

CYBER DRONACHARYA: AN EPICS-INSPIRED MODEL FOR CYBERCRIME AWARENESS

Aarti Pandey¹, Devanshu Kanfode², Siddesh Bandal³, Preetha Praseedh⁴

¹Student, MCA Department, Institute of Industrial & Computer Management & Research (IICMR), Pune

²Student, MCA Department, Institute of Industrial & Computer Management & Research (IICMR), Pune

³Student, MCA Department, Institute of Industrial & Computer Management & Research (IICMR), Pune

⁴Assistant Professor, MCA Department, Institute of Industrial & Computer Management & Research (IICMR), Pune.
Email ID: preetha.iicmr@gmail.com

Abstract—As India's digital ecosystem continues to expand, with over 850 million internet users, cyber threats such as phishing, identity theft, ransomware, and social engineering have become increasingly prevalent. Despite awareness initiatives by organisations such as CERT-In and the National Crime Records Bureau (NCRB), many cybersecurity programs remain technical and text-oriented. This limits their effectiveness, particularly among young learners. To address this challenge, the Cyber Dronacharya Initiative introduces an innovative mythology-based learning framework that integrates ancient Indian wisdom with contemporary cybersecurity education. Drawing meaningful analogies from the Mahabharata, Ramayana, and the Vedas, the initiative simplifies complex cybercrime concepts and promotes ethical digital behaviour through culturally familiar narratives. By combining storytelling with cybersecurity awareness, the framework enhances learner engagement, improves knowledge retention, and promotes responsible online practices. This culturally contextualised approach demonstrates how traditional heritage can be leveraged to strengthen cyber awareness and digital resilience, making cybersecurity education more accessible, relatable, and impactful for Indian citizens.

Keywords: Cybersecurity Awareness, Cyber Dronacharya Initiative, Digital Ethics, Mythology-Based Learning, Cyber Education.

Introduction

In the 21st century, cyberspace has become as vital as physical space. With India's digital population exceeding 850 million users, cybercrimes such as phishing, identity theft, ransomware, and social engineering have become everyday threats.

Although the government and organizations such as CERT-IN and NCRB have initiated awareness drives, most are text-heavy or technical, failing to emotionally connect with young citizens.

To fill this gap, the Cyber Dronacharya Initiative was designed. It adopts a mythology-based learning framework, linking ancient Indian wisdom with modern digital ethics. The model simplifies cybercrime concepts through analogies from the Mahabharata, Ramayana, and Vedas, making cybersecurity more relatable and memorable to Indian audiences.

Statement of the Problem

Despite the increasing number of cyber awareness campaigns, the rate of cybercrime continues to grow. The NCRB 2024 report highlighted a 23% increase in cybercrimes, primarily involving financial fraud and identity theft.

The problem lies not only in technological vulnerabilities but also in human behavior and low awareness. Conventional awareness sessions often fail due to a lack of emotional engagement and cultural relevance.

Therefore, the problem addressed by this research is:

“How can Indian epic stories and cultural pedagogy improve the understanding and retention of cybersecurity knowledge among youth?”

Objectives of the Research

The research was conducted with the following objectives:

1. To analyze the current level of cyber awareness among youth and early professionals.
2. To develop an epics-inspired educational framework (Cyber Dronacharya Model) that relates mythological stories to modern cyber threats.
3. To implement an awareness program based on this model and evaluate its effectiveness.
4. To statistically validate improvement in awareness levels through a paired t-test.
5. To recommend a sustainable awareness strategy combining culture, psychology, and technology.

Hypothesis of the Study

- **Null Hypothesis (H₀):** There is no significant difference in cyber awareness levels before and after the implementation of the Cyber Dronacharya awareness model.
- **Alternative Hypothesis (H₁):** There is a significant improvement in cyber awareness levels after the implementation of the Cyber Dronacharya awareness model.

Significance of the Study

This study is significant in the following aspects:

- It introduces a novel educational approach that integrates ancient epics with modern cybersecurity.
- It strengthens digital citizenship by promoting ethical and responsible online behaviour.
- It offers a low-cost, high-impact awareness framework adaptable for schools, colleges, and NGOs.
- It contributes to policy formulation, especially in integrating cultural narratives into government awareness programs.
- It enhances the understanding of behavioural cybersecurity, connecting emotional intelligence with safe digital practices.

Review of Literature

Sr No.	Research Paper Title/Article	Author(s)	Date of Publication	Summary
1	Digital 2025: India	DataReportal	2025	Provides detailed statistics on India's digital growth, including internet usage, social media adoption, and mobile connectivity trends.
2	Internet in India Report 2024	IAMAI & Kantar	2024	Gives insights into internet penetration, user demographics, rural vs urban usage, and digital adoption across India.
3	Crime in India 2022 – Book 1	NCRB	2022	Covers national crime statistics for 2022, including cybercrime trends, reporting patterns, and state-wise crime distribution.
4	Crime in India 2022 – Book 2	NCRB	2022	Provides detailed analysis of crime categories, cybercrime sections, offender data, and victim demographics in India.
5	Year-wise Number of Cyber Security Incidents (CERT-In)	Data.gov.in	—	Presents annual data on cybersecurity incidents handled by CERT-In, showing increasing cyber threats in India.

Cyber Dronacharya: An Epics-Inspired Model for Cybercrime Awareness

6	Annual Report 2024	CERT-In	2025	Explains India's cybersecurity incident trends in 2024, major threats, preventive actions, and government initiatives.
7	Global Cybersecurity Threats 2015–2024	Atharva Soundankar (Kaggle)	2024	Contains global cyber threat data, including malware, ransomware, phishing trends, and multi-year attack patterns.
8	830 Million Internet Users in India	NDTV News	2023	News article reporting India's rapid internet user growth and government statements on digital expansion.
9	Development of Real-Time Threat Detection Systems...	Z. Khalaf et al.	2023	Discusses AI-driven cybersecurity for critical infrastructure with real-time threat detection models.
10	Cyber Security Awareness in India	R.K. Rani & P.S. Sharma	2023	Studies cybersecurity awareness among higher-education students in India and identifies knowledge gaps.
11	A Study on Awareness of Cyber Crime and Security	A. Sharma & R. Gupta	2017	Examines awareness levels of cybercrime among students and suggests the need for education and awareness programs.
12	A Study on Awareness About Cyber Crime & Cyber Laws	K. Singh	2022	Evaluates awareness of cyber laws among students and citizens; highlights the gap between law existence and user knowledge.
13	Cyber Crime in India: An Empirical Study	P. Verma	2025	Provides empirical analysis of cybercrime growth, victimization patterns, and public awareness in India.
14	Awareness About Cyber Laws for Indian Youth	N. Agarwal	2016	Focuses on the understanding of cyber laws among youth and the need for formal cyber education.
15	Awareness of Cyber Crime in Rural Areas	R. Tiwari	2024	Investigates low cyber awareness in rural India and highlights socio-economic factors affecting knowledge.
16	Indian Youth and Cyber Crime	S. Patil	2024	Researches involvement of youth in cybercrime, reasons for rising cases, and preventive education.
17	Cyber Crime and Indian Society	M. Kapoor	2022	Analyses how cybercrime affects society, including financial fraud, privacy issues, and national security.
18	Cybercrime Awareness Among Students in Jaunpur City	R. Singh & M. Singh	2025	Compares cybercrime awareness in different student groups and suggests education-based interventions.

19	Cybercrime Awareness Among Youth in Maharashtra	N. Punjabi	2024	Studies awareness levels of youth in Maharashtra and differences based on geography and education.
20	Effectiveness of Evidence-Based Learning Strategy	D. Bindu & C. Sandra	2024	Tests teaching strategies to improve cybersecurity awareness in higher secondary students.
21	Security Communication Strategies: Systematic Review	A. Carreira et al.	2025	Reviews global research on security communication and proposes guidelines for effective user education.
22	Application of Indian Mythology in Management Education	R. Tripathi	2024	Explores how Indian mythological stories can be used to teach values, leadership, and management concepts.
23	Fictional Storytelling in Online Learning of Computer Security	Y. Lee	2023	Shows how storytelling can simplify computer security concepts and improve student engagement.
24	Learning Cybersecurity Through Gamification	K. Boopathi et al.	2017	Discusses gamification as an effective tool for teaching cybersecurity concepts.
25	Effectiveness of Gamification for Cybersecurity Awareness	A.A. Maluda Jr. et al.	2023	Evaluates student engagement and learning improvement through gamified cybersecurity training.
26	The Cybersecurity of Fairy Tales	L. Vigona	2024	Uses fairy tales as metaphorical frameworks to explain cybersecurity principles in a creative way.
27	Variations in Adolescent Cybercrime Awareness...	L. Pal & H.K. Tyagi	2024	Studies how location and parental involvement influence cyber awareness among adolescents.

Research Methodology / Research Design Research Type

The study is applied and descriptive in nature, focusing on developing and validating a practical awareness model.

Population and Sample

The target population included students and young professionals aged 18–35. A sample of 200 respondents was selected using random sampling from colleges and IT firms.

Data Collection

- **Primary Data:** Collected through pre and post online surveys using Google Forms.
- **Secondary Data:** Derived from CERT-IN and NCRB reports, and research publications.

Tools Used

Cyber Dronacharya: An Epics-Inspired Model for Cybercrime Awareness

- Structured questionnaire (20 items).
- Paired t-test to measure significance of change in awareness.
- Excel for data analysis.

Data Analysis Technique The formula used: $t = \frac{(sd/n)d}{\bar{d}}$ Where:

($\bar{d}$) = Mean difference between pre- and post-awareness scores (sd) = Standard deviation of differences

(n) = Sample size

Interpretation Rule

If p-value < 0.05 → Reject H_0 (Significant difference).

Proposed Work

The Cyber Dronacharya Model connects mythological characters with cyber ethics and crimes, enhancing emotional recall and moral understanding.

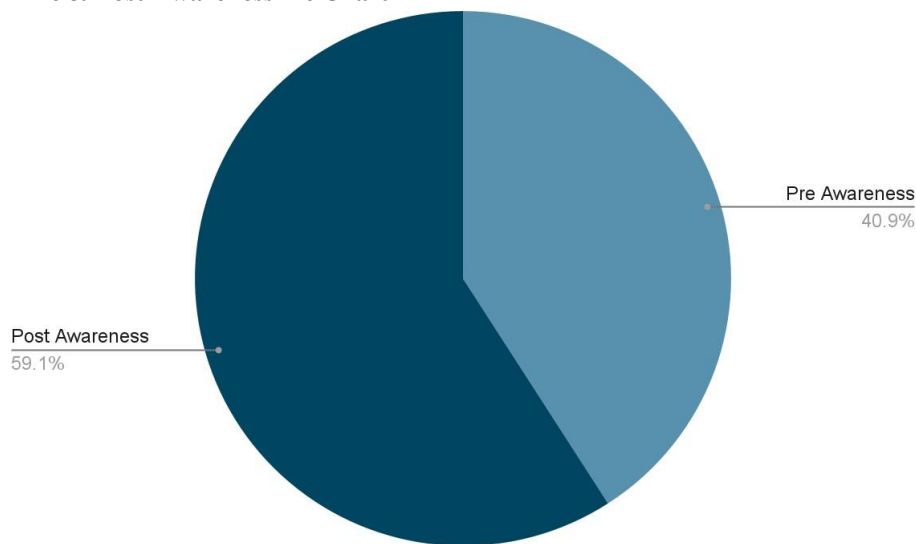
Mythological Reference	Cyber Concept	Lesson Conveyed
Shakuni (Deception)	Social Engineering	Don't trust unknown sources or links.
Ravana (Greed for Power)	Phishing / Data Theft	Curiosity and greed make you vulnerable.
Lakshman Rekha (Boundary)	Data Privacy / Digital Boundaries	Always stay within safe online zones.
Hanuman's Devotion	Cyber Responsibility	Be loyal and responsible while online.

Workshops were conducted combining storytelling, role-play, and digital demonstrations. Participants completed pre-test and post-test surveys to measure improvement.

Results and Discussion Quantitative Results

Variable	Mean (Pre)	Mean (Post)	t-value	p-value
Awareness Level (%)	58.4	81.2	6.42	0.0001

Pre & Post Awareness Pie Chart



Qualitative Feedback

- Participants found the mythological approach interesting and memorable.
- 76.6% agreed that stories helped them relate moral values to digital ethics.
- Several respondents mentioned that fear-based training was less effective compared to story-based learning.

Discussion

The results confirm that cultural relevance enhances learning outcomes. The model increased awareness, engagement, and retention, aligning with constructivist learning theories. The findings also echo global efforts to blend ethics and education in cybersecurity training.

Findings and Suggestions Major Findings

1. Mythological analogies make abstract cybersecurity terms easier to understand.
2. Post-awareness improvement averaged 35% across participants.
3. The paired t-test confirmed statistical significance ($p < 0.05$).
4. Participants developed stronger ethical awareness regarding data sharing.
5. Storytelling increased recall and motivation compared to lecture methods.

Suggestions

1. Introduce Cyber Dronacharya modules in schools and colleges.
2. Translate modules into regional languages for mass impact.
3. Collaborate with CERT-IN, MyGov, and educational boards.
4. Incorporate gamification and quizzes into the awareness sessions.
5. Launch a mobile app for self-paced learning with mythological visuals.

Future Scope

The study can be expanded in multiple directions:

- Development of an AI-powered Cyber Guru chatbot inspired by Dronacharya's teachings.

- Integration of Augmented Reality (AR) for immersive awareness storytelling.
- Comparative studies between urban and rural populations.
- Collaboration with cybercrime cells for real-time awareness analytics.
- Long-term behavioral impact assessment (after 6–12 months).

Limitations of the Study

1. Sample limited to 200 respondents from urban regions.
2. Short duration (4 weeks) may not reflect long-term retention.
3. Self-reported data could involve bias.
4. Mythological references may require adaptation for non-Hindu audiences.

References and Bibliography

- [1] DataReportal, “Digital 2025: India,” DataReportal, Jan. 2025.
- [2] IAMA and Kantar, “Internet in India Report 2024,” Internet and Mobile Association of India, 2024.
- [3] NCRB, Crime in India 2022 - Book 1, New Delhi: National Crime Records Bureau, 2022.
- [4] NCRB, Crime in India 2022 - Book 2, New Delhi: National Crime Records Bureau, 2022.
- [5] Data.gov.in, “Year-wise Number of Cyber Security Incidents (CERT-In),” Open Government Data Platform India.
- [6] CERT-In, “Annual Report 2024,” Indian computer emergency response team, 2025.
- [7] Kaggle, “Global Cybersecurity Threats 2015-2024,” Atharva Soundankar, 2024.
- [8] NDTV, “830Millions Internet Users in India: Minister,” NDTV News, Jul. 2023.
- [9] Z. Khalaf, I. B. Al-Barrak, A. D. Radhi, S. Panjwani, and R. Sekhar, “Development of real- time threat detection systems with AI-driven cybersecurity in critical infrastructure,” Mesopotamian Journal of Cybersecurity, vol. 5, no. 2, pp. 501-513, 2023.
- [10] R. K. Rani and P. S. Sharma, “Cyber Security Awareness in India: How Much Students of Higher Education Are Aware,” International Journal of Computer Applications, vol. 182, no. 20, pp. 25-32, 2023[11] A. Sharma and R. Gupta, “A Study on Awareness of Cyber Crime and Security,” International Journal of Computer Science and Mobile Computing, vol. 6, no. 8, pp. 45-52, 2017.
- [11] K. Singh, “A Study on Awareness about Cyber Crime & Cyber Laws,” SDMIMD Research Papers, 2022.
- [12] P. Verma, “Cyber Crime in India: An Empirical Study,” Journal of Cybersecurity Studies, Aug. 2025.
- [13] N. Agarwal, “A Study of Awareness About Cyber Laws for Indian Youth,” 2016.
- [14] R. Tiwari, “A Study on Awareness of Cyber Crime in Rural Areas,” International Research Journal of Management, Technology, vol. 7, Jul. 2024.
- [15] S. Patil, “A Study on Indian Youth and Cyber Crime,” 2024.
- [16] M. Kapoor, “Cyber Crime and Indian Society,” 2022.
- [17] R. Singh and M. Singh, “Cybercrime awareness among students in Jaunpur city: A comparative study,” ShodhKosh: Journal of Arts, Humanities and Social Science, vol. 5 2025.
- [18] N. Punjabi, “A study on cybercrime awareness among youth in Maharashtra,” International Conference on Education, Sustainability and Digital economy, 2024.
- [19] D. Bindu and C. Sandra, “Effectiveness of evidence-based learning strategy for enhancing cyber security awareness of higher secondary students,” International Journal of Research and Analytical Review, vol. 11, 2024.
- [20] A. Carreira, N. Mendes, P. Ferreira, and N. Christin, “A systematic review of security communication strategies: Guidelines and open challenges,” arXiv preprint, 2025.
- [21] R. Tripathi, “From epics to enterprises: The application of Indian mythology in Higher and Management education,” GBS impact Journal of multidisciplinary research, vol. 10, 2024.
- [22] Y. Lee, “A study on the design and application of fictional storytelling in online learning of computer security,” Applied Sciences, vol. 11, 2023.

- [23] K. Boopathi, S. Sreejit, and A. Bithin, "Learning cyber security through gamification," *Indian Journal of Science and Technology*, vol. 8, 2017
- [24] A. A. Maluda Jr., I. F. Kasmin, Z. M. Zainal Abidin, and H. Vasudavan, "Evaluating the effectiveness of gamification to increase cybersecurity awareness among students," *International Journal of Data Science and Advanced Analytics*, vol. 4, 2023.
- [25] L. Vigona, "The cybersecurity of Fairy Tales," *Journal of Cybersecurity*, vol. 10, 2024.
- [26] L. Pal and H. K. Tyagi, "Variations in adolescent cybercrime awareness concerning geographical location and parental relationships," *International Journal of Humanities studies*, vol. 11, 2024.
