

AI and Indian Knowledge System for Promoting Value-Based Cyber Safety among Students

DOI: <https://doi.org/10.63345/ijrhrs.net.v14.i8.2>

Priyanka Sharma

Assistant Professor

Laureate Institute of Education and Training
Shimla, Himachal Pradesh

Bharti Sharma

Research Scholar

Department of Education
Himachal Pradesh University, Summerhill, Shimla

Abstract— The rapid growth of digital technology has made students highly connected but also made them more vulnerable to cyber risks. Although Artificial Intelligence (AI) tools help in detecting and controlling the risks, they do not help in developing ethical understanding among students. Technology can protect, but only values can guide behaviour. This study highlighted the need to combine AI-based cyber safety tools with Indian Knowledge Systems (IKS) to promote values like dharma, satya, ahimsa, and self-discipline among students. This study is based on a qualitative approach by using secondary data and proposing the AI-IKS conceptual framework. This study suggests including these concepts in the school curriculum and teacher training programs. Overall, the study puts stress on combining the technology with values or the Indian Knowledge System for promoting safe and responsible digital behaviour among students.

Keywords: artificial intelligence (AI), cyber safety, values, Indian knowledge systems, AI-IKS framework

AI and Indian Knowledge Systems for Promoting Value-Based Cyber Safety among Students

In the 21st century, artificial intelligence has become an important part of our lives. It allows us to search for anything we want to know. Even in education, it is used in a more personalised way, according to the needs of students and teachers (Holmes et al., 2019). AI-based tools keep students more engaged and help them in learning according to their level (Luckin et al., 2016). While these tools facilitate learning, broaden social boundaries, and are useful in any pandemic situation, such as COVID-19, they also expose users to a variety of online threats. Students often do not have

enough awareness about online safety, and they are more vulnerable to cyber threats like phishing, cyberbullying, and identity theft (Livingstone et al., 2017; UNICEF, 2020). Nowadays, we hear or read about cyber fraud news almost every day. Cybercrime has emerged as a serious issue not only in India but around the world. In the last few years, cyber fraud, phishing, and other online scams have become much more common. The NCRB and PIB reported this in 2023 and 2025. Shadowed Beautiful Himachal Pradesh. Cybercrime has darkened the nation. Bad schemes have increased and become bolder in the digital age. Examples are online fraud, fake social media accounts and cryptocurrency scams (PIB, 2025; Tribune India, 2025). Cybersecurity for students and faculty is emphasised. Respect, honesty and responsibility are taught in India's Knowledge System. Students can stay safe, responsible, and respectful online with these virtues. This is crucial because the digital world is dangerous (Ministry of Education, 2020). Therefore, AI should be combined with cyber safety and ethical education to help students learn better and be aware, safe, and responsible in the digital world.

Literature Review

This study is based on technological and ethical perspectives to understand cyber safety. Social learning theory (Bandura, 1977) explains that students learn whatever they observe or experience. Students develop unsafe or harmful online behavior when using digital platforms without any proper guidance. AI has improved learning by making it more personalised according to the level of students and more engaging (Luckin et al., 2016; Holmes et al., 2019), but the increasing use of the internet has also increased cyber risks. Studies show that due to a lack of awareness and digital literacy, students are more vulnerable to online threats (Livingstone et al., 2017). Ribble (2015) explains in his study

about digital citizenship. This study highlighted that students should be aware, respectful, and responsible when they use digital platforms. Hinduja and Patchin (2018) highlighted that cyberbullying has become a serious issue due to a lack of awareness and preventive education. Solove (2008) discusses the importance of data privacy. Cyber security issues cause many human behaviours, say Parsons et al. (2017). Russell and Norvig (2021) mention that AI based on algorithms lack morality and cannot facilitate ethical behaviour. UNESCO (2021) stresses on technology and ethical and human values to prepare students for digital participation. Value-based education is important in India. Students learn character, discipline, ethics and responsibility through Indian Knowledge Systems (IKS) (Sharma, 2019). A 2020 National Education Policy mentions Indian Knowledge Systems to promote ethics. But most of the studies either talk about technology or ethics. There is very little research that combines AI, cyber safety, and ethical values. This study tries to fill this gap by combining an AI tool with Indian Knowledge Systems so that students learn about cyber safety and digital ethics.

Objectives

Objectives of the study are:

- To study AI-based cyber safety tools used for protecting students from online risks.
- To analyse the role of Indian Knowledge Systems (IKS) in shaping digital ethics among students.
- To develop an AI-IKS integrated framework for promoting value-based cyber safety.
- To suggest recommendations for integrating AI tools and IKS in schools.

Methodology

This study is based on a qualitative approach. The information has been collected from different secondary sources, like research papers, government reports (NCRB, PIB), and policy documents like NEP 2020 and UNICEF reports. These sources are carefully studied to understand the cyber safety issues, use of AI tools, and the role of Indian Knowledge Systems. So the research mainly depends on literature review and document analysis to explore the content.

AI-Based Cyber Safety Tools

AI-based cyber safety tools like Bark, QUSTODIO, Net Nanny, GoGuardian, Securly, and Google Family Link are being used nowadays (Indian Cyber Squad, n.d.). Bark analyzes the message and detects cyberbullying and harmful content. Qustodio helps in controlling screen time and blocking unsafe websites. GoGuardian and security tools are

used to monitor students' activity and safe browsing in educational environments.

Table 1: AI-Based Cyber Safety Tools and Their Functions

AI Tool Name	Function
Bark	Bark primarily checks messages and social media. It tells parents or schools if there is any bullying or something harmful, so they can step in.
Qustodio	Qustodio helps in managing screen time and keeps track of what students are doing online. It also blocks unsafe websites, so things don't go wrong.
Net Nanny	It works in real time. Net Nanny blocks bad websites, images, or videos, so students don't accidentally see anything inappropriate.
Go Guardian	The most used AI tool in schools is GoGuardian to see what students are doing online and to stop any unsafe searches during study time.
Securly	Securly can even detect serious things like bullying or self-harm and quickly alert teachers so they can help.
Google Family Link	It is a free app for parents that helps to set a time limit on a child's device, approve or block apps, and see their location.

Source: Indian Cyber Squad (n.d.)

Table 1 indicates the AI tools and their functions in monitoring, filtering, and controlling the students' online activities. However, despite these advanced AI tools, misuse of technology, cyberbullying, and fake information continue. The reason is, firstly, AI only focuses on detecting and controlling behaviour, not developing ethical understanding among students, and secondly, these tools have limited free editions; some are highly costly, which parents and schools cannot afford. It is clearly visible that cyber safety cannot be achieved through technology alone; it can be achieved by combining AI tools and IKS-based value education.

To Analyse the Role of Indian Knowledge Systems (IKS) in Shaping Digital Ethics

We are living in a digital world, where technologies are used for communication, for studies, news, entertainment, and many other things. Along with the benefits, many problems are also increasing, like cyber safety issues, fake

news, privacy issues, and misuse of technologies (Livingstone et al., 2017; UNICEF, 2020). In this context, the Indian Knowledge System became useful for inculcating human values like speaking the truth, doing the right things, not harming others, and maintaining self-control. According to NEP 2020, education should provide technical knowledge along with ethical thinking, respect, and responsibility (Ministry of Education, 2020). Ethical principles of the Indian knowledge system, like Dharma, satya, ahimsa, and self-discipline, can guide students in online behavior (Sharma, 2019). If students follow the idea of satya, they will not spread any fake news. If they understand ahimsa, they will avoid hurting others online or cyberbullying. Similarly, self-discipline helps them in controlling excessive screen time and avoiding addiction to games or social media. The All India Council for Technical Education has created the IKS division to bring these traditional values into modern education, digital, and technical fields. According to PIB (2023-2025), several IKS centres have introduced courses and training to teachers regarding IKS (Press Information Bureau, 2023).

AI is doing a great job in detecting cyber threats like hacking, phishing, and cyberbullying. But AI works on data and algorithms, which means that it does not understand what is right and what is wrong naturally (Russell & Norvig, 2021). So, the Indian knowledge system became really useful for this. How is it useful?

Helps in values and ethical thinking: The Indian Knowledge System helps in adding values and ethical thinking. For example, the IKS ethical principle “dharma” means doing the right things, which helps the AI system to act responsibly and fairly. The principle of satya means truth, which AI focuses on identifying and reducing fake information. Ahimsa, another principle of IKS help students in promoting respectful digital behaviour and reducing cyberbullying (Sharma, 2019).

Self-discipline and control: In this era, many students are facing problems like screen addiction and misuse of technology. The teaching of Patanjali yoga sutras focuses on self-discipline and self-control, which can help students to manage digital behaviour properly (Bryant, 2009).

Makes AI more human-centred: According to NEP 2020, education should be that which develops human skills as well as values. When AI is combined with IKS, it becomes more focused on human values, well-being, safety, and fairness rather than only providing technical performance.

Fairness and reduced bias: Many times, AI makes biased decisions, the reason being that they depend on data only. But when we include values like equality and justice from IKS, it will help in making these systems fairer. Researchers like Floridi et al. (2018) put importance on ethics in building responsible AI systems.

Threat detection with ethical support: AI tools in schools detect unsafe websites, harmful content, and suspicious online activities. When AI tools combine with IKS values, they will not only detect threats but also promote safe and responsible behaviour among students (UNICEF, 2020).

Awareness of cyber safety: By combining IKS with AI tools, it will help students to become aware of cyber risks like phishing, scams, and privacy misuse from an early age.

Balance between technology and values: AI provides technical protection, but IKS provides moral guidance. By combining both, it ensures effective and ethical cyber safety practices in school (Russell & Norvig, 2021).

Integrating AI tools with IKS: By combining both, AI protects and IKS guides.

Table 2: Integration of AI Tools with Indian Knowledge System (IKS) Values

Tool Name	IKS Value Added	Outcome in Cyber Safety (Students)
Bark	Ahimsa (non-violence)	Students avoid hurting others online and reduce bullying when the IKS value is combined with AI tools.
Qustodio	Self-discipline (Yoga philosophy)	Better control over screen usage, reduced addiction
Net Nanny	Satya (truth)	Students avoid false/misleading content
GoGuardian	Dharma (responsibility)	Responsible use of school devices and the internet
Securly	Social responsibility	Safer school digital environment and awareness
Google Family Link	Parental guidance (Seva & Dharma)	Parents’ guide children’s online activity, better screen

		time control, and safer internet use.
--	--	---------------------------------------

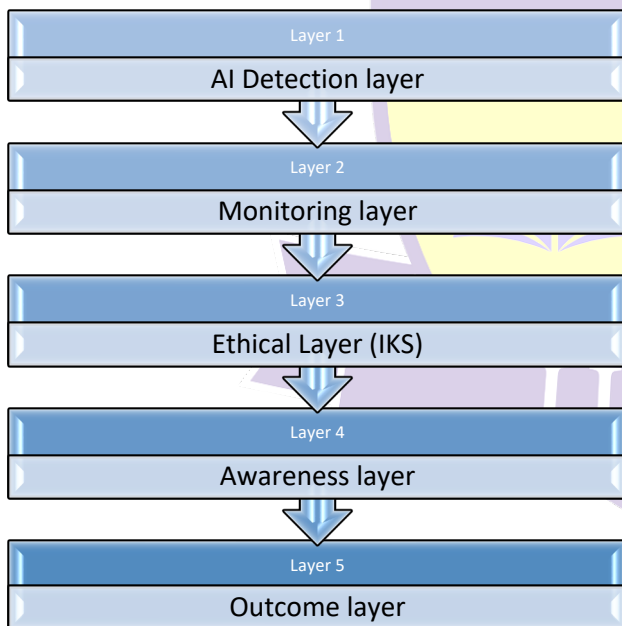
Source: Author's compilation based on Sharma (2019), NEP (2020), and UNICEF (2020)

Table 2 highlights how AI tools can integrate with IKS to promote ethical, safe, and responsible digital behaviour of students. This integration supports the holistic approach to cyber safety.

Proposed AI-IKS Integrated Framework for Value-Based Cyber Safety among Students

Based on the existing literature and findings of the study, an integrated framework is proposed for effective cyber safety among students. It is the combined efforts of technology, parents, teachers, and students to ensure effective cyber safety. This framework has five layers. These layers are:

AI-IKS Integrated Framework Layers



Source: Compiled by the researcher from various sources

Layer No.	Layer Name	Description
Layer 1	AI Detection Layer	This layer focuses on detecting cyber safety threats with the help of AI-based tools. In this layer, cyberbullying, phishing, and harmful content will be detected (Holmes et al., 2019).

Layer 2	Monitoring Layer	This layer helps in controlling the screen time of children and helps in blocking harmful websites to protect them from cyber fraud (UNICEF, 2020).
Layer 3	Ethical Layer (IKS)	This is a very important layer that helps students in understanding values like dharma, satya, ahimsa, and self-discipline (Ministry of Education, 2020; Sharma, 2019).
Layer 4	Awareness Layer	In this layer, students will be taught about online risks. When students know about online risks like phishing, cyber fraud, etc., they become aware of cyber fraud (Livingstone et al., 2017).
Layer 5	Outcome Layer	The last layer makes students responsible, ethical, safe, and respectful digital users. This framework shows that good values and awareness are needed with technology (Floridi et al., 2018).

This proposed framework highlights that cyber safety cannot be achieved alone through technology. There is a need to integrate ethical values and awareness along with AI tools. This proposed framework emphasizes the holistic approach where technology ensures protection and values guide the behaviour of students. This framework is conceptual in nature, based on existing studies, and has not been tested.

Recommendations

- Cyber ethics and morality classes ought to be required in school curricula. Use of cyber safety tools powered by AI requires prudence and moral direction. Schools and parents should have free access to these resources.
- Educators should acquire proficiency in AI tools to better instruct their students in the proper and ethical use of technology.
- Conduct regular workshops and awareness programmes on digital ethics, phishing, cyberbullying and online fraud.
- There is a need for government and educational bodies to come up with policies that integrate the Indian Knowledge System or ethics education along with technology.
- Parents need to know about digital dangers, watch their children's online actions and guide them.

- Students should be motivated to adopt the Indian Knowledge System-based values while using digital platforms.
- Schools should use this AI-IKS framework by combining AI tools, ethical education and awareness programs to improve cyber safety.
- These concepts should also be introduced in teacher training programs and curriculum, for both in-service and pre-service, so that they can guide students properly.

Conclusion

In this digital era, students are using technology but also facing many cyber safety issues like fraud, bullying, fake information, and many others. AI tools help in detecting and controlling these problems, but the issue is that they cannot teach students what is right and what is wrong. This paper shows that only providing technology knowledge is not enough. Indian Knowledge System values help students behave properly and safely online. Therefore, combining AI with value-based education makes students safe, responsible, and digitally aware users, and these concepts should also be included in teacher training and curriculum for both in-service and pre-service.

References

1. Sharma, C. (2025). Ethics and morality in the Indian knowledge system: A framework of values-based education. *Advanced International Journal for Research*, 6(6), 1–18. <https://www.aijfr.com/papers/2025/6/2321.pdf>
2. Government of India, Ministry of Human Resource Development. (2020). *National education policy 2020*. https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English.pdf
3. Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial intelligence in education: Promise and implications for teaching and learning*. Center for Curriculum Redesign. <https://curriculumredesign.org/wp-content/uploads/AIED-Book-Excerpt-CCR.pdf>
4. Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). *Intelligence unleashed: An argument for AI in education*. Pearson. <https://www.pearson.com/content/dam/corporate/global/pearson-dot-com/files/innovation/Intelligence-Unleashed-Publication.pdf>
5. Livingstone, S., Mascheroni, G., & Staksrud, E. (2018). European research on children's internet use: *Assessing the past and anticipating the future*. *New Media & Society*, 20(3), 1103–1122. https://researchonline.lse.ac.uk/id/eprint/68516/1/Livingstone_European%20Research%20on%20Children_2018.pdf
6. UNICEF. (2022). *Child online protection in and through digital learning: Considerations for decision-makers*. <https://www.unicef.org/eca/media/22501/file>
7. International Telecommunication Union. (2020). Guidelines for policy-makers on Child Online Protection. https://www.itu-cop-guidelines.com/files/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf
8. National Crime Records Bureau. (2023). *Crime in India—Table content*. Ministry of Home Affairs, Government of India. <https://www.ncrb.gov.in/crime-in-india-table-content.html?year=2023>
9. Press Information Bureau. (2025). *Cyber crime statistics in India*. Government of India. <https://pib.gov.in>
10. Our Correspondent. (2026, March 18). Cyber fraud network involving Rs 40 crore busted in Gurugram, 10 arrested. *The Tribune*. <https://www.tribuneindia.com/news/delhi/cyber-fraud-network-involving-rs-40-crore-busted-in-gurugram-10-arrested/>
11. Indian Cyber Squad. (n.d.). *Parental control software: A guide for parents*. <https://www.indiancybersquad.org/parental-control-software>
12. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Vayena, E. (2018). AI4People: *An ethical framework for a good AI society*. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
13. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
14. Solove, D. J. (2008). *Understanding privacy*. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888
15. Hinduja, S., & Patchin, J. W. (2018). *Cyberbullying: Identification, prevention, and response*. Cyberbullying Research Center. <https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2018.pdf>
16. Tribune News Service. (2026, February 21). *Himachal sees surge in cybercrimes, 18,706 complaints in 2025*. *The Tribune*. <https://www.tribuneindia.com/news/himachal/himachal-sees-surge-in-cybercrimes-18706-complaints-in-2025/>
17. Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press. <https://www.hup.harvard.edu/books/9780674987555>
18. Bandura, A. (1977). *Social learning theory*. Prentice Hall. https://ia601807.us.archive.org/14/items/BanduraSocialLearningTheory/Bandura_SocialLearningTheory_text.pdf
19. Ribble, M. (2015). *Digital citizenship in schools* (3rd ed.). International Society for Technology in Education. https://archive.org/details/digitalcitizensh0000ribb_x4u3
20. Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson. <https://aima.cs.berkeley.edu/>