The International Journal of Indian Psychology
ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print)
Volume 13, Issue 2, April- June, 2025
DIP: 18.01.269.20251302, DOI: 10.25215/1302.269
https://www.ijip.in

Review Paper

Artificial Intelligence Threats to Indian Public and Private Organizations: A Systematic Review

Rahul Surawat[1]*, Sandeep Kumar[2]

ABSTRACT

Artificial intelligence is a lifeline for government and commercial organizations in today's technologically advanced world. Artificial Intelligence has completely taken over the lives of working professionals, organizational policies, and work culture; however, it has become a threat to Indian public and private organizations. We addressed this problem by conducting a systematic literature review to illuminate the Artificial Intelligence Threats to Indian Public and Private Organizations. Systematically review empirical published English language articles from April 8, 2015, to April 8, 2025, in Scopus, Web of Science, PsycNet, PubMed, and a random Google search using the appropriate filter. Twenty research studies remained after applying inclusion and exclusion criteria to the identified eight hundred ninety-five publications. The present study formulates nine major themes such as cybersecurity vulnerabilities and fraud in financial institutions, privacy, security, and surveillance-related threats in the workplace, systemic weaknesses in cyber threat response, threats of fake news and misinformation, ethical challenges and legal gaps amplify threats for governance, socioeconomic exclusion due to cybersecurity threats, cybersecurity threats promote bias, exclusion & structural inequality, human resource & skill deficiencies, organizational readiness and resistance. The findings from this research express deep concern about the Indian public and private organizations, to analyze artificial intelligence threats, to understand the pros & cons of artificial intelligence threats, & to use protective and defensive strategies against artificial intelligence threats in the workplace.

Keywords: *Artificial Intelligence, Cybersecurity, Privacy, Threats, Governance*

In India, artificial intelligence is becoming increasingly crucial for decision-making, service delivery, and efficiency in both the public and private sectors. Its quick adoption does, however, also present social, professional, and personal difficulties. The increasing use of AI poses questions about organizational stability, ethical norms, and structural integrity.

AI has a far longer history than most people realize. Many tales and myths in Greek mythology include references to the earliest stages of artificial intelligence (Mayor, 2018). These myths and legends portray intelligent beings that were thought to have been

[1]Research Scholar, Department of Psychology, Banaras Hindu University, Varanasi, India.
[2]Professor, Department of Psychology, Banaras Hindu University, Varanasi, India.
*Corresponding Author

Received: May 24, 2025; Revision Received: June 03, 2025; Accepted: June 06, 2025

constructed by talented artists in antiquity. Aristotle (384–322 B.C.) is widely regarded as the founder of artificial intelligence since he was the first to develop a precise set of rules describing how the human mind works. He asserted that "Logic is the novel and essential reasoning" (Aristotle, 1963; Robin, 2017). The ancient Greeks are credited with creating Talos, the earliest humanoid robot in history (Mayor, 2018).

John McCarthy, known as the father of artificial intelligence and credited with coining the term in 1956, defined "Artificial intelligence is the combination of science and engineering to make intelligent devices for human welfare." At the Dartmouth Conference, the field of artificial intelligence (AI) was initially introduced (McCarthy, 1956). Gil de Zúñiga et al. (2023) defined artificial intelligence *"the tangible real-world capability of non-human machines or artificial entities to perform, task solve, communicate, interact, and make decisions that would otherwise require human intelligence."*

Conceptual Framework of Artificial Intelligence Threats

AI simplifies processes for both public and private sectors in industries including banking, healthcare, and IT. But it also presents issues that affect workplace culture, organizational policy, and professionals' work-life.

The increasing integration of artificial intelligence into digital infrastructures has profoundly shaped modern societal operations, becoming essential for navigating contemporary social and economic systems (de Lima-Santos & Ceron, 2021; Hepp, 2020; Lobera et al., 2020). However, alongside its benefits, AI presents a range of potential threats that warrant critical attention. One central concern is its disruptive impact on the labor market. As AI systems become more advanced in performing tasks traditionally requiring human intelligence, such as data interpretation, predictive modeling, and autonomous operations, the risk of displacement grows, particularly for low-skilled and routine-based occupations (Autor, 2019). This transition may lead to structural unemployment and socioeconomic inequality. In addition, concerns about the ethical & governance issues raised by AI are becoming more widespread. Leading figures in the scientific and technical community have underlined how crucial it is to maintain transparency and control over AI research. Calls for responsible innovation stress that while AI holds the promise to address global challenges like poverty and disease, its unchecked evolution could lead to unintended consequences that surpass human oversight (Sparkes, 2015).

Thomas (2021) reports remarks of Elon Musk, the creator of SpaceX, warned at a conference that "AI is far more dangerous than nukes." Several AI threats are listed in the same report (Thomas, 2021): algorithmic bias brought on by faulty data, inequality among social groups, market volatility, the creation of dangerous weapons, the possibility of an AI arms race, algorithmic high frequency trading causing stock market instability, automatic job losses, privacy violations, and the possibility that some AI techniques could be lethal to humans.

Rationale of the study

This systematic literature review sets out to answer the question: *"What types of threats does artificial intelligence pose to Indian public and private organizations, and in what ways do these threats manifest?"* The objective is to synthesize and integrate prior non-Indian studies revealing that instead of being eradicated, the problems posed by AI have grown bigger, more tangible, and more serious (Kieslich et al., 2021; Thomas, 2021). The world economy and other sectors, including engineering, agriculture, politics, and the media,

have been severely disrupted by the rapid advancements in artificial intelligence (AI), which have produced technologically driven systems for the production, dissemination, and preservation of information and services (Birtchnell, 2018; Kamble & Shah, 2018; Kieslich et al., 2022).To accomplish this, we systematically employ literature review, that comprises utilizing an appropriate search strategy to locate empirically published English-language research articles conducted between 2015 and 2025 in a range of databases, such as Scopus, Web of Science, PsycNet, and Pub Med, to illuminate artificial intelligence threats to Indian public and private organizations.

METHOD

Research Design

To ensure a thorough and transparent review procedure, this study systematically identified, selected, and screened pertinent literature using the PRISMA framework (Selcuk, 2019).

Search Strategy

A comprehensive search for literature published between April 8, 2015, and April 8, 2025, was conducted using a variety of databases, including PubMed, Web of Science, PsycNet, and Scopus (refer to Figure 1 for an overview). Initially, a keyword-based search was conducted using terms such as artificial AND intelligence AND threats AND Indian AND public OR private AND organizations, combined using appropriate Boolean operators.

To select the articles, the author first independently screened for the inclusion of the full-text articles; for conflicting studies, the second author decided to select the articles. Only studies on artificial intelligence threats to Indian public and private organizations have been incorporated.

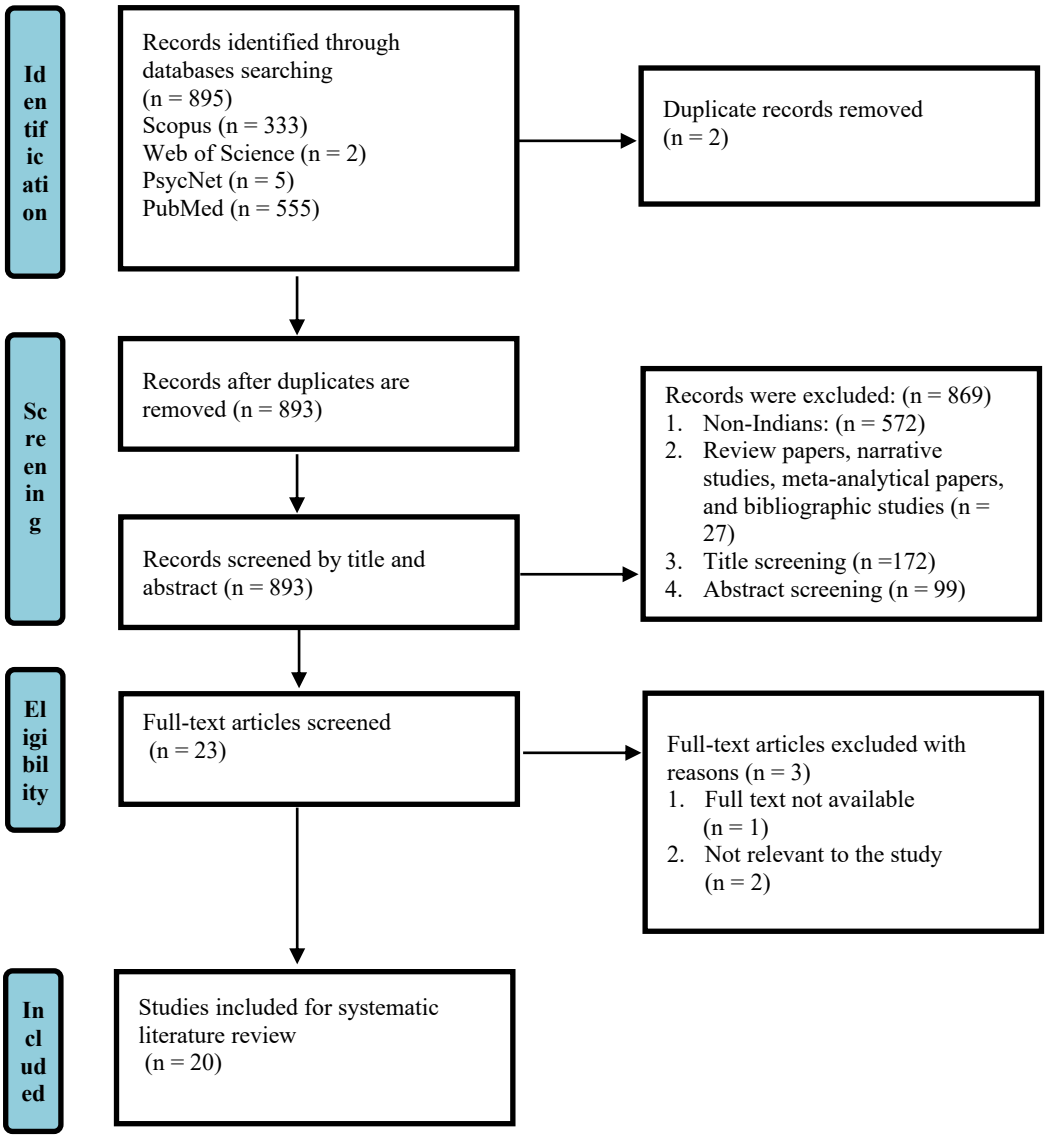
Figure 1: Search String in databases

Artificial AND intelligence AND threats AND indian AND public OR private AND organizations AND (LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA , "ARTS") OR LIMIT-TO (SUBJAREA , "PSYC") OR LIMIT-TO (SUBJAREA , "BUSI")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (AFFILCOUNTRY , "India")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (PUBSTAGE , "final"))

Inclusion and Exclusion Criteria

Primary mixed-methods design, cross-sectional, and correlational studies that examined artificial intelligence threats to Indian public and private organizations aged above 19 and below 60, published in English, between April 8, 2015, to April 8, 2025, were included. The study eliminated research on Indian professionals aged <19 and <60, and non-Indian people. languages other than English, published before 2015, review papers, and meta-analyses. The PRISMA flow diagram (see Figure 2) illustrates how to eliminate the first sample of related articles.

Figure 2: PRISMA flow chart of the selection and distribution of selected articles



Risk of Bias (Quality) Assessment

Each included study's methodological rigor was critically assessed, with particular attention paid to participant selection, outcome evaluation, follow-up adequacy, and data completeness. The framework for evaluating the quality of the evidence was the Newcastle-Ottawa Scale (NOS) (Luchini et al., 2017). Studies were ranked from low to high quality based on the NOS criteria, with high-quality studies providing the strongest evidence for the associations under investigation. Strong methodological soundness, with clearly described research procedures and comprehensible interpretations, was identified in all of the chosen articles.

RESULTS

Brief about the incorporated studies

The systematic literature review was conducted to analyze empirically published English-language articles from April 8, 2015, to April 8, 2025. It reveals that artificial intelligence poses various threats to the Indian public and private organizations.

After analyzing the systematic literature review of twenty full-text articles, nine themes were formulated based on artificial intelligence threats to Indian public and private organizations.

Table 1: This table demonstrates nine themes along with supporting authors and productive interpretations.

S.NO.	Authors	Themes	Interpretation
1.	Afzal et al. (2024), Chhabra and Prabhakaran (2023), Pai and Chandra (2022), Roy and Prabhakaran (2024).	**Cybersecurity Vulnerabilities and Fraud in Financial Institutions.**	Insider-led frauds, UPI scams, phishing, and a lack of threat modeling in financial AI systems. Weak security of AI infrastructure in cloud and biometric systems in Indian institutions.
2.	Chatterjee et al. (2021), Nilanjana Sinha (2024), Sinha et al. (2019).	**Privacy, Security, and Surveillance-Related Threats in the Workplace**	AI-driven CRM tools raise data protection and consumer trust issues in service industries. Aadhaar, mobile payments, and digital ID systems pose major privacy and surveillance risks.
3.	Chhabra and Prabhakaran (2023).	**Systemic Weaknesses in Cyber Threat Response**	Outdated fraud detection systems and poor incident response capabilities in AI ecosystems.
4.	Gupta et al. (2024), Kaur et al. (2025).	**Threats of Fake News and Misinformation**	Algorithmic amplification of fake news is affecting brand reputation and public trust.
5.	Prakash and Das (2023), Misra et al. (2023), Sinha (2024).	**Ethical Challenges and Legal Gaps Amplify Threats for Governance.**	Absence of GDPR-like data protection laws and gaps in AI oversight mechanisms. Misuse of AI tools due to a lack of standard legal frameworks for algorithmic accountability.
6.	Sinha (2024).	**Socioeconomic Exclusion due to Cybersecurity Threats**	AI systems reinforce the exclusion of the poor, migrants, and unbanked through errors or bias.
7.	Misra et al. (2023), Shukla et al., (2023), Sinha (2024).	**Cybersecurity Threats Promote Bias, Exclusion & Structural Inequality**	AI misclassifications in ID systems are causing denial of services or benefits to marginalized groups.
8.	Mukhopadhyay and Jain (2024), Singh et al. (2025).	**Human Resource & Skill Deficiencies**	Public sector AI adoption suffers due to low AI expertise and weak implementation capacity.
9.	Misra et al. (2023), Shukla et al. (2023), Singh et al. (2025).	**Organizational Readiness and Resistance**	Fear of job loss, infrastructure limitations, and digital unreadiness in both sectors.

DISCUSSION

The current study attempts to thoroughly review empirically published English-language literature on artificial intelligence threats to Indian public and private organizations. From 2015 to 2025, eight hundred ninety-five articles were searched in various databases, and for the review, only twenty articles made the short list. Nine main themes have been found as a result of the systematic literature review, such as cybersecurity vulnerabilities and fraud in financial institutions, privacy, security, and surveillance-related threats in the workplace, systemic weaknesses in cyber threat response, threats of fake news and misinformation, ethical challenges and legal gaps amplify threats for governance, socioeconomic exclusion due to cybersecurity threats, cybersecurity threats promote bias, exclusion & structural inequality, human resource & skill deficiencies, organizational readiness and resistance.

The first theme of the study reveals cybersecurity vulnerabilities and fraud in financial institutions (Afzal et al., 2024; Chhabra & Prabhakaran, 2023; Pai & Chandra, 2022; Roy & Prabhakaran, 2024), such as insider-led frauds, UPI scams, phishing, and a lack of threat modeling in financial AI systems. Weak security of AI infrastructure in cloud and biometric systems in Indian institutions. It has some supporting evidence to manage the situation of cybersecurity vulnerabilities, and financial fraud has been trending in the workplace. Reducing the extent and duration of data retention lowers the possibility of sensitive information being exposed, misused, or accessed without authorization (Hauer, 2015). To safeguard sensitive data and systems, implement robust access controls and authentication procedures (Djenna et al., 2021).

The study's second theme claims that privacy, security, and surveillance-related threats in the workplace (Chatterjee et al., 2021Sinha, 2024; Sinha et al., 2019). AI-driven CRM tools raise data protection and consumer trust issues in the service industries. Aadhaar, mobile payments, and digital ID systems pose major privacy and surveillance risks. The present study has some supporting evidence to tackle the AI threats of privacy, security, and surveillance concerns at the workplace. Building trust is facilitated by the idea of protecting privacy and security concerns (Bartoli et al., 2011). Modern technologies used in enterprises come with inherent privacy and security risks. To address these challenges, businesses need to develop robust yet practical policies that are easy to implement (Hone & Eloff, 2002; Straub & Welke, 1998).

The third theme of the study demonstrates systemic weaknesses in cyber threat response (Chhabra & Prabhakaran, 2023). Outdated fraud detection systems and poor incident response capabilities in AI ecosystems. Some supporting studies have provided a comprehensive understanding related to systemic weaknesses in cyber threat response. Vona (2008) discovered that flaws in internal systems act as pull igniters, making insider attacks possible with ease. Technology flaws and inadequate firewalls encourage staff to commit fraud. Due to inadequate internal controls and significant levels of cybercrime, 523 banks in the United States failed between 2000 and 2014 (Heiman-Hoffman et al., 1996).

The fourth theme of the study reveals threats of fake news and misinformation (Gupta et al., 2024; Kaur et al., 2025). Algorithmic amplification of fake news is affecting brand reputation and public trust. Previous studies have shown that fake news literature is mostly concentrated towards the fake news detection and fake news sharing behaviour by individuals (Apuke and Omar, 2021; Di Domenico et al., 2021), however, Pennycook and Rand (2021) explored the psychology behind fake news and highlighted several key insights. They found that recent data challenges the common belief that people are

influenced by partisanship and political biases in accepting fake news. Instead, poor truth detection is attributed to factors like weak reasoning, lack of knowledge, reliance on source heuristics, and familiarity. They also emphasized that inattention, rather than the intentional spread of misinformation, is the primary cause of believing fake news.

The fifth theme of the study addresses the ethical challenges and legal gaps that amplify threats for governance (Misra et al., 2023; Prakash & Das, 2023; Sinha, 2024). It draws attention to problems like insufficient control processes for AI and the lack of data protection laws akin to the General Data Protection Regulation (GDPR). The lack of standard legal frameworks for algorithmic accountability also contributes to AI misuse. Previous research underscores the need to exercise caution when it comes to AI's ethical, legal, and social ramifications, as Bryson and Winfield (2017) point out. Torresen (2018) pointed out potential ethical concerns during AI deployment, while Kar and Kushwaha (2023) explored ethical issues specific to AI use in government settings. Finally, Basu and Omotuboraa (2024) critically examined the ethical and governance struggles faced by the Global South in dealing with AI-driven surveillance systems.

The sixth theme of the study demonstrates socioeconomic exclusion due to cybersecurity threats (Sinha 2024). AI systems reinforce the exclusion of the poor, migrants, and unbanked through errors or bias. Previous studies have some supporting evidence. Okolo (2023) emphasizes how artificial intelligence helps industries like healthcare and agriculture, but it also exacerbates marginalization because of inadequate data governance and a lack of local research.

the seventh theme of the study reveals cybersecurity threats promote bias, exclusion & structural inequality (Misra et al., 2023; Shukla et al., 2023; Sinha, 2024). AI misclassifications in ID systems are causing denial of services or benefits to marginalized groups. Previous studies have some supporting evidence that artificial intelligence (AI) systems, when trained on non-representative datasets, have been shown to perpetuate systemic bias and exclusion, often resulting in catastrophic social consequences (Kar et al., 2021; Vaughan, 2021). The concentration of AI development within Global North countries further exacerbates these inequalities by systematically excluding disadvantaged communities, especially women and populations from the Global South, from both data representation and technological benefits (Chan et al., 2021; Sambasivan et al., 2020).

The eighth theme of the study reveals that artificial intelligence has become a threat to human resources and adversely affects their skills (Mukhopadhyay & Jain, 2024; Singh et al., 2025). Public sector AI adoption suffers due to low AI expertise and weak implementation capacity. Some previous studies strongly support the present study, which emphasizes the socio-technical nature of cyber risk. According to Wong et al. (2022), organizational security culture, governance, and staff training all have a big impact on the likelihood of ransomware attacks and are not just influenced by technical defenses. This underscores the critical need for HR-led interventions focused on awareness and skill-building within the workforce. Similarly, Souppaya and Scarfone (2013) advocate for structured employee training to recognize and avoid phishing attempts, along with the implementation of basic technical safeguards like content filtering, further reinforcing the importance of human behavior and preparedness in cyber defense strategies. Expanding the context into immersive digital environments.

The ninth theme of the study illuminates that artificial intelligence hampers organizational readiness and resistance (Misra et al., 2023; Shukla et al., 2023; Sinha, 2024). Fear of job loss, infrastructure limitations, and digital unreadiness in both sectors. The theme of organizational readiness and resistance is well-supported by prior research highlighting structural, cultural, and technical barriers to AI adoption. Borins (2001) explains that public sector organizations often lack an innovation-oriented culture and are constrained by bureaucratic procedures, making them resistant to adopting emerging technologies. Suzor (2019) stresses the need for robust governance structures, indicating that organizational preparedness is critical for ensuring ethical and responsible technology adoption.

Limitations and suggestions for further studies

A systematic literature review has certain limitations. The current review has investigated the Indian public and private organizations, consisting of only English-language articles published over the last ten years. Empirical papers using mixed methods, correlational, and cross-sectional designs have also been investigated. Further studies should be conducted on other countries' public and private organizations, meta-analysis, bibliometric analysis, and systematic reviews, considering another industrial and organizational psychological variable.

Theoretical and practical implications

Based on a thorough and systematic analysis of the literature on artificial intelligence threats to Indian public and private organizations, the current paper provides both theoretical & practical implications.

Theoretically, this research contributes to the following areas: Socio-Technical Systems Theory by highlighting the need to balance AI developments with ethical, institutional, and human factors; Technology Acceptance Models by incorporating psychological, cultural, and organizational barriers; insights into cybersecurity and misinformation broaden Risk Society Theory by demonstrating the unpredictable societal risks of AI; and, finally, it emphasizes the necessity of adaptive legal and ethical governance in India's dynamic AI landscape.

Practically, the RBI, IRDAI, and MeitY, among other Indian authorities, must develop flexible legislative frameworks to combat AI threats, including algorithmic bias and surveillance. Organizations should put in place cybersecurity and threat-response strategies tailored to AI, particularly in vital industries. HR, CRM, and finance personnel in particular need to receive compliance training to use AI ethically. To counteract false information and deepfakes, programs for digital literacy and public awareness are crucial. Cross-sector AI readiness indexes, bias audits, and workforce upskilling are essential for ethical and sustainable AI integration.

CONCLUSION

This study presents the most in-depth investigation to date of artificial intelligence threats to Indian public and private organizations. We set out to answer the question, *"What types of threats does artificial intelligence pose to Indian public and private organizations, and in what ways do these threats manifest?"* The findings from this research provide the theoretical and empirical framework for artificial intelligence threats to Indian public and private organizations. Which need to be analyzed artificial intelligence threats, to understand the pros & cons of artificial intelligence threats and to use protective and defensive strategies against artificial intelligence threats in the workplace. Overall, the study illuminates for proactive, interdisciplinary approach to managing artificial intelligence threats, one that

aligns technological innovation with ethical governance, institutional capacity, and inclusive policy-making. As India moves forward in its digital transformation journey, addressing these threats holistically will be essential for leveraging artificial intelligence responsibly and sustainably.

REFERENCES

Afzal, M., Ansari, M. S., Ahmad, N., Shahid, M., & Shoeb, M. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: An integrated model approach. *Journal of Financial Services Marketing, 29*(4), 1503–1523. https://doi.org/10.1057/s41264-024-00279-3

Aristotle. (1963). *Categories and De Interpretatione* (J. L. Ackrill, Ed. & Trans.). Oxford University Press.

Autor, D. (2019). *Artificial intelligence and employment: Will robots take your job?* USA: National Bureau of Economic Research.

Bartoli, A., Hernandez Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011). Security and privacy in your smart city. *Proceedings of the Barcelona Smart Cities Congress*, 1–6.

Bhattacharyya, S. S. (2024). Co-working with robotic and automation technologies: Technology anxiety of frontline workers in organisations. *Journal of Science and Technology Policy Management, 15*(5), 926–947. https://doi.org/10.1108/JSTPM-05-2022-0087

Birtchnell, T. (2018). Listening without ears: Artificial intelligence in audio mastering. Big Data &Society, 5(2), 2053951718808553. https://doi.org/10.1177/205395171880855 3

Borins, S. (2001). Encouraging innovation in the public sector. *Journal of Intellectual Capital, 2*(3), 310–319. https://doi.org/10.1108/14691930110400128

Bryson, J., & Winfield, A. (2017). Standardizing ethical design for artificial intelligence and autonomous systems. *Computer, 50*(5), 116–119. https://doi.org/10.1109/MC.2017.1 54

Chaslot, G. M. J.-B., Winands, M. H. M., van den Herik, H. J., Uiterwijk, J. W. H. M., & Bouzy, B. (2008). Progressive strategies for Monte-Carlo tree search. *New Mathematics and Natural Computation, 4*(3), 343–357. https://doi.org/10.1142/s1793 005708001094

Chatterjee, S., Ghosh, S. K., Chaudhuri, R., & Chaudhuri, S. (2021). Adoption of AI-integrated CRM system by Indian industry: From security and privacy perspective. *Information & Computer Security, 29*(1), 1–24. https://doi.org/10.1108/ICS-02-2019-0029

Chaudhuri, A., Behera, R. K., & Bala, P. K. (2025). Factors impacting cybersecurity transformation: An Industry 5.0 perspective. *Computers & Security, 150*, 104267. https://doi.org/10.1016/j.cose.2024.104267

Chhabra, N., & Prabhakaran, S. (2023). Internal-led cyber frauds in Indian banks: An effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management, 75*(2), 246–296. https:// doi.org/10.1108/AJIM-11-2021-0339

de-Lima-Santos, M., & Ceron, W. (2022). Artificial Intelligence in News Media: Current Perceptions and Future Outlook. *Journalism and Media, 3*(1), 13. https://doi.org/10. 3390/journalmedia3010002

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Sciences, 11*(10), 4580. https://doi.org/10.3390/app11104580

Dutta, D., & Mishra, S. K. (2024). Bots for mental health: The boundaries of human and technology agencies for enabling mental well-being within organizations. *Personnel Review, 53*(5), 1129–1156. https://doi.org/10.1108/PR-11-2022-0832

Gil de Zúñiga, H., Goyanes, M., & Durotoye, T. (2023). A scholarly definition of artificial intelligence (AI): Advancing AI as a conceptual framework in communication research. *Political Communication, 41*(2), 317–334. https://doi.org/10.1080/10584609.2023.2290497

Gupta, P., Mishra, V., & Rana, S. (2024). An exploratory study of the impact of perceived fake news on brand attachment: Mediating role of brand trust and consumer-brand identification. *International Journal of Technological Learning, Innovation and Development, 15*(3), 329–346. https://doi.org/10.1504/IJTLID.2024.10062104

Hauer, B. (2015). Data and information leakage prevention within the scope of information security. *IEEE Access, 3*, 2554–2565. https://doi.org/10.1109/ACCESS.2015.2506185

Heiman-Hoffman, V.B., Morgan, K.P. and Patton, J.M. (1996), "The warning sins of fraudulent financial reporting", *Journal of Accountancy, Vol. 182* No. 4, pp. 75-89.

Hepp, A. (2020). Artificial companions, social bots and work bots: Communicative robots as researchobjects of media and communication studies. Media, Culture & Society, 42(7–8), 1410–1426. https://doi.org/10.1177/0163443720916412

Hone, K., & Eloff, J. H. P. (2002). Information security policy – What do international security standards say? *Computers & Security, 21*(5), 402–409.

Jain, S., Mukhopadhyay, A., & Jain, S. (2023). Can cyber risk of health care firms be insured? A multinomial logistic regression model. *Journal of Organizational Computing and Electronic Commerce, 33*(1–2), 41–69. https://doi.org/10.1080/10919392.2023.2244386

Kamble, R., & Shah, D. (2018). Applications of artificial intelligence in human life. *International Journal of Research – Granthaalayah, 6*(6), 178–188. https://doi.org/10.29121/granthaalayah.v6.i6.2018.1363

Kar, A. K., & Kushwaha, A. K. (2023). Facilitators and barriers of artificial intelligence adoption in business: Insights from opinions using big data analytics. *Information Systems Frontiers, 25*, 1351–1374. https://doi.org/10.1007/s10796-021-10219-4

Kaur, D., Kushwah, S., & Sharma, A. (2025). The "what" and "why" of fake news: An in-depth qualitative investigation of young consumers. *Qualitative Market Research: An International Journal, 28*(2), 313–352. https://doi.org/10.1108/QMR-07-2023-0093

Kieslich, K., Keller, B., & Starke, C. (2022). Artificial intelligence ethics by design: Evaluating public perception on the importance of ethical design principles of artificial intelligence. *Big Data & Society, 9*(1), 20539517221092956. https://doi.org/10.1177/20539517221092956

Kieslich, K., Lünich, M., & Marcinkowski, F. (2021). The threats of artificial intelligence scale (TAI): Development, measurement, and test over three application domains. *International Journal of Social Robotics, 13*, 1563–1577. https://doi.org/10.1037/t87566-000_

Lobera, J., Fernández Rodríguez, C. J., & Torres-Albero, C. (2020). Privacy, values and machines:Predicting opposition to artificial intelligence. Communication Studies, 71(3), 448–465. https://doi.org/10.1080/10510974.2020.1736114

Luchini, C., Stubbs, B., Solmi, M., & Veronese, N. (2017). Assessing the quality of studies in meta-analyses: Advantages and limitations of the Newcastle Ottawa Scale. *World Journal of Meta-Analysis, 5*(4), 80–84. https://doi.org/10.13105/wjma.v5.i4.80

Mayor, A. (2018). *Gods and robots: Myths, machines, and ancient dreams of technology*. Princeton University Press. https://doi.org/10.2307/j.ctvc779xn

McCarthy, J. (1956). *Artificial intelligence (AI) coined at Dartmouth*. Dartmouth College. Retrieved October 28, 2021, from https://250.dartmouth.edu/highlights/artificial-intelligence-ai-coined-dartmouth

Misra, S. K., Sharma, S. K., Gupta, S., & Das, S. (2023). A framework to overcome challenges to the adoption of artificial intelligence in Indian Government Organizations. *Technological Forecasting and Social Change, 194*, 122721. https://doi.org/10.1016/j.techfore.2023.122721

Mukhopadhyay, A., & Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management, 74*, 102724. https://doi.org/10.1016/j.ijinfomgt.2023.102724

Okolo, C. T. (2023). *AI explainability in the Global South: Towards an inclusive praxis for emerging technology users* (Doctoral dissertation, Cornell University). https://doi.org/10.13140/RG.2.2.25596.51841

Pai, V., & Chandra, S. (2022). Exploring factors influencing organizational adoption of artificial intelligence (AI) in corporate social responsibility (CSR) initiatives. *Pacific Asia Journal of the Association for Information Systems, 14*(5), 82–115. https://doi.org/10.17705/1pais.14504

Prakash, A. V., & Das, S. (2022). Explaining citizens' resistance to use digital contact tracing apps: A mixed-methods study. *International Journal of Information Management, 63*, 102468. https://doi.org/10.1016/j.ijinfomgt.2021.102468

Praneetha, N., Srinivasa Rao, S., & Brahmanandam, P. S. (2024). A case study on using threat modeling to secure cloud computing data. *Proceedings on Engineering Sciences, 6*(4), 1837–1848. https://doi.org/10.24874/PES.SI.25.03b.016

Robin, S. (2017). *Aristotle's logic*. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2017 Edition). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=aristotle%20logic

Roy, N. C., & Prabhakaran, S. (2023). Sustainable response system building against insider-led cyber frauds in banking sector: A machine learning approach. *Journal of Financial Crime, 30*(1), 48–85. https://doi.org/10.1108/JFC-12-2021-0274

Roy, N. C., & Prabhakaran, S. (2024). Insider employee-led cyber fraud (IECF) in Indian banks: From identification to sustainable mitigation planning. *Behaviour & Information Technology, 43*(5), 876–906. https://doi.org/10.1080/0144929X.2023.2191748

Selcuk, A. A. (2019). A guide for systematic reviews: PRISMA. *Turkish Archives of Otorhinolaryngology, 57*(1), 57–58. https://doi.org/10.5152/tao.2019.4058

Shukla, A., Agnihotri, A., & Singh, B. R. (2023). Analyzing how AI and emotional intelligence affect Indian IT professional's decision-making. *EAI Endorsed Transactions on Pervasive Health and Technology, 9*(4), 1–13. https://doi.org/10.4108/eetpht.9.4654

Singh, N. K., Ray, R. K., Silayach, N., Dash, D. P., & Singh, A. (2025). Avatars at risk: Exploring public response to sexual violence in immersive digital spaces. *Computers in Human Behavior, 163*, 108500. https://doi.org/10.1016/j.chb.2024.108500

Sinha, N. (2024). Aadhaar, AI, and identity: Negotiating power and surveillance in the Global South. *Russian Sociological Review, 23*(4), 80–112. https://doi.org/10.17323/1728-192x-2024-4-80-12

Souppaya, M., & Scarfone, K. (2013). *Guide to malware incident prevention and handling for desktops and laptops* (NIST Special Publication 800-83 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-83r1

Sparkes, M. (2015, January 12). Top scientists call for caution over artificial intelligence. *The Telegraph*. https://www.telegraph.co.uk/technology/news/11342200/Top-scientists-call-for-caution-over-artificial-intelligence.html

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.

Suzor, N. P. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press. https://doi.org/10.1017/9781108666428

Thomas, M. (2021, March 1). Dangerous risks of artificial intelligence. *Builtin*. https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence

Vona, I. W. (2008). *Fraud risk assessment: Building a fraud audit programme*. John Wiley & Sons. https://www.wiley.com/enus/Fraud+Risk+Assessment%3A+Building+a+Fraud+Audit+Program-p-9780470130945

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, Article 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Acknowledgment

The author(s) appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest

The author(s) declared no conflict of interest.

How to cite this article: Surawat, R. & Kumar, S. (2025). Artificial Intelligence Threats to Indian Public and Private Organizations: A Systematic Review. *International Journal of Indian Psychology*, *13*(2)*,* 3020-3031. DIP:18.01.269.20251302, DOI:10.25215/1302.269