DRA Annual International Conference On
Developed India @2047: Global Pathways for Sustainable Socio- Economic, Linguistic, Science and Technological Transformation

Ind. Jr. of Mod. Res. and Rev *PEER-REVIEWED JOURNAL* *Volume 4 [Special Issue 1] Year 2026*

Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Article

Critical Issues at the Intersection of Cybersecurity and Artificial Intelligence in Developing India

Dr. Smith Vyas
Assistant Professor, Department of Law, Dr. Anushka Vidhi Mahavidhyalaya, Udaipur, Rajasthan, India

Corresponding Author: *Dr. Smith Vyas

DOI: https://doi.org/10.5281/zenodo.21450057

Abstract

India's rapid digital development has created a complex environment where cybersecurity and artificial intelligence (AI) gradually intersect, shaping both national opportunities and vulnerabilities. As government services, financial organizations, healthcare networks, and critical infrastructure undergo enhanced digitization, the integration of AI into these systems offers transformative potential. AI-enabled tools can strengthen cyber-defense through predictive analytics, automated threat detection, and real-time incident response. Yet, these same technologies introduce new layers of risk, including adversarial attacks, data manipulation, deepfake-driven misinformation, and autonomous cyber-exploits that challenge traditional security frameworks. For a developing India, these challenges are intensified by uneven digital literacy, infrastructural disparities, and limited cybersecurity capacity across institutions. The rapid adoption of AI without parallel advancements in regulation, ethical governance, and workforce readiness creates gaps that malicious actors can exploit. Issues such as privacy protection, algorithmic bias, data sovereignty, and the security of large-scale digital identity systems further complicate the landscape. As India positions itself as a global digital leader, addressing these vulnerabilities becomes essential to safeguarding national security, economic stability, and citizen trust. This research paper seeks to examine the critical issues emerging at the intersection of cybersecurity and AI in developing India. It aims to bring together experts from academia, industry, and government to explore strategic pathways for building a resilient digital ecosystem. Key themes include responsible AI deployment, adaptive regulatory frameworks, capacity building, public-private collaboration, and the development of indigenous technologies tailored to India's socio-economic context. This paper will be focused on examining the critical challenges, risks, and opportunities that arise at the intersection of cybersecurity and artificial intelligence (AI) within the context of a developing India.This paper presents an overview on how cybersecurity vulnerabilities and artificial intelligence technologies interact in developing India, highlighting the major threats, governance gaps, socio-economic constraints, and potential pathways for building a secure and resilient digital ecosystem.

Manuscript Information

- **ISSN No:** 2584-184X
- **Received:** 01-01-2026
- **Accepted:** 25-06-2026
- **Published:** 05-07-2026
- **MRR:**4(SP1); 2026: 307-312
- **©2026, All Rights Reserved**
- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Vyas S. Critical Issues at the Intersection of Cybersecurity and Artificial Intelligence in Developing India. Indian J Mod Res Rev. 2026;4(SP1):307-312.

Access this Article Online

www.mrrjournal.in

KEYWORDS: Cyber Space, Cyber-Security, Artificial Intelligence, e-governance, and e-commerce.

© 2026 Dr. Smith Vyas. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

INTRODUCTION

India's rapid shift toward a digital economy has transformed the way citizens interact, businesses operate, and governments deliver services. With expanding internet penetration, widespread adoption of smartphones, and the growth of digital platforms such as e-governance, digital payments, and online marketplaces, the nation is experiencing an unprecedented technological evolution. At the center of this transformation lie two powerful forces: **cybersecurity** and **artificial intelligence (AI)**. While both are essential for enabling innovation and efficiency, they also introduce a new set of challenges that developing India must urgently address.

Cybersecurity has become a national priority as cyber threats grow in scale, sophistication, and impact. India faces rising incidents of data breaches, ransomware attacks, identity theft, and vulnerabilities in critical infrastructure. Limited digital literacy, inadequate security practices, and uneven implementation of regulatory frameworks further complicate the situation. As more services move online, the risks associated with weak cyber hygiene and insufficient protection mechanisms become increasingly severe.

Simultaneously, AI is emerging as a transformative technology with applications in healthcare, agriculture, governance, finance, and public services. However, its rapid adoption brings concerns related to data privacy, algorithmic bias, lack of transparency, and potential misuse of AI-driven systems. In a developing nation like India where digital ecosystems are still maturing these issues pose significant ethical, social, and security challenges.

The intersection of cybersecurity and AI therefore represents a critical area of concern. AI can strengthen cyber defense through predictive analytics and automated threat detection, yet it can also be exploited to create more advanced cyberattacks. Understanding this dual nature is essential for shaping India's digital future. This introduction sets the stage for examining the key issues, emerging risks, and strategic imperatives required to build a secure, trustworthy, and resilient technological environment in developing India.

Cybersecurity has become an essential component of modern information management. As digital technologies continue to expand, protecting personal data and ensuring privacy have turned into some of the most challenging responsibilities of the digital age. Although the idea of cyber protection is widely acknowledged, defining it clearly remains difficult. Over time, it has often been confused with related concepts such as anonymity, information exchange, intelligence gathering, and digital surveillance.

In today's information-centric world, the need for a strong data-security framework to shield the growing ICT infrastructure is more critical than ever. ICT systems serve as the backbone for all major national infrastructures, making their security requisite. The rapid rise of e-governance and e-commerce initiatives across the globe further highlights the importance of having a dependable cybersecurity model to support this digital development.

Cyber Security: -Cybersecurity is the practice of protecting computers, networks, data, and digital systems from attacks, damage, or unauthorized access. In simple terms, it's all about keeping information safe from hackers and other online threats. Cybersecurity focuses on protecting data from being stolen or leaked, securing networks so attackers can't break in, preventing malware like viruses and ransomware, ensuring systems stay available and don't get shut down by cyber-attacks. Cyber security matters in everything today like banking, shopping, communication, even government systems run on technology. Without cybersecurity, all of that becomes vulnerable.

Artificial Intelligent (AI): AI or artificial intelligence, is the field of computer science focused on creating machines that can perform tasks that normally require human intelligence. Think of it as teaching computers to learn, reason, solve problems, understand language, and make decisions. AI actually does learn from data like how apps predict what you want to watch, understands language like chatbots and voice assistants, recognizes patterns such as identifying faces or detecting fraud and makes decisions — from recommending products to helping drive cars. AI is everywhere now like in phones, cars, hospitals, games, and even agriculture. It's shaping the future in a big way.

Intersection of Cybersecurity and Artificial Intelligence: - The rapid evolution of digital technologies has brought us to a defining moment where cybersecurity and artificial intelligence converge to reshape the future of global security. As organizations increasingly rely on interconnected systems, the threats they face have grown more sophisticated. At the same time, AI has emerged as a transformative force capable of enhancing defenses, predicting attacks, and automating complex security operations. This intersection represents not just a technological advancement but a strategic necessity for the digital age.

Cybersecurity has traditionally relied on human expertise, rule-based systems, and reactive approaches. However, the scale and speed of modern cyber threats demand more adaptive and intelligent solutions. This is where AI plays a pivotal role. Machine learning models can analyze vast datasets, detect anomalies, and identify malicious patterns far faster than human analysts. AI-powered threat detection systems continuously learn from new data, enabling them to recognize emerging attack vectors and respond in real time. This shift from reactive to proactive security marks a major milestone in the evolution of digital defense.

At the same time, AI itself introduces new security challenges. As AI systems become integrated into critical infrastructure, healthcare, finance, and national security, they become attractive targets for cybercriminals. Attacks such as data poisoning, adversarial manipulation, and model theft threaten the integrity and reliability of AI systems. Ensuring the security of AI models—both during training and deployment—has

© 2026 Dr. Smith Vyas. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

become a crucial component of modern cybersecurity strategies. Protecting AI is no longer optional; it is essential for maintaining trust in automated decision-making systems.

The synergy between AI and cybersecurity is also evident in automation. Security teams today face overwhelming workloads due to the volume of alerts and the complexity of modern networks. AI-driven automation helps streamline incident response, prioritize threats, and reduce human error. By handling repetitive tasks, AI allows cybersecurity professionals to focus on strategic decision-making and advanced threat analysis. This collaboration between human expertise and machine intelligence creates a more resilient and efficient security ecosystem.

However, the integration of AI into cybersecurity also raises ethical and governance considerations. Issues such as data privacy, algorithmic transparency, and responsible AI deployment must be addressed to ensure that these technologies are used safely and fairly. Collaboration between policymakers, researchers, and industry leaders is essential to establish standards that promote innovation while safeguarding public trust.

The intersection of cybersecurity and artificial intelligence represents one of the most dynamic and impactful areas of technological development today. AI enhances cybersecurity by enabling faster detection, smarter analysis, and automated response, while cybersecurity ensures that AI systems remain secure, reliable, and trustworthy. Together, they form the foundation of a safer digital future. As we move forward, embracing this synergy will be critical for protecting our digital world and unlocking the full potential of intelligent technologies.

Advantages of cyber-Security and AI: - In today's digital era, two forces are shaping our future.i.e. **Cybersecurity** and **Artificial Intelligence**. One safeguards our digital world, while the other empowers it with intelligence and innovation. Together, they form the backbone of trust and progress in the 21st century." Cybersecurity and Artificial Intelligence are two pillars shaping the digital future, each offering unique advantages that, when combined, create a powerful synergy for organizations and societies. Cybersecurity serves as the guardian of digital assets, protecting sensitive information from theft, misuse, and unauthorized access. It builds trust among customers and stakeholders, ensures compliance with regulatory standards, and maintains business continuity by preventing costly disruptions. By reducing financial losses associated with breaches and downtime, cybersecurity not only safeguards data but also strengthens the resilience of enterprises in an increasingly hostile digital environment. On the other hand, Artificial Intelligence acts as the engine of innovation and efficiency.

AI automates repetitive tasks, enabling humans to focus on creativity and strategic thinking. It enhances decision-making by analyzing vast datasets, offering predictive insights that drive smarter business strategies. AI also personalizes customer experiences, fuels the development of new products and services, and reduces risks by detecting fraud and predicting failures before they occur. Its ability to operate continuously without fatigue ensures round-the-clock productivity and responsiveness. Together, cybersecurity and AI form a complementary partnership: cybersecurity ensures safety and trust, while AI ensures progress and intelligence. This combination empowers organizations to innovate confidently, operate efficiently, and build resilience in a connected world. In essence, cybersecurity provides the shield, and AI provides the spear one defends against threats, the other drives advancement. As digital transformation accelerates, embracing both is no longer optional but essential for thriving in the modern era.

Key Issues at the Intersection of Cybersecurity and AI in India

The intersection of **cybersecurity** and **artificial intelligence (AI)** in India brings enormous opportunities but also a set of serious, fast-growing challenges. Based on recent reports and analyses, India is facing a surge in **AI-driven cyber threats**, rising vulnerabilities, and structural gaps in readiness. Below is a clear, conference-ready overview of the major issues, grounded in current information.

1. AI-Driven Cyberattacks Are Increasing Rapidly

India is experiencing a sharp rise in cyberattacks powered by AI, including automated malware, deepfake-based fraud, and sophisticated phishing. Trend Micro's 2025 report shows India ranks **2nd globally in email threats** and **3rd in malware detections**, highlighting how AI is amplifying attack scale and precision. Attackers use AI to craft convincing phishing emails. Malware can now mutate automatically using machine learning and Deepfake-based fraud is rising in financial and political domains are most important cyber threats in India.

2. AI Is Also Strengthening Attacks Like Brute Force & DDoS

AI tools can automate password cracking, accelerate reconnaissance, and optimize denial-of-service attacks, generate highly personalized messages, voices, and videos. This makes scams far more convincing. Reports note that India is seeing a surge in AI-powered impersonation and fraud attempts. India AI notes that AI is increasingly used in **brute-force attacks, DDoS campaigns, and social engineering**. Deepfake voice calls mimicking officials or family members and AI-generated scam messages targeting bank customers are main target of cyber fraud.

3. Inadequate and Weak AI Security Infrastructure

India's digital expansion is outpacing its security capabilities. As One India reports, many threats now originate **inside organizational networks**, and India's cybersecurity posture is struggling to keep up with rapid AI and cloud adoption. Many organizations still rely on outdated systems, making them vulnerable to AI-driven attacks. Analysts highlight that internal

© 2026 Dr. Smith Vyas. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

network threats are increasing as AI tools become more accessible. lack of skilled AI-security work force, Limited deployment of AI-based defense tools and Legacy systems unable to detect modern threats are main issues for Insufficient AI Security infrastructure

4. AI Systems Themselves Are Becoming Targets
As India deploys AI in banking, governance, and public services, attackers are targeting the AI models directly. Key risks include data poisoning corrupting training data, model theft stealing or replicating AI models and adversarial attacks tricking AI with manipulated inputs. These threats can compromise banking systems, biometric authentication, and government AI platforms.

5. Regulatory and Governance Gaps
India does not yet have a unified legal framework for AI security. While CERT-In is strengthening national cyber defense, experts note the need for clearer standards on AI governance, data protection, and model transparency still in India no dedicated AI securitylaw, Limited guidelines for responsible AI deployment. Need for stronger compliance frameworks and AI governance and AI model transparency.

6. Growing Threats to Critical Sectors
Banking, financial services, and government systems are the most targeted sectors in India's AI-driven threat landscape, identity theft, and attacks on digital public infrastructure are increasing. many more like financial institutions face AI-powered fraud attempts, Government digital services are frequent targets, Healthcare data is at risk due to weak security controls

7. Deepfake and Fabrication Risks
AI-generated deepfakes are becoming a major national-level concern, enabling political misinformation, financial scams, and impersonation attacks. India AI highlights deepfakes as a **massive emerging threat**. They can influence public opinion, damage reputations, or enable scams. Analysts warn that deepfake misuse is rising sharply in India. Deepfake political manipulation and AI-generated impersonation scams are major issues in developing India.

India stands at a critical point where AI is both **strengthening cybersecurity** and **intensifying cyber threats**. The biggest issues include AI-driven attacks, weak AI governance, vulnerable critical sectors, and the growing misuse of deepfakes. Addressing these challenges requires stronger regulation, AI-skilled cybersecurity professionals, and rapid adoption of AI-based defense systems.

Solutions: - India can absolutely tackle the challenges at the intersection of AI and cybersecurity, but it requires coordinated action across technology, policy, workforce, and infrastructure. Based on the latest insights from national cybersecurity reports and expert analyses, here are the strongest, evidence-backed solutions. India's AI boom brings sharper threats and bigger opportunities. Solving the cybersecurity–AI nexus demands technical hardening, trustworthy AI governance, sector-specific controls, and India-first capacity building that matches the country's scale and risk profile
India can overcome AI-cybersecurity challenges by combining AI-powered defense, strong governance, skilled talent, and sector-specific protections. With CERT-In's growing AI initiatives and rising national awareness, India is already moving in the right direction but scaling these solutions is essential for long-term digital safety.

Solutions to Issues at the Intersection of Cybersecurity and AI in India: -

1. **zero-trust architecture across AI systems: -** The rapid adoption of artificial intelligence in India has created both opportunities and challenges in the field of cybersecurity. One of the most pressing solutions is the implementation of **zero-trust architecture** across AI systems. By enforcing identity-centric access controls, continuous verification, and micro-segmentation, organizations can reduce the risk of unauthorized access and model tampering. This approach ensures that every interaction with AI pipelines—whether in training, deployment, or monitoring is verified and secure.

2. **Strengthen National AI-Driven Cyber Defense**
India's national cybersecurity agency, CERT-In, is already expanding AI-based monitoring, research partnerships, and rapid-response systems. Scaling these initiatives nationwide can help detect and neutralize AI-powered attacks faster like AI-enabled threat intelligence sharing, real-time anomaly detection systems and public–private cybersecurity collaboration.

3. **AI-native threat detection and response**: -Another critical solution lies in **AI-native threat detection and response**. Since attackers are increasingly using AI to launch sophisticated phishing and malware campaigns, India must deploy machine learning models that can detect anomalies in emails, endpoints, and cloud systems. These models should be tuned to local linguistic and behavioral patterns, making them more effective against region-specific threats. Coupled with strong identity controls like multi-factor authentication and behavioral biometrics, this can significantly reduce the success rate of AI-driven social engineering attacks.

4. **Deploy AI for Proactive Threat Detection: -** Reports show India ranks 2nd globally in email threats and 3rd in malware detections. AI-based security tools can drastically reduce these risks as such AI-powered phishing filters, machine-learning malware detectors and automated incident response platformsSecuring the AI lifecycle itself

© 2026 Dr. Smith Vyas. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

is equally important. **MLOps security** must include data provenance checks to prevent poisoned datasets, adversarial training to strengthen models against manipulation, and runtime hardening to mitigate risks such as prompt injection or model exfiltration. Logging and auditing of model decisions should also be mandatory, enabling organizations to review and respond to incidents effectively. This ensures that AI systems remain trustworthy and resilient against evolving cyber threats.

5. **Sector-specific solutions: -** In the **banking and financial sector**, strong customer authentication combined with transaction-level anomaly detection can help counter fraud in UPI and netbanking systems. Deepfake detection tools are essential to prevent impersonation in financial transactions. For government and critical infrastructure, segregated networks and verified communication channels can safeguard sensitive data and services from AI-generated misinformation or spear-phishing. In healthcare, privacy-preserving techniques such as federated learning and differential privacy can protect patient data while still enabling AI-driven innovation.

6. **Build a Skilled AI-Cybersecurity Workforce**: -Beyond technology, workforce development and skilling are crucial. India must invest in training professionals in secure coding, AI red-teaming, and incident response. National hackathons and competitions focused on AI defense can accelerate innovation and build a strong talent pipeline. For smaller enterprises, affordable managed security services can provide AI-enabled monitoring without requiring large in-house teams, ensuring that even MSMEs are protected against AI-driven cyber threats.

7. **Establish Strong AI Governance & Regulation**: -Finally, policy and governance frameworks must evolve to keep pace with AI. India should establish clear legal standards for synthetic media, deepfakes, and AI-generated fraud, ensuring rapid takedown and accountability. Public–private partnerships can enable the sharing of anonymized threat intelligence, while universities and startups can contribute by developing benchmarks for deepfake detection and adversarial resilience. By combining technical hardening, governance, and capacity building, India can create a robust ecosystem that addresses the challenges at the intersection of cybersecurity and AI.

CONCLUSION

The intersection of artificial intelligence and cybersecurity in India represents both a powerful opportunity and a complex challenge. As the nation accelerates its digital transformation, AI is becoming essential for defending against rapidly evolving cyber threats. At the same time, AI introduces new vulnerabilities from adversarial attacks to deepfake driven fraud that demand stronger safeguards and smarter governance.

India's path forward depends on three pillars:

- Strengthening AI-enabled cyber defense, ensuring faster detection and response to threats
- Building a skilled workforce capable of securing AI systems and using AI responsibly
- Developing clear governance frameworks that protect data,ensure transparency, and guide ethical AI deployment

By investing in these areas, India can transform AI from a potential risk into a strategic advantage. The goal is not just to defend against threats but to build a resilient, intelligent, and future-ready digital ecosystem. The synergy between AI and cybersecurity will shape India's technological leadership, economic growth, and national security in the years ahead. India stands at a pivotal moment and the choices made today will define the safety and strength of its digital future.

REFERENCES

1. ETCISO. AI adoption surges in Indian cybersecurity: report showing 94% of enterprises already using AI for cyber defense. 2025 [cited 2026 Jul 18]. Available from: https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/report-ai-adoption-surges-in-indian-cybersecurity-94-of-enterprises-already-using-it/125213801
2. NITI Aayog. *National Strategy for Artificial Intelligence*. New Delhi: NITI Aayog; 2023. Available from: https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
3. Press Information Bureau. *Transforming India with AI*. New Delhi: Government of India; 2025. Available from: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/dec/doc20251230747901.pdf
4. Press Information Bureau. CERT-In & SISA launch AI Security Certification. New Delhi: Government of India; 2024. Available from: https://pib.gov.in/PressReleasePage.aspx?PRID=2057868
5. CERT-In. *Indian Computer Emergency Response Team*. New Delhi: Ministry of Electronics and Information Technology. Available from: https://www.cert-in.org.in/
6. Data Security Council of India, Seqrite. *India Cyber Threat Report 2025*. 2024. Available from: https://www.quickheal.co.in/documents/media/2024/ai-driven-deepfake-enabled-cyberattacks-to-increase-in-2025-dec2024.pdf
7. Times of India. Key sectors facing cyber threats from deepfakes, AI-generated content: report. 2025. Available from: https://timesofindia.indiatimes.com/india/key-sectors-facing-cyber-threats-from-deepfakes-ai-generated-content-report/articleshow/120076636.cms
8. ETCISO. AI adoption surges in Indian cybersecurity. 2025. Available from: https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/report-ai-adoption-surges-in-indian-cybersecurity-94-of-enterprises-already-using-it/125213801
9. NITI Aayog. *National Strategy for Artificial Intelligence*. New Delhi: NITI Aayog; 2023. Available from:

© 2026 Dr. Smith Vyas. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
10. Press Information Bureau. *Transforming India with AI*. New Delhi: Government of India; 2025. Available from: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/dec/doc20251230747901.pdf
11. Press Information Bureau. CERT-In & SISA launch AI Security Certification. New Delhi: Government of India; 2024. Available from: https://pib.gov.in/PressReleasePage.aspx?PRID=2057868
12. IndiaAI. CERT-In & SISA launches first-of-its-kind ANAB-accredited AI Security Certification (CSPAI) program. 2024. Available from: https://indiaai.gov.in/news/cert-in-sisa-launches-first-of-its-kind-anab-accredited-ai-security-certification-cspai-program
13. CERT-In. *Indian Computer Emergency Response Team*. New Delhi: Ministry of Electronics and Information Technology. Available from: https://www.cert-in.org.in/
14. Data Security Council of India, Seqrite. *India Cyber Threat Report 2025*. 2024. Available from: https://www.quickheal.co.in/documents/media/2024/ai-driven-deepfake-enabled-cyberattacks-to-increase-in-2025-dec2024.pdf
15. Times of India. Key sectors facing cyber threats from deepfakes, AI-generated content: report. 2025. Available from: https://timesofindia.indiatimes.com/india/key-sectors-facing-cyber-threats-from-deepfakes-ai-generated-content-report/articleshow/120076636.cms
16. Press Information Bureau. India's cyber response to deepfakes. New Delhi: Government of India. Available from: https://pib.gov.in/PressReleasePage.aspx?PRID=2154268

Creative Commons License

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution–Non-commercial–No Derivatives 4.0 International (CC BY-NC-ND 4.0) License. This license permits users to copy and redistribute the material in any medium or format for non-commercial purposes only, provided that appropriate credit is given to the original author(s) and the source. No modifications, adaptations, or derivative works are permitted.

Disclaimer: The views, opinions, statements, and conclusions expressed in the papers, abstracts, presentations, and other scholarly contributions included in this conference are solely those of the respective authors. The organisers and publisher shall not be held responsible for any loss, harm, damage, or consequences — direct or indirect — arising from the use, application, or interpretation of any information, data, or findings published or presented in this conference. All responsibility for the originality, authenticity, ethical compliance, and correctness of the content lies entirely with the respective authors.

© 2026 Dr. Smith Vyas. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/