International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. 11 Issue 02 | 2026

Cybersecurity Ethics Through the Lens of Indigenous Knowledge Systems

M.T.Tekade[1] ,Khyati Choudhary[2],Sharda Lande[3], Radhika Bihade[4]
[1]*Assistant Professor, Padm. Dr.V .B. Kolte College of Engineering, Maharashtra, India*

DOI: 10.5281/zenodo.19204937

ABSTRACT

Cybersecurity ethics is often framed through Western philosophical traditions that emphasize individual rights, property, and control. While these frameworks have contributed valuable principles such as privacy, consent, and accountability, they do not fully address the relational, communal, and ecological dimensions of digital life. Indigenous Knowledge Systems (IKS) offer alternative ethical lenses rooted in relationality, stewardship, reciprocity, and respect. Applying these perspectives to cybersecurity ethics can expand how societies understand responsibility, harm, and protection in digital spaces.

At the core of many Indigenous worldviews is the concept of relationality. Knowledge, land, people, and technology are understood as interconnected rather than separate or owned in isolation. When applied to cybersecurity, this challenges the idea that data is merely an asset to be controlled or monetized. Instead, data can be viewed as an extension of people and communities, carrying cultural, spiritual, and historical significance. From this perspective, a data breach is not only a technical failure or financial loss but a violation of relationships and trust.

Stewardship is another foundational principle in Indigenous Knowledge Systems. Rather than emphasizing ownership, stewardship focuses on caretaking responsibilities across generations. In cybersecurity ethics, stewardship reframes the role of organizations and governments as guardians of digital information rather than proprietors. This perspective encourages long-term thinking about data protection, including how today's cybersecurity decisions may impact future generations, particularly when dealing with sensitive cultural, health, or genetic data belonging to Indigenous communities.

Reciprocity further distinguishes Indigenous ethical frameworks from conventional cybersecurity models. Reciprocity implies mutual responsibility and benefit between all participants in a system. In digital contexts, this raises ethical questions about how data is collected, used, and shared. If communities provide data, what protections, benefits, or decision-making power do they receive in return? Ethical cybersecurity, viewed through this lens, requires transparent practices and meaningful consent rather than one-sided extraction of information.

Indigenous Knowledge Systems also emphasize respect for boundaries, including sacred or restricted knowledge. Not all information is meant to be shared openly, even if technology makes it possible. This challenges the prevailing assumption that increased access and openness are always ethical goods. In cybersecurity, respecting digital boundaries means recognizing that some data should remain inaccessible, even to powerful institutions, and that ethical restraint is as important as technical capability.

Finally, Indigenous perspectives encourage a holistic understanding of harm. Cyber harm is not limited to economic loss or system downtime but includes cultural erasure, loss of autonomy, and disruption of communal well-being. Ethical cybersecurity frameworks informed by Indigenous Knowledge Systems therefore prioritize collective resilience, cultural survival, and relational repair alongside technical defences.

Incorporating Indigenous Knowledge Systems into cybersecurity ethics does not mean rejecting existing frameworks, but complementing them. By foregrounding relationality, stewardship, reciprocity, and respect, Indigenous perspectives offer a more holistic and human-centered approach to digital security. As cybersecurity challenges grow increasingly complex and global, these ethical insights can guide more just, inclusive, and sustainable digital futures.

Keywords: - Cybersecurity ethics; Indigenous Knowledge Systems; data sovereignty; digital stewardship; relational ethics; information security; cultural protection; data governance

1. INTRODUCTION

The rapid expansion of digital technologies has transformed how information is created, stored, and exchanged, making cybersecurity a critical concern for governments, organizations, and communities worldwide. Ethical frameworks guiding cybersecurity practices have traditionally emerged from Western philosophical traditions, emphasizing individual rights, data ownership, risk mitigation, and legal compliance. While these approaches have contributed significantly to protecting digital infrastructures, they often fail to address the broader social, cultural, and relational impacts of cyber practices, particularly for Indigenous and marginalized communities.

ISSN: 2456-236X
Vol. 11 Issue 02 | 2026

Indigenous Knowledge Systems (IKS) offer alternative ethical foundations grounded in relationality, stewardship, reciprocity, and respect for knowledge boundaries. These systems understand knowledge and information as living, contextual, and deeply connected to community identity, land, and intergenerational responsibility. When applied to cybersecurity, Indigenous perspectives challenge dominant assumptions that data is a neutral commodity and that technological capability alone determines ethical action. Instead, they emphasize responsibility, care, and long-term consequences in the handling of digital information.

This paper explores cybersecurity ethics through the lens of Indigenous Knowledge Systems, arguing that Indigenous ethical principles can enrich and expand contemporary cybersecurity discourse. By examining concepts such as data stewardship, collective responsibility, and cultural protection, the study highlights how Indigenous perspectives reframe cyber threats as relational and cultural harms rather than solely technical failures. Integrating Indigenous Knowledge Systems into cybersecurity ethics offers a more holistic, inclusive, and sustainable approach to digital security, one that aligns technological innovation with social justice and cultural integrity.

2. RELATED WORK

The intersection of Indigenous Knowledge Systems (IKS) and technology ethics is an emerging area of interdisciplinary inquiry, though most existing research focuses on broader digital governance and data sovereignty rather than cybersecurity per se. A substantial body of work has developed around Indigenous data sovereignty, which foregrounds community control and governance of data related to Indigenous peoples and challenges Western paradigms of data ownership and extractive practices. The CARE Principles—Collective Benefit, Authority to Control, Responsibility, and Ethics—have been proposed to guide ethical engagement with Indigenous data within open data ecosystems, emphasizing relational accountability and community-defined purposes for data use and access.

Scholars have critiqued conventional data mining and algorithmic systems as reproducing colonial power structures and erasing Indigenous epistemologies, arguing for frameworks that centre Indigenous legal and ethical norms in data governance. Systematic reviews in health research illustrate how Indigenous data governance principles can be operationalized, though they note that implementation of such frameworks remains inconsistent across domains. Similarly, the First Nations principles of OCAP (Ownership, Control, Access, and Possession) offer a governance standard for Indigenous information and research data, reinforcing Indigenous authority over digital representations.

Beyond governance frameworks, broader technological ethics literature highlights the value of Indigenous thought in critiquing dominant Western assumptions about technology. Researchers have advocated for incorporating Indigenous worldviews into the ethics of technology generally, showing how relational ethics and community-centered values can deepen critiques of technological development and use. Closely related work examines how information technology can either honour or undermine Indigenous sovereignty when deployed in research partnerships, emphasizing transparency, accessibility, and relational practices that align with Indigenous priorities.

While much of this literature concentrates on data governance, artificial intelligence, and research methodologies, it lays essential ethical groundwork for cybersecurity. The focus on data as relational and culturally embedded, community authority over digital knowledge, and decolonial critiques of technological systems collectively contribute to rethinking cybersecurity ethics beyond individualistic and technical paradigms.

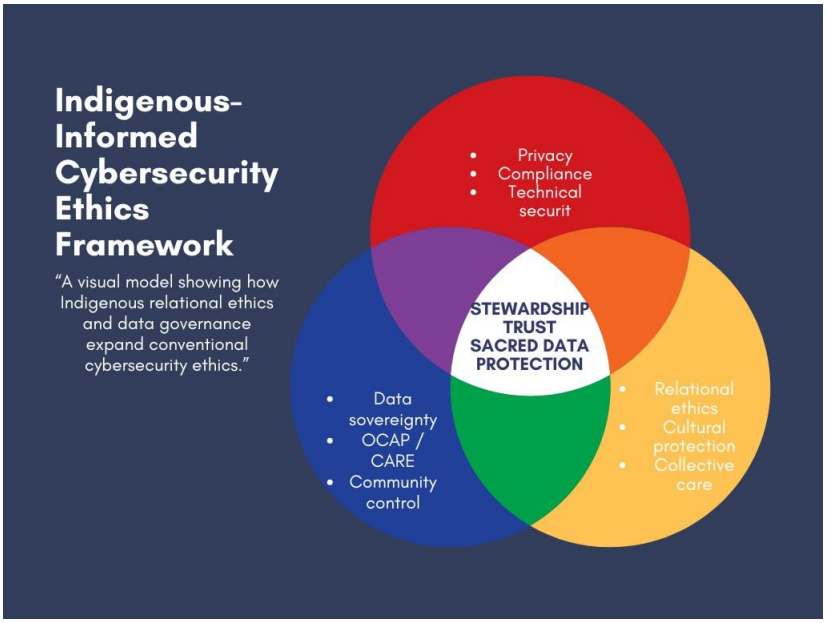

Fig -1: Proposed Venn Model of Cybersecurity Ethics using IKS

3. PROPOSED WORK

This paper proposes an Indigenous Knowledge Systems (IKS)-inspired ethical framework for cybersecurity decision-making. The main goal of the proposed work is to bridge the gap between technical cybersecurity practices and ethical responsibility by embedding Indian ethical values such as Dharma (duty), Karma (consequence), Satya (truth), Ahimsa (non-harm), and Nyaya (justice) into practical cybersecurity actions. Modern cybersecurity approaches primarily focus on compliance and risk management, but they often lack moral reasoning and cultural context. The proposed framework introduces a values-driven ethical layer that can guide professionals when facing dilemmas like surveillance, privacy conflicts, misinformation, hacking for defence, insider threats, or AI misuse.

The proposed work is designed as a three-layer model consisting of (i) IKS ethical principles, (ii) cybersecurity operational practices, and (iii) decision validation through ethical scoring and justification. The model is represented visually using a Venn-based conceptual diagram to highlight the intersection between IKS ethics and cybersecurity.

3.1Proposed IKS-Based Cybersecurity Ethics Framework

The framework consists of the following core modules:

➢ **1**.Ethical Value Mapping Layer

This layer maps key IKS principles to cybersecurity ethics:

- Dharma (Duty): Promotes responsible disclosure, lawful defence, and professional integrity.
- Karma (Consequence): Evaluates impact of cyber actions (short-term and long-term harm/benefit).
- Ahimsa (Non-harm): Prevents actions that may cause unnecessary damage such as destructive malware, data misuse, or unethical surveillance.
- Satya (Truth): Encourages transparency, accuracy in reporting breaches, and truthful security communication.
- Nyaya (Justice): Ensures fairness, non-discrimination, and rights-based security enforcement.

➢ **2**.Cybersecurity Practice Layer

This layer includes real cybersecurity operations where ethical conflict arises, such as:

- Incident Response and Threat Handling
- Vulnerability Discovery & Disclosure
- Penetration Testing and Red Teaming
- Cyber Monitoring & Surveillance
- Digital Forensics
- AI in Security and Automated Decision-Making
- Data Privacy & Information Protection

➢ **3**.Ethical Decision & Validation Layer

This layer provides a structured method to evaluate whether a cybersecurity action is ethically acceptable. Each

decision is tested using a set of guiding questions:

- Does the action align with Dharma (professional duty and lawful intent)?
- What is the Karma impact (who may benefit, who may be harmed)?
- Does it violate Ahimsa (can harm be minimized)?
- Is it consistent with Satya (truthful, accountable reporting)?
- Is the outcome Nyaya-based (fair, rights-respecting)?

3.2 Workflow of Proposed System

The proposed work follows the below steps:

- **Identify cybersecurity scenario** (e.g., breach, phishing, insider misuse, digital investigation).
- **Determine action options** available for the security team.
- **Map each action option to IKS principles** using the ethical value mapping layer.
- **Assign ethical weights / scores** (Low–Medium–High risk of ethical violation).
- **Choose best option** that maximizes protection while minimizing harm.
- **Generate ethical justification report** to support transparency and accountability.

3.3Key Contribution of Proposed Work

The proposed framework contributes the following:

- Introduces IKS-driven ethical reasoning in cybersecurity which is culturally grounded and practically useful.
- Provides a clear model to guide cyber professionals in gray-area decisions where law may not fully address morality.
- Offers a structured framework that can be extended into:
- cyber ethics training modules,
- policy formulation,
- and AI-driven ethical decision support systems.

Table -1: Mapping cybersecurity cases with IKS ethical principles

Cyber Scenario	Ethical Dilemma	IKS Principle Applied	Decision Outcome
Phishing Email Attack on Employees	Should the organization monitor employee inboxes for detection?	Dharma + Nyaya (duty + fairness)	Use monitoring only for threat patterns; avoid personal email inspection; ensure transparency policy.
Insider Data Theft (Employee stealing files)	Whether to publicly name the employee or handle privately?	Satya + Nyaya (truth + justice)	Report to authority with evidence; protect organization; avoid public shaming unless legally required.
Vulnerability Found in Govt System	Should researcher disclose immediately online for awareness?	Dharma + Ahimsa (responsibility + non- harm)	Follow responsible disclosure; inform authority first; publish only after patch.
Surveillance for Threat Prevention	How much monitoring is ethical in the name of security?	Ahimsa + Nyaya	Use minimum surveillance needed; avoid continuous tracking; protect citizen privacy.
Digital Forensics of Suspected User	Can investigators access private personal data during investigation?	Dharma + Satya	Access only relevant data; maintain evidence integrity; document chain of custody.
Ransomware Incident Response	Should the organization pay ransom to restore services?	Karma + Dharma (consequence + duty)	Do not pay unless life-critical services affected; prefer recovery/backup; report to cyber cell.

AI-Based Hiring Security Clearance	AI may reject candidates unfairly	Nyaya + Satya	Ensure explainable AI; human review mandatory; avoid biased decision automation.
Penetration Testing in Client Network	Ethical limits in exploitation (data access)	Ahimsa + Dharma	Test only agreed scope; no unnecessary access to personal files; immediate reporting & cleanup.

4. RESULTS AND DISCUSSION

The effectiveness of the proposed IKS-based cybersecurity ethics framework can be observed through its structured decision-making ability in real-world cyber scenarios. Unlike conventional cybersecurity ethics models which are mostly compliance-driven, the proposed framework introduces a culturally grounded ethical reasoning layer that supports professionals in handling complex dilemmas.

The framework produces outcomes in three key areas:

- **Improved Ethical Decision Clarity**
  In common cybersecurity activities such as monitoring, digital forensics, or incident response, ethical boundaries are not always clearly defined by law. The proposed model provides clarity by mapping actions to IKS principles like Dharma and Ahimsa, which helps in selecting responsible actions with minimal harm.
- **Transparency and Accountability**
  The Satya principle strengthens breach reporting, documentation, and stakeholder communication. This promotes honest and transparent cybersecurity practices, reducing suppression of incidents and encouraging responsible disclosure.
- **Fairness in Cyber Governance**
  Nyaya-based evaluation ensures that cybersecurity controls do not unfairly target specific groups and that monitoring decisions remain proportionate. This is highly useful in AI-enabled security systems where biased outputs may create unfair outcomes.

Further, the case mappings presented in Table-1 demonstrate that the proposed framework consistently leads to balanced decisions that protect systems while respecting privacy, justice, and harm minimization. Hence, the proposed work can be effectively adopted for cyber ethics training, governance policy formulation, and future AI- driven ethical decision support in cybersecurity.

5. CONCLUSIONS

This paper presented an Indigenous Knowledge Systems (IKS)-based ethical framework for cybersecurity decision-making, with the aim of integrating culturally grounded moral reasoning into modern cyber practices. The proposed model bridges the gap between technical security operations and ethical responsibility by applying IKS principles such as Dharma (duty), Karma (consequence), Ahimsa (non-harm), Satya (truth), and Nyaya (justice). The conceptual evaluation through multiple cybersecurity scenarios shows that the framework supports consistent

ethical choices, encourages harm minimization, and improves transparency and accountability during incident response, monitoring, vulnerability disclosure, and AI-driven security governance.

Further, the study highlights that compliance-based cybersecurity alone is insufficient to address modern ethical dilemmas such as privacy conflicts, surveillance boundaries, and biased automation. The proposed approach strengthens decision clarity by providing a structured ethical validation layer, making cybersecurity more human- centric and socially aligned. As future work, the framework can be implemented as a measurable scoring model and integrated into cybersecurity policy, training modules, and AI-enabled decision support systems to enable real-time ethical evaluation in practical environments.

6. REFERENCES

[1]. Luciano Floridi, “Information Ethics: An Introduction,” *Ethics and Information Technology*, Springer, 1999.
[2]. National Institute of Standards and Technology (NIST), *Cybersecurity Framework (CSF) 2.0*, NIST, 2024.
[3]. NIST, *Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*, 2020.
[4]. OECD, *OECD AI Principles*, Organisation for Economic Co-operation and Development, 2019. [5].
UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, UNESCO Publishing, 2021.
[6]. European Union Agency for Cybersecurity (ENISA), *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, ENISA, 2019.
[7]. Michael J. Quinn, *Ethics for the Information Age*, Pearson Education, 7th Edition, 2017.
[8]. Debabrata Chatterjee, “Indian Philosophy and Business Ethics,” *Journal of Business Ethics*, Springer, 1998.

[9]. S. Radhakrishnan, *Indian Philosophy: Volume 1*, Oxford University Press, 1923.
[10]. Patrick Lin, Keith Abney and Ryan Jenkins (Eds.), *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence*, Oxford University Press, 2017.
[11]. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.
[12]. Ministry of Electronics and Information Technology (MeitY), Government of India, *National Cyber Security Policy*, 2013.