www.nesa-india.org • E-mail: nesapublications@gmail.com
International Journal on Biological Sciences

International Journal on Biological Sciences
ISSN No.: 0976-4518 • Vol. 17 (Iss. 1) **January-June 2026, Pp. 18-23**
https://doi.org/10.53390/IJBS.2026.17104

ARTIFICIAL INTELLIGENCE (AI) FROM THE PERSPECTIVES OF SECURITY, ETHICAL AND PRIVACY ISSUES

S. K. Basu

PFS, Lethbridge, Alberta, Canada

Review Paper

Received: 27.02.2026 **Revised:** 10.03.2026 **Accepted:** 20.03.2026

ABSTRACT

Artificial Intelligence (AI) has rapidly transitioned from a research discipline to a foundational component of critical infrastructure, commerce, education, healthcare, defence, and everyday digital services. This paper examines AI through the interconnected lenses of security, ethics, and privacy, arguing that these dimensions must be addressed holistically to ensure trustworthy and sustainable deployment. From a security perspective, AI systems introduce novel attack surfaces, including data poisoning, model inversion, adversarial examples, and supply-chain vulnerabilities, while simultaneously serving as defensive tools in cybersecurity operations. The dual-use nature of AI amplifies systemic risk, particularly as large-scale models are integrated into high-stakes environments. Ethically, AI systems raise concerns about bias, discrimination, opacity, and accountability. Algorithmic decision-making can reproduce or exacerbate societal inequalities when trained on skewed or unrepresentative data. The opacity of complex models challenges traditional notions of explainability and informed consent, complicating governance and redress mechanisms. Furthermore, the concentration of AI capabilities within a small number of powerful organizations creates asymmetries in power, access, and influence. Privacy considerations are equally pressing. AI's reliance on vast datasets, often containing sensitive personal information, heightens risks related to surveillance, re-identification, and unauthorized secondary use. Techniques such as differential privacy and federated learning offer partial mitigation but introduce trade-offs in utility, transparency, and accountability. Regulatory frameworks, including data protection laws and emerging AI governance regimes, struggle to keep pace with technological advances. The paper concludes that robust AI governance requires integrated security-by-design, ethics-by-design, and privacy-by-design approaches, supported by interdisciplinary collaboration, technical safeguards, regulatory oversight, and public engagement. Only by aligning technical innovation with normative principles can AI systems be deployed in ways that enhance societal welfare while minimizing harm.

No. of Pages: 6 **References: 10**

Keywords: Artificial Intelligence, AI, ethical, privacy, government, public, security.

INTRODUCTION

Artificial Intelligence (AI) is the field of computer science focused on creating systems that can perform tasks that normally require human intelligence (Ikwuanusi et al., 2023). In simple terms: AI is when machines are designed to think, learn, or make decisions like humans (Lee, 2024). AI represents one of the most transformative technological advancements of the modern era, distinguished by its capacity to augment human capabilities, optimize complex systems, and generate innovative solutions across diverse domains (Ikwuanusi et al., 2023; Khan,

*Corresponding author: *saikat.basu@alumni.uleth.ca*

2024). Among its most positive attributes is scalability: AI systems can process vast amounts of data with speed and precision far beyond human capability, enabling real-time insights and evidence-based decision-making (Ikwuanusi et al., 2023). This efficiency enhances productivity in sectors such as healthcare, education, finance, and transportation (Santosh and Gaur, 2022).

Another significant strength of AI is its consistency and accuracy in pattern recognition. By reducing human error and bias when properly designed and monitored, AI can improve diagnostic accuracy in medicine, strengthen fraud detection in finance, and enhance safety in industrial operations (Khan, 2024). Its adaptability through machine learning further allows systems to improve over time, refining performance as they encounter new data (Zhang et al., 2021).

AI also promotes accessibility and personalization (Gautam et al., 2022). Intelligent tutoring systems tailor educational experiences to individual learners (Ikwuanusi et al., 2023); while assistive technologies empower individuals with disabilities through speech recognition, computer vision, and natural language processing (Lee, 2024). In business and research, AI accelerates innovation by automating repetitive tasks, freeing human professionals to focus on creativity, strategy, and critical thinking (Shukla and Taneja, 2024).

Importantly, AI fosters global connectivity and collaboration. By enabling advanced communication tools, language translation, and knowledge discovery, AI reduces barriers across cultures and disciplines (Santosh and Gaur, 2022). When guided by ethical principles and human oversight, AI serves as a powerful tool for social good supporting sustainability initiatives, disaster response, medical breakthroughs, and inclusive growth (Khan, 2024).

AI-related privacy issues

AI brings huge benefits to our daily lives (Ikwuanusi et al., 2023); but, it also raises serious privacy concerns that directly affect how we live, work, and interact (Santosh and Gaur, 2022). Here's how AI-related privacy issues impact us:

Constant data collection: AI systems rely on large amounts of data to function. This means that smart phones track location, search history, and voice commands. Similarly, social media platforms analyze posts, likes, and messages. Smart home devices record voice and usage patterns (Lee, 2024). For example, companies like Google, Meta, and Amazon collect behavioural data to personalize services (Ikwuanusi et al., 2023). One may feel like one is being constantly watched. Even ordinary activities searching online or talking near a smart speaker can generate personal data profiles (Khan, 2024).

Loss of personal control over information: AI can analyze and combine data from multiple sources to predict our political views, health conditions, shopping habits, and personality traits (Santosh and Gaur, 2022). Often, people don't know what data is collected, how it's used and who it's shared with (Ikwuanusi et al., 2023). One may lose control over his/her digital identity. Decisions about you may be made by algorithms without your knowledge (Shukla and Taneja, 2024).

Targeted advertising and manipulation: AI powers personalized advertising and content feeds. Platforms like YouTube and TikTok use AI to recommend content that keeps you engaged. One may see advertisements tailored to our specific fears, interests, or vulnerabilities. Content algorithms can influence opinions, buying decisions, and even political beliefs. Filter bubbles may limit exposure to diverse viewpoints (Ikwuanusi et al., 2023; Stahl, 2021).

Facial recognition and surveillance: AI-powered facial recognition is used in airports, and law enforcement (Santosh and Gaur, 2022). Some governments and companies deploy large-scale surveillance systems. Reduced anonymity in public spaces, risk of wrongful identification, potential misuse for mass surveillance, and monitoring are important steps (Gautam et al., 2022). This can affect freedom of expression and behaviour (Khan, 2024).

Data breaches and security risks: AI systems store massive datasets. When breached, they expose financial information, medical records, and private conversations. Identity theft, financial fraud, reputational damage, and emotional stress are common (Dhirani et al., 2023; Santosh and Gaur, 2022).

Bias and discriminatory decisions: AI systems can make decisions about loan approvals, and job applications (Lee, 2024). Insurance eligibility in the training data contains bias, and AI may unfairly disadvantage certain groups. Opportunities may be

limited based on flawed or biased algorithmic predictions often without transparency or appeal (Shukla and Taneja, 2024).

Deepfakes and identity misuse: AI can generate realistic fake videos, voice recordings, and images (Santosh and Gaur, 2022). Impact on life include reputation damage, fraud scams (*e.g.*, fake voice calls) and systematic spread of misinformation (Khan, 2024). It becomes harder to trust what we see and hear.

Dynamics of AI security

The future of AI security is shaping up to be one of the most important technology challenges of the next decade. As AI systems become more powerful and integrated into infrastructure, education, business, and defence, security will evolve across several key dimensions (Li and Zhang, 2017).

Attackers can manipulate AI inputs (*e.g.*, slightly altered images or data) to cause incorrect outputs (Li and Zhang, 2017). Future defences will include adversarial training, robust model architectures, and real-time anomaly detection (Stahl, 2021). Companies like OpenAI, Google DeepMind, and Anthropic invest heavily in preventing model stealing through secure APIs, watermarking outputs and hardware-based protections (Dhirani et al., 2023).

AI is increasingly used to detect zero-day vulnerabilities, monitor network anomalies and in automate incident response. Platforms from companies like CrowdStrike and Palo Alto Networks already integrate AI-driven threat detection (Gautam et al., 2022). Future systems will predict attacks before execution, use autonomous defensive agents, and coordinate across global threat networks (Khan, 2024). Unfortunately, AI also empowers attackers like automated phishing generation, deepfake scams, AI-generated malware, and social engineering at scale (Stahl, 2021). The rise of generative AI tools following breakthroughs like OpenAI's GPT models has dramatically lowered the barrier for sophisticated attacks (Lee, 2024). Future counter measures include deepfake detection systems, AI content authentication standards, and cryptographic identity verification (Dhirani et al., 2023).

Governments across the planet now treat AI as strategic infrastructure (Gautam et al., 2022). AI models may be classified as critical assets that export controls on advanced chips and increased AI weaponization concerns (Santosh and Gaur, 2022). Countries like the United States and China are investing heavily in both AI capabilities and AI security frameworks. Hence, there is need for AI-specific cybersecurity regulations. The international AI arms control discussions, and mandatory model auditing (Shukla and Taneja, 2024).

AI governance and regulation: We are entering the era of AI policy involving risk-tiered regulations, mandatory transparency reports, as well as alignment and safety standards (Li and Zhang, 2017). The European Union AI Act is one of the first large-scale regulatory frameworks. Future trends will therefore focus around licensing requirements for frontier models, third-party safety audits and liability frameworks for AI harm (Lee, 2024).

Ethical and privacy issues of AI

Artificial Intelligence (AI) is rapidly transforming societies by enabling automation, predictive analytics, personalization, and decision-making at unprecedented scale (Stahl, 2021). While these systems promise efficiency, innovation, and economic growth, they also raise significant ethical and privacy concerns that challenge existing legal, social, and moral frameworks (Gautam et al., 2022; Lee, 2024). The ethical and privacy issues surrounding AI stem largely from its reliance on large-scale data collection, opaque algorithmic processes, and autonomous decision-making capabilities (Dhirani et al., 2023; Gautam et al., 2022).

One of the central privacy concerns in AI systems is mass data collection. AI models, particularly machine learning and deep learning systems, depend on vast datasets that often include personal, behavioural, biometric, and location-based information (Gautam et al., 2022). This data is frequently gathered through online platforms, smart devices, surveillance systems, and social media, sometimes without meaningful informed consent (Stahl, 2021). The aggregation and analysis of such data increase the risks of surveillance, re-identification of anonymized information, and misuse by corporations or governments. Even when anonymization techniques are applied, advances in data analytics can re-link anonymized datasets to identifiable individuals, undermining privacy protections (Zhang et al., 2021).

Another major ethical issue is bias and discrimination. AI systems learn patterns from historical data, which may reflect societal inequalities and prejudices (Gautam et al., 2022). When these biased datasets are

used to train models, the resulting systems can perpetuate or even amplify discrimination in areas such as hiring, credit scoring, healthcare, and law enforcement. For example, algorithmic decision-making tools have been criticized for disproportionately affecting marginalized communities (Gautam et al., 20220. This raises concerns about fairness, accountability, and the need for transparent auditing processes (Shukla and Taneja, 2024).

Transparency and explainability also present ethical challenges. Many advanced AI models, especially deep neural networks, operate as "black boxes," making it difficult to understand how specific outputs are generated. This opacity complicates accountability when AI systems make harmful or erroneous decisions (Stahl, 2021). Individuals affected by automated decisions may lack the ability to challenge outcomes if the reasoning behind them is not interpretable (Gautam et al., 2022). The demand for explainable AI reflects the broader ethical principle that systems influencing human lives should be understandable and contestable (Li and Zhang, 2017).

Accountability and responsibility are closely linked concerns. When AI systems cause harm; whether through faulty medical diagnoses, autonomous vehicle accidents, or erroneous legal risk assessment, it is often unclear who should be held responsible: the developer, the deploying organization, the data provider, or the algorithm itself (Gautam et al., 2022; Khan, 2024l Lee, 2024). Existing legal frameworks struggle to address distributed responsibility in complex AI ecosystems, necessitating updated regulatory approaches and governance models (Ikwuanusi et al., 2023; Stahl, 2021).

Security risks further compound privacy issues (Ikwuanusi et al., 2023). AI systems are vulnerable to adversarial attacks, data poisoning, and model inversion techniques that can extract sensitive information from trained models (Khan, 2024). Such vulnerabilities threaten both individual privacy and broader societal security (Ikwuanusi et al., 2023; Stahl, 2021). As AI becomes integrated into critical infrastructure, healthcare systems, and financial markets, the stakes of these security breaches grow significantly (Gautam et al., 2022; Lee, 2024).

In response to these concerns, regulatory initiatives and ethical guidelines have emerged globally. Frameworks such as the General Data Protection Regulation (GDPR) emphasize data minimization, user consent (Stahl, 2021); and the right to explanation in automated decision-making (Lee, 2024). International organizations, including UNESCO, have developed ethical AI recommendations promoting human rights, transparency, and accountability (Li and Zhang, 2017). However, enforcement challenges and rapid technological advancement continue to test the effectiveness of such measures (Khan, 2024).

A comprehensive response to ethical and privacy issues requires law + ethics + technology + participation + accountability, working together (Ikwuanusi et al., 2023; Stahl, 2021). This approach is especially crucial in areas like ethnomedicine, indigenous knowledge systems, biodiversity research, and digital data governance, where ethical failures can cause irreversible harm (Li and Zhang, 2017).

In conclusion, AI's ethical and privacy challenges are multifaceted and evolving. They encompass issues of data protection, bias, transparency, accountability, and security (Lee, 2024). Addressing these concerns requires interdisciplinary collaboration among technologists, policymakers, ethicists, and civil society (Ikwuanusi et al., 2023; Khan, 2024). Effective governance must balance innovation with safeguards that protect individual rights and promote equitable outcomes, ensuring that AI development remains aligned with fundamental ethical principles and democratic values (Ikwuanusi et al., 2023; Li and Zhang, 2017).

The big future question hangs around

Alignment- Can we ensure AI systems act in accordance with human values?

Autonomous Systems: How do we secure AI agents that can independently act online?

AGI risk: If Artificial General Intelligence emerges, security shifts from "cyber risk" to existential risk.

Where this is heading from the perspectives of 2026-2035 outlooks?

1. AI security becoming its own major industry.
2. Governments creating AI safety agencies.
3. AI red-teaming becomes mandatory.
4. Hardware-level AI isolation (secure AI chips).
5. Cryptographic proof-of-origin for all AI-generated content.

Conclusion and future directions

In summary, the positive attributes of AI lie in its efficiency, accuracy, adaptability, personalization, and collaborative potential. As a complement to human intelligence rather than a replacement, AI holds significant promise to enhance quality of life, drive economic development, and address some of the world's most complex challenges. AI privacy issues impact personal freedom, democracy, financial security, social trust and mental well-being. As AI becomes more integrated into daily life-smart cities, healthcare, education, and workplaces-privacy concerns become more significant. AI is not inherently bad. It improves healthcare, navigation, fraud detection, and accessibility. The real challenge is balancing innovation, data protection, ethical regulation and documentation. Many countries are developing privacy laws (like data protection regulations) to address these concerns, but technology evolves faster than regulation. Ethical and privacy-related issues can be addressed comprehensively only through a multi-layered, integrated approach that combines law, technology, institutional governance, and social awareness. Below is a structured framework that is widely applicable across sectors such as research, healthcare, technology, ethnomedicine, environment, and social sciences.

1. Strong legal and policy frameworks: Clear data protection laws (*e.g.*, informed consent, data ownership, right to withdraw). Alignment with national and international standards (e.g., GDPR-like principles, India's Digital Personal Data Protection Act). Sector-specific ethical guidelines (research ethics, indigenous knowledge protection, biomedical ethics). Key outcome: Legal accountability and enforceable safeguards.

2. Ethical governance and oversight: Establish Ethics Committees / Institutional Review Boards (IRBs), Mandatory ethical impact assessments before any projects begin. Inclusion of diverse stakeholders (scientists, legal experts, community representatives)in the system to avoid bias, nepotism and corruptions. Key outcome: Ethical risks are identified and mitigated early.

3. Informed consent and community participation: Use free, prior, and informed consent (FPIC), especially for indigenous and tribal communities. Consent must be clearly explained, voluntary, culturally appropriate and there should be a process of ongoing consent, not a one-time formality. Key outcome: Respect for autonomy and cultural rights.

4. Data minimization and purpose limitation: Collect only necessary data, use data strictly for stated purposes, and avoid secondary use without renewed consent. Key outcome: Reduced risk of misuse or exploitation.

5. Privacy-by-Design and security measures: Anonymization and pseudonymization of personal data, and secure storage, encryption, and controlled access. Regular security audits and breach-response plans. Key outcome: Technical protection of sensitive information.

6. Transparency and accountability: Clearly communicate what data is collected, why it is collected, and who has access. Public disclosure of funding sources and potential conflicts of interest, and provide clear mechanisms for grievance redressal. Key outcome: Trust and institutional credibility.

7. Benefit sharing and fair use: Ensure equitable sharing of benefits, especially when using traditional knowledge or biological resources. Recognition, compensation, and co-authorship where appropriate. Compliance with access and benefit-sharing (ABS) frameworks (e.g., Nagoya Protocol). Key outcome: Prevention of biopiracy and exploitation.

8. Capacity building and ethical literacy: Regular training on ethics and privacy for researchers, practitioners, and administrators. Awareness programs for communities about their rights. Integration of ethics into academic curricula. Key outcome: Ethical culture rather than rule-based compliance alone.

9. Continuous monitoring and review: Periodic review of ethical practices as technologies and social contexts evolve. Adaptive policies responsive to emerging risks (AI, genomics, digital health). Key outcome: Long-term ethical resilience.

10. Ethical pluralism and context sensitivity: Respect cultural, social, and ecological contexts, and avoid one-size-fits-all solutions. Balance innovation with human dignity, ecological sustainability, and social justice. Key outcome: Context-appropriate and inclusive ethics.

References

1. **Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., and Newe, T.** 2023. Ethical dilemmas and privacy issues in emerging technologies: A review. Sensors. 23(3): 1151.

2. **Gautam, G., Arora, H., Choudhary, J. and Raj, A.** 2022. Data privacy and ethical concerns in AI and computer science. *Industrial Engineering Journal*. 51(08): 25-31.

3. **Ikwuanusi, U. F., Adepoju, P. A., and Odionu, C. S.** 2023. Advancing ethical AI practices to solve data privacy issues in library systems. *International Journal of Multidisciplinary Research Updates*. 6(1): 33-44.

4. **Khan, W. N.** 2024. Ethical challenges of AI in education: Balancing innovation with data privacy. AI EDIFY Journal. 1(1):1-13.

5. **Lee, R. S. T.** 2024. AI ethics, security and privacy. Artificial Intelligence in Daily Life. pp. 369-384.

6. **Li, X., and Zhang, T.** 2017. An exploration on artificial intelligence application: From security, privacy and ethic perspective. The 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), pp. 416-420.

7. **Santosh, K. C., and Gaur, L.** 2022. Privacy, security, and ethical issues. Artificial intelligence and machine learning in public healthcare: opportunities and societal impact, pp. 65-74.

8. **Shukla, R. P., and Taneja, S.** 2024. Ethical considerations and data privacy in artificial intelligence. Integrating Generative AI in Education to Achieve Sustainable Development Goals, pp. 86-97.

9. **Stahl, B. C.** 2021. Ethical issues of AI. Artificial Intelligence for a better future: An ecosystem perspective on the ethics of AI and emerging digital technologies, pp. 35-53.

10. **Zhang, Y., Wu, M., Tian, G. Y., Zhang, G., and Lu, J.** 2021. Ethics and privacy of artificial intelligence: Understandings from bibliometrics. Knowledge-Based Systems, 222, 106994.