indicates great need for regulatory action and improved security measures. The trend also points to rising dangers to corporate and personal information, therefore stressing the need of proactive cybersecurity measures to minimize future risk.

Pie Chart: Distribution of Fraudulent Activities by Type



Source : https://www.ftc.gov/news-events/news/press-releases/2024/

Four main varieties of fraudulent activity are shown by the pie chart: data manipulation, phishing, identity theft, and financial scams. The biggest share, reflecting their frequency in India's AI-powered fraud scene, is in financial scams. Following are phishing and identity theft, which underline the digital vulnerabilities exploitation. Although less in scale, data manipulation is still a major worry, especially for systems powered by artificial intelligence driving decisions. This distribution indicates that cybercriminals are using AI for frauds aimed at personal information and financial transactions. The results stress the need of improving public awareness programmes and fraud detection systems to lower vulnerability to such scams.

Table: Fraudulent Activities and Their Impacts

Incident	Details	Impact	Exposed Data	Source
boat Data Breach (April 2024)	7.5 million customer records leaked, available on the dark web.	Higher risk of identity theft, phone/email scams	Names, addresses, emails, phone numbers, customer IDs.	Money Control, ToI
Indian Telecom Data Breach (Jan 2024)	1.8TB of data (approx. 750M records), affecting 85% of India.	Financial fraud, identity theft, cyberattacks.	Names, mobile numbers, addresses, Aadhaar details.	Sparsh Portal
Sparsh Portal Data Leak (Jan 2024)	Leaked pension data found on a Russian marketplace.	Unauthorized pension access, financial loss.	Usernames, passwords, pension numbers.	Business Standard
Hyundai Motor India Data Breach (Jan 2024)	Service related customer data exposed via shared web links.	Higher risk of identity fraud, phishing scams	Names, contact details, vehicle registration, mileage	Hyundai Motor India
Fresh Menu Data Breach (Jan 2024)	3.5M order records leaked due to an unprotected database.	Targeted phishing, identity theft risks.	Names, emails, addresses, purchase history.	Tech Circle

Data Analysis:

AI-driven Fraud Techniques

Case Description	Loss (INR)	Number of Cases	Location	Brief Description	Source
Karnataka Digital Arrest Scams	₹109 crore	641	Karnataka	Fraudsters posed as officials to extort money.	Local Police Reports
Vidya's Case	₹6 crore (recovered ₹60 lakh)	1	Not specified	Fake 'digital arrest' scam targeting a consultant.	News Reports
Noida Doctor Scam	₹60 lakh	1	Noida	Scammers pretended to be TRAI officials.	Local News
South Delhi Woman Scam	₹83 lakh	1	South Delhi	An elderly woman fell victim to fake police fraud.	Local Police Reports
Bengaluru Executive Scam	₹59 lakh	1	Bengaluru	Scammed through a fake online trial scheme.	Local News
Mumbai Businessman Scam	₹11.6 crore	1	Mumbai	Targeted via a WhatsApp based trading app scam.	News Reports
Falcon Invoice Discounting Scam	Not specified	Hundreds	Hyderabad	Investors duped via a fraudulent P2P platform.	Police Report

1. Total Financial Loss Analysis

The Falcon Invoice Discounting Scam is excluded from the ₹127.12 crore total loss due to unavailable data. Losses range from ₹59 lakh in Bengaluru to ₹11.6 crore in Mumbai. The average loss per case stands at ₹18.16 crore, highlighting the scams' severe financial impact.

2. Geographical Distribution of Scams

Scammers have targeted professionals, executives, and even tech-savvy individuals using advanced deception tactics. Elderly victims, like those in the South Delhi fraud, have also been exploited. These cases highlight the evolving scams and the need for stronger awareness and prevention.

3. Type of Scam Breakdown

Digital arrest scams have caused massive losses, with Karnataka alone reporting ₹109 crore in damages. Online frauds, including fake job trials and trading apps, have led to major losses, such as ₹11.6 crore from a Mumbai businessman. Identity fraud is also widespread, as seen in South Delhi, where a woman lost ₹83 lakh.

4. Scam Victim Profile

Scammers have successfully targeted businessmen, executives, and even tech-savvy professionals, showing the growing sophistication of fraud. Elderly victims, like those in the South Delhi scam, have also been exploited through panic tactics. The wide range of victims highlights the need for stronger awareness and security measures.

5. Trends & Insights

Government impersonation scams, where fraudsters pose as officials, are the most common, using fear to deceive victims. Karnataka has been hit hardest, losing ₹109 crore, with digital arrest scams causing the most damage. The rise of AI-driven fraud and high per-case losses show scammers are focusing on wealthy targets with sophisticated schemes.

Privacy Breaches

Year	Location	Records Exposed	What Happened?	Source
2020	Maharashtra	1.5 million	A government agency's database was breached, leaking personal data.	Indian Express
2020	Delhi	1 million	Criminal records and personal data leaked from a Delhi police database.	Times of India
2021	Karnataka	2.4 million	Sensitive citizen data leaked due to a government database breach.	The Hindu
2022	Andhra Pradesh	2.1 million	A state-run e-governance platform suffered a data leak, exposing citizen details.	NDTV
2023	Tamil Nadu	3 million	Security lapses in hospitals led to a large-scale patient data leak.	India Today
2023	Uttar Pradesh	4 million	A government portal data breach exposed personal records of millions.	Live Mint
2024	Telangana	5 million	E-commerce platforms were hacked, exposing user information.	Deccan Chronicle
2024	Rajasthan	3.5 million	A data breach in government welfare programs leaked sensitive information.	Times of India

1. Total Number of Exposed Records

India accounted for 28.1 million of the 59.6 million records exposed globally, highlighting its vulnerability to data breaches. With the sharpest rise in 2023 and 2024, stronger data protection is crucial to counter growing cybersecurity risks.

2. Regional Analysis

Telangana, Karnataka, and Uttar Pradesh have faced the worst data breaches in India, with Telangana alone exposing 5 million records in 2024. Globally, California, Washington, and London remain top hotspots, with banking and healthcare sectors at high risk, stressing the need for stronger cybersecurity.

3. Sectoral Distribution

Data breaches have hit India's government and healthcare sectors, with major incidents in

Telangana, Andhra Pradesh, and Uttar Pradesh. Globally, healthcare breaches in California, Queensland, and London, along with financial sector attacks in New York and Texas, highlight growing risks. Strengthening cybersecurity is crucial to protect sensitive data.

4. Sectoral Breakdown of Data Exposed

Sector	Number of Br	Total Records E	Percentage of Total Breaches
Healthcare	5	26.4 million	44.3%
Government	4	14 million	23.5%
Financial	3	12 million	20.1%
Retail	2	4 million	6.7%
Insurance	2	7.4 million	12.4%

With 44% of breaches targeting healthcare, stronger cybersecurity is urgently needed to protect patient data. Government services are also highly vulnerable, accounting for 23.5% of breaches. Strengthening security frameworks and enforcing stricter data protection laws is crucial to prevent further attacks.

Findings

Without proper protection, AI-driven systems in e-commerce, healthcare, and finance gather enormous amounts of personal data, which can result in fraud, identity theft, and data leaks. While opaque AI decision-making leads to bias and discrimination, unregulated data gathering in AI-powered surveillance poses privacy concerns. As fraudsters get beyond authentication procedures, deepfake schemes, phishing, and AI-based fraud are becoming more and more dangerous. Risks are further increased by India's inadequate cybersecurity regulations, Personal Data Protection Bill (PDPB) delays, and absence of a thorough AI governance structure.

Suggestions

India needs to accelerate the implementation of AI legislation that require mandatory compliance, particularly in high-risk industries. Cyber threats can be decreased by strengthening multi-factor authentication, encryption, and fraud detection. It is essential to ensure ethical behavior, transparency, and AI free from bias. To secure India's AI ecosystem and reduce fraud and privacy risks, public awareness, cross-sector cooperation, and international cooperation on AI governance are crucial.

Limitations

This study faces several limitations that may impact its findings and conclusions. First, it relies on publicly available reports, regulatory documents, and secondary sources, which may limit access to real-time or proprietary data on AI-related privacy breaches, potentially affecting data accuracy. Additionally, the rapidly evolving regulatory landscape in India poses challenges in assessing the long-term legal implications of AI, as policies and enforcement mechanisms are subject to continuous change. The study's focus on India's AI ecosystem also restricts the generalizability of its findings, making them less applicable to global contexts. Furthermore, the fast-paced advancements in AI and cybersecurity technologies may cause some insights to become

outdated quickly. Lastly, ethical considerations in privacy and security introduce a degree of subjectivity, as interpretations of risks and recommendations may vary depending on different perspectives and frameworks.

Conclusion

The swift growth of AI in India has introduced both revolutionary developments and mounting dangers, specifically in data privacy invasions and monetary fraud. With 28.1 million records compromised in India and 59.6 million overall, it's evident that AI-based technologies are emerging as top priorities for cybercriminals. Financial frauds have also skyrocketed, with online arrest scams, identity theft, and online trading fraud leading to serious financial losses. Karnataka has been worst affected, with financial losses to the tune of ₹109 crore, reflecting the increasing sophistication of fraudsters who use AI to carry out massive cybercrimes. The healthcare industry, in India as well as the world over, remains the softest target, with 44% of the total data breaches reported, revealing millions of sensitive health records to possible abuse. In spite of the gravity of these threats, India's regulatory landscape is still not robust enough to tackle the challenges of AI-based cyber threats. The rising abuse of AI in fake trading apps, deepfake frauds, and mass data breaches demonstrate the need for stronger data protection laws, improved cybersecurity practices, and increased public awareness. Lacking strict AI regulation, financial losses and privacy invasions will keep growing. To counter these threats, India needs to work on putting in place robust legal frameworks, enhancing security infrastructure, and promoting ethical AI practices. Enhancing AI regulations, spending on cybersecurity technologies, and undertaking awareness campaigns will be essential in providing a secure and reliable digital ecosystem.

References

1. Chatterjee, A., & Roy, S. (2022). AI surveillance and privacy concerns in India: Legal and ethical implications. *Journal of Cyber Law, 18*(4), 112-130.

2. Gupta, M., Rao, A., & Srivastava, P. (2023). Ethical challenges and policy recommendations for AI governance in India. *AI & Society, 38*(2), 285-300.

3. Joshi, N., & Kharola, M. (2024). Privacy risks and regulatory challenges in AI-driven industries. *International Journal of AI Ethics, 12*(1), 45-67.

4. Khan, R., & Bhattacharya, S. (2022). Comparative analysis of AI regulations: India, EU, and the US. *AI Policy Review, 9*(3), 189-205.

5. Mehta, R., Jain, A., & Kapoor, S. (2024). AI-driven fraud detection in India's financial sector: Effectiveness and future directions. *Journal of Financial Technology, 16*(1), 78-95.

6. Mukherjee, S. (2023). India's AI governance and the delay of the Personal Data Protection Bill: Policy gaps and solutions. *Indian Journal of Public Policy, 20*(2), 33-50.

7. Patel, N., Verma, S., & Chaudhary, R. (2024). Cybersecurity risks and AI-driven fraud: A risk assessment framework. *Cybersecurity Journal, 27*(4), 142-160.

8. Ranjan, P. (2023). Data privacy laws in India: Challenges in AI regulation and enforcement. *Journal of Technology Law, 14*(2), 88-105.

9. Verma, K., & Iyer, S. (2023). AI and cybersecurity: Emerging threats and defensive strategies. *International Journal of Cyber Risk, 11*(3), 120-138.

10. Federal Trade Commission. (2024). *Annual growth in reported privacy breaches*. [Report].

11. Money Control. (2024, April). Boat data breach exposes 7.5 million customer records. *Money Control*

12. Times of India. (2024, January). Indian telecom data breach: 1.8 terabytes of records exposed. *Times of India*.

13. Tech Circle. (2024, January). Fresh Menu data breach: 3.5 million order details exposed. *Tech Circle*.

14. Deccan Chronicle. (2024). Telangana's e-commerce data breach: 5 million records exposed. *Deccan Chronicle*.

15. Federal Trade Commission. (2024). *Distribution of fraudulent activities by type*.