IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 6, Issue 2, March 2026

Impact Factor: 8.2

Resilient Digital Learning Ecosystems: Positioning Cybersecurity as the Foundational Pillar of Education 4.0 for Learner Safety

Mrs. Anupama Mishra[1] and Ms. Anita Pattnaik[2]

Assistant Professor of Educational Studies (TE), Department of Teacher Education
Vikram Dev University, Jeypore, Koraput[1]
Research Scholar, Department of Education
Asian International University, Ghari, West Imphal, Manipur, India[2]

Abstract: *Education 4.0 represents a revolutionary paradigm shift from traditional classroom to a digital classroom that incorporates artificial intelligence, virtual learning environments and technology enhanced learning aids. This shift has promoted most adaptable learner centred classroom environment by providing educational opportunities beyond the conventional classroom boundaries. Although, the AI powered digital platforms accompanies serious cybersecurity concerns for the learner's safety in virtual spaces.*

As students spend more time in online learning space, they are facing excessive cyber risk such as cyberbullying, identity theft, privacy breaches, misinformation, digital addiction and exposer to inappropriate harmful content which ultimately hampers their social as well as cognitive health. Amid these circumstances, cybersecurity acts as a central part of education 4.0 aimed at protecting learner's digital world.

This study emphasises the importance of cybersecurity ensuring student's safety within the framework of education 4.0. it outlines the various cyber risks faced by students in current scenario and responsibilities of educational institutions and teachers to build secure digital environment. Additionally, this paper discusses the involvement of parents and policy level support to achieve digital protection.

The study also explores the importance of embedding cybersecurity awareness and digital citizenship with school curricula and teacher education programmes. Furthermore, national initiatives are examined to illustrate ongoing efforts for strengthening cyber safety awareness in education. It asserts that ensuring student's safety within the framework of education 4.0 necessitates a collective and forward-looking effort from educators, parents, institutions, and policymakers. Integrating cybersecurity education into the core of mainstream schooling is vital for fostering comprehensive student development and safeguarding learners in the expanding digital learning environment. .

Keywords*:* Cybersecurity, artificial intelligence, digital environment, education 4.0

I. INTRODUCTION

Modern education is undergoing transformations in terms of educational practices, skillsets and competencies, teaching and learning methodologies which include flipped classroom, blended learning, self-regulated learning, project-based learning, inquiry-based learning, student-centred pedagogy etc. incorporating such varieties of teaching techniques led to the emergence of a new phrase called "Education 4.0". This aligns itself with emerging fourth industrial revolution that focuses on artificial intelligence, smart technologies, Internet of things, robotics etc. The framework of Education 4.0 prioritizes tailored instruction, workforce-ready competencies, and technological integration to cultivate a flexible, student-focused learning ecosystem.

DOI: 10.48175/IJARSCT-31539

Our new generation is now witnessing the integration of artificial intelligence, virtual learning environments, and digital tools that make education more student-cantered than ever before. Coursera, expanding GenAI skills in India through collaborations with IITs, IIMs, BITS Pilani, and Fractal Analytics, recorded a 107% YoY surge to 2.6M Generative AI course enrolments—especially among women and learners from weaker academic backgrounds—as of August 2025 (IBEF report).

However, this digital revolution simultaneously exposes learners to pervasive cyber threats that endanger their cognitive, social, and emotional health. Cybersecurity incidents in India rose from 10.29 lakh in 2022 to 22.68 lakh in 2024 (Press Information Bureau, GoI); while Odisha alone reported over 43,740 cyber fraud complaints worth ₹415 crore, highlighting the urgent need for cybersecurity in education. Such vulnerabilities highlight the necessity of embedding cybersecurity awareness into educational frameworks to safeguard learners in the era of Education 4.0.

Cybersecurity is the discipline of protecting individuals, systems, and data against cyberattacks through the application of advanced technologies, structured processes, and robust policies. The growing reliance on the Internet as an essential component of educational infrastructure underscores the urgent need to strengthen cybersecurity awareness and practices among all stakeholders. Comprehensive programs must reach diverse audiences, especially students, who require proper guidance and supervision to handle cyber vulnerabilities responsibly. Educational institutions, teachers, and parents share a collective responsibility to safeguard students against cybercrimes by embedding digital literacy, monitoring online behaviour, and fostering safe technology use.

In this context, the study underscores the urgent need to embed cybersecurity awareness and digital citizenship within Education 4.0. By examining student vulnerabilities, institutional responsibilities, parental involvement, and national initiatives, it highlights safeguarding learners in the digital era requires a collective, forward-looking approach. Integrating cybersecurity education into mainstream schooling is therefore essential for ensuring student safety and fostering holistic development in an increasingly technology-driven environment.

OBJECTIVES:

- To examine the role of cybersecurity in education.
- To evaluate the challenges for cyber security in education.
- To evaluate the responsibilities of educational institutions and teachers in promoting safe online practices.
- To review national and state level initiatives aimed at enhancing cyber safety awareness and resilience in education systems.

EDUCATION 4.0:

Education 4.0 denotes a transformative, technology-driven model of teaching and learning that integrates artificial intelligence, the Internet of Things, cloud computing, and immersive digital tools to create adaptive, learner-centred environments. This paradigm shifts emphasis from content delivery to competency development—fostering the 4Cs (critical thinking, creativity, collaboration, communication), personalized and active pedagogies, and seamless use of smart platforms. Robust cybersecurity is integral to Education 4.0, ensuring that digital infrastructures, learner data, and online interactions remain secure, private, and ethically managed so that technological innovation supports safe, equitable, and trustworthy learning experiences.

CYBERSECURITY:

The evolution of internet allows human to indulge in both real and virtual life. With search engines, social networking sites and digital platforms all information are on fingertips. This amplifies users' exposer to cyber risks. Cybersecurity refers to the protection of computers, servers, mobile devices, electronic systems, networks, and data against malicious intrusions targeting both organizational infrastructures and personal devices. Such threats are categorized into multiple domains, including network security, application and information security, operational safeguards, disaster recovery, and continuity of teaching and learning.

EMERGING CYBER THREATS IN EDUCATION:

In the new digital era, educational institutions encounter a wide range of cybersecurity challenges that threaten the integrity of their systems and the safety of their stakeholders.

Budget Constraints

Budget constraints remain a major hurdle for schools and universities, with nearly 50% citing limited funds as the primary barrier to cybersecurity. Reduced funding restricts investment in advanced tools, regular assessments, and staff training, leaving institutions vulnerable to digital threats.

Ransomware

Ransomware attacks in the education sector extend beyond classroom disruption, affecting entire communities of students, families, and educators. Cybercriminals lock essential systems through encryption and demand ransom for restoration. Such attacks interrupt educational activities, postpone examinations, and jeopardize the integrity of student records. According to a report from Times of India, in **June 2025**, a ransomware attack on **Surya Shakti Infotech** disrupted college admissions, erased student records, and forced a system restart at institutes including **Scottish Church College.**

Phishing and Social Engineering

Phishing is the most common cyberattack in education, using deceptive emails to steal credentials or spread malicious links. Indian universities face thousands of weekly phishing emails, misleading staff and students into revealing credentials that are later sold on the dark web.

Juice jacking

Juice jacking is a cyberattack that takes advantage of public USB charging ports to either steal information from a device or install harmful software. Charging stations in places like airports, schools, colleges and university, hotels, and cafés may look convenient, but their USB ports are not always secure. Since USB connections can carry both power and data, attackers can exploit this feature to gain access to your device while it charges.

Data breaches and student record theft

Educational institutions, housing extensive student data, are highly vulnerable to breaches that compromise academic records, medical information, and personal identifiers. An example of a major breach on January 2023 is the **Diksha app** flaw, which exposed data of nearly 6 lakh Indian students after information stored on an unprotected cloud server was left vulnerable, including names, email IDs, and school details (Indiatoday.in)

Unsecured ed-tech platforms

Educational tools and apps are becoming part of everyday learning, yet many still lack strong security measures. Third-party EdTech platforms, if not carefully reviewed and monitored, can serve as entry points for cyberattacks. Odisha, like other states, faces heightened risks due to rapid digital adoption in schools without adequate cybersecurity safeguards.

DDoS (Distributed Denial-Of - Service) Attacks

A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server or network by flooding the target system and nearby infrastructure with excessive Internet traffic. Such attacks can cause major system outages, financial setbacks, and serious harm to an organization’s reputation. On May 7, 2025, government websites and telecom portals were crippled for 19 hours by a massive surge of malicious traffic, exposing the fragility of India’s digital defences (etedge-insights.com).

Outdated software

Many educational institutions continue to rely on legacy systems, including outdated Windows versions, obsolete learning platforms, and unsupported servers, which expose them to security risks.

Espionage and Intellectual Property Theft

Universities engaged in advanced research are increasingly vulnerable to cyber espionage. Nation-state actors often target higher education institutions to illicitly acquire sensitive scientific, engineering, and medical innovations.

Insider Threats and Human Error

Serious cybersecurity risks can also originate within institutions., inadequately trained employees, and individuals with privileged access may cause harm, whether through intentional misuse or accidental error.

NEWS OF CYBER ATTACKS ON ODISHA:

Date	**Institution**	**Nature of Attack**	**Impact on Students**	**Response**
July 27–28, 2025	**Ravenshaw University (Cuttack)**	Website hacked; mobile users redirected to *Bento-4D* betting app	Students unable to download certificates during admissions	Registrar confirmed issue resolved; no official statement initially issued
July 2025	**Odisha Higher Education Department (Bhubaneswar)**	Instagram account hacked; obscene and betting-related content posted	Misleading content spread; reputational damage	FIR filed at Saheed Nagar Police Station; account restored
January 2026	**Gangadhar Meher University (Sambalpur)**	Website defaced with Pakistani flag	Students faced disruption accessing academic resources	Hackers' identity unclear; investigation ongoing (reported widely in Odisha media)
Earlier Incidents (2023–2024)	**Multiple Odisha colleges** (reported in surveys of cybercrime)	Phishing, malware, and exam portal breaches	Students' personal data exposed; exam schedules disrupted	Highlighted in academic studies on cybercrime in Odisha

Ravenshaw University Website Hacked (July 27–28, 2025)

Ravenshaw University's official website in Cuttack was hacked late July 2025, redirecting users on both mobile and desktop to a suspicious betting platform called BENTO4D. The breach left students unable to access certificates or academic services, sparking fears of compromised data. This incident, coming two years after a similar attack, has raised serious questions about the effectiveness of the university's cybersecurity measures, despite its investment in a ₹2 crore high-performance Blade Server meant to safeguard against such threats.

Odisha Higher Education Department's Instagram Account Hacked, FIR Filed

In July 2025, the official Instagram account of the Odisha Higher Education Department in Bhubaneswar was hacked, with obscene and betting-related content being posted. The breach not only spread misleading material but also caused reputational damage to the department. Following the incident, an FIR was lodged at Saheed Nagar Police Station, and

DOI: 10.48175/IJARSCT-31539

the account was subsequently restored, highlighting both the vulnerability of institutional social media platforms and the need for stronger cybersecurity safeguards.

Gangadhar Meher University Website Defaced, Investigation Underway

In January 2026, the official website of Gangadhar Meher University in Sambalpur was defaced with a Pakistani flag, causing widespread concern among students and faculty. The breach disrupted access to essential academic resources, leaving students unable to use the portal effectively during the period. While the hackers' identity remains unclear, the matter has been reported extensively in Odisha media, and an investigation is currently underway. The incident has once again highlighted the growing vulnerability of educational institutions to cyberattacks and the urgent need for stronger digital safeguards.

THE NEED FOR CYBERSECURITY IN EDUCATION 4.0:

Cybersecurity is an essential part of education 4.0, as the integration of AI, IoT, cloud-based learning environment exposes schools and universities to risks of data breaches, cyberattacks, and digital exploitation. Smart classrooms, IoT technologies, and digital learning platforms increase the range of entry points available to hackers. Cybercrime complaints have witnessed an alarming surge, rising from approximately 4.5 lakh in 2021 to over 22 lakhs in 2024—marking an increase of more than 400% within four years (the 420-web desk). Likewise, data from the Odisha Legislative Assembly shows that financial fraud complaints rose sharply by over 140% in 2024, climbing to 43,740 cases from 18,081 in 2023. The monetary losses exceeded ₹415.90 crore, reflecting a fourfold increase from the previous year.

Research shows that cybercrime victims often face anxiety, depression, stress, and reduced trust in digital systems, with vulnerable groups like older adults and students experiencing persistent mental health consequences. Cybersecurity is also needed to control addiction to computer games. According to recent national data, nearly 60% of Indian youngsters between 9 and 17 years spend more than three hours daily engaged in social media or gaming activities (India today). These addictions result in profound health concerns and considerable academic setbacks in children, especially adolescents.

Given the evidences presented, cybersecurity plays a pivotal role in ensuring academic integrity, and protect intellectual property. With the increasing use of online examinations, digital assignments, and AI-driven evaluation systems, the risk of cheating, plagiarism, and manipulation of results has grown significantly. Robust cyber safeguards are therefore indispensable to uphold fairness and transparency in academic processes. Additionally, as education becomes more globalized through virtual collaborations and international partnerships, secure digital platforms are necessary to counter global cybersecurity challenges. By mastering basic security practices and recognizing possible threats, individuals can help build a safer digital space.

NATIONAL AND STATE LEVEL INITIATIVES IN EDUCATION SECTOR:

The National Cyber Security Strategy (Draft 2020) was prepared by the Data Security Council of India (DSCI) to provide a comprehensive framework for strengthening India's cyber resilience. it outlined 21 focus areas including education. emphasized capacity building as a cornerstone of India's cyber resilience. It proposed structured training for government officials, industry professionals, and academic institutions, while also recommending the integration of cybersecurity modules into higher education curricula

ISEA Project (started in 2005 and currently in its third phase since Oct. 2023 onwards) :- The ISEA Project**,** aims to develop skilled human resources in information security and to spread cyber awareness among citizens, students, and government officials. It is structured around four core verticals: building a pool of highly skilled and certified cybersecurity professionals, nurturing students to innovate and develop products and solutions in the field, advancing research and academic activities in emerging areas of information security, and fostering mass awareness to create cyber-aware digital citizens. Together, these pillars aim to strengthen India's cybersecurity ecosystem through education, innovation, and public engagement.

The National Cybercrime Training Centre (CyTrain 2020): It operates under the Indian Cybercrime Coordination Centre (I4C) and is managed by the National Crime Records Bureau (NCRB). It is a virtual training centre hosted by the National Crime Records Bureau (NCRB), aims to standardize cybersecurity curricula, develop hands-on modules for cybercrime detection and reporting in simulated environments, create MOOCs, and establish cyber labs. It trains officers of all ranks from States, Union Territories, and Central Police/Armed Forces.

The Indian Computer Emergency Response Team (CERT-In) is India's national nodal agency for cybersecurity, responsible for monitoring, responding to, and mitigating cyber incidents across the country. Established in 2004 under the Ministry of Electronics and Information Technology, it plays a central role in safeguarding India's digital infrastructure.

The Indian Cybercrime Coordination Centre (I4C): approved on 5 October 2018 and dedicated to the nation on 10 January 2020, is a Ministry of Home Affairs initiative to address cybercrime in a coordinated and comprehensive manner. Managed under the NCRB, it enhances India's capability to combat cyber threats by improving coordination among law enforcement agencies and stakeholders, driving systemic change in cybercrime response, and ensuring greater citizen satisfaction.

Odisha cyber security policy (OCSC 2021): was introduced by the Government of Odisha to establish a secure digital ecosystem, protect critical infrastructure, and promote cyber awareness across the state. It emphasizes governance, resilience, and capacity-building, aligning with India's national cybersecurity vision.

Cyber security awareness drive (oct- Nov 2025): Odisha's Higher Education Department has launched a statewide Cyber Security Awareness Campaign (Oct 18–Nov 17, 2025) in collaboration with Odisha Police, the Home Department, and other organizations, directing all degree colleges to ensure active student participation. The initiative aims to educate students, women, the elderly, and the public on safe digital practices and reporting cyber-crimes, with debate competitions in Odia and English held at block, district, range, and state levels to select winners and build awareness across the state.

CYBERSECURITY INITIATIVES IN ODISHA SCHOOLS

Initiative	**Organizer**	**Target Schools**	**Key Activities**	**Impact**
AI-Powered Classrooms (2025–2026)	Odisha School Education Programme Authority (OSEPA)	**5,370 govt & aided secondary/higher secondary schools**	AI-integrated learning, smart boards, digital labs	Bridging digital divide; future-ready tech skills for rural students
Cybersecurity Training Camps	Odisha Computer Application Centre (OCAC) + SME Dept.	**100+ higher secondary schools annually**	Hands-on training in cyber hygiene, phishing awareness, safe browsing	Students sensitized to online risks and career paths in cybersecurity
Cybersecurity Awareness Campaign (Oct–Nov 2025)	Higher Education Dept.	**Schools & colleges statewide**	Debates, competitions, awareness drives at block/district/state levels	Thousands of students engaged in digital safety education
Digital Safety Education in Remuna Tehsil (Balasore)	Fakir Mohan University	**Govt schools in Balasore district**	Mass awareness sessions, phishing prevention, privacy education	Improved digital resilience in semi-rural school clusters
Wipro Earthian Sustainability	Wipro + Azim Premji	**Select schools including Louis**	Water audits, digital documentation,	Promoted ethical tech use and digital

DOI: 10.48175/IJARSCT-31539

Program (2025)	University	**Braille School (Bhubaneswar)**	privacy-linked sustainability	responsibility

RESPONSIBILITIES OF EDUCATIONAL INSTITUTIONS AND TEACHERS TO BUILD A SECURE DIGITAL ENVIRONMENT:

Educational institutions and educators serve as pivotal architects of a secure digital ecosystem by embedding cyber safety into academic curricula, cultivating responsible online conduct among learners, and fortifying institutional IT infrastructures against emerging threats.

Educational institutions as virtual guardians:

Schools serve as pivotal guardians of internet safety, bearing the primary responsibility for ensuring that systems, computers, and network devices remain secure and fully functional. Equally vital is the protection of information, which must be safeguarded with the same rigor and diligence applied to maintaining the integrity of technological infrastructure within the institution.

To build a secure digital environment in schools, institutions must adopt a comprehensive cybersecurity framework that begins with identifying vulnerabilities, assessing risks, and implementing robust protection measures such as firewalls, strong password protocols, licensed software, and restricted access to systems. Regular updates of operating systems and antivirus software, encryption of network traffic, multi-factor authentication, and secure Wi-Fi practices are essential to safeguard infrastructure. Policies should discourage personal device use, enforce access controls, and ensure third-party vendors maintain strong security standards.

Equally important is protecting sensitive data through secure storage, off-site backups, and clear reporting mechanisms for breaches. Schools must also establish incident response strategies—assessing, recovering, investigating, and preventing recurrence of cyber incidents—while fostering awareness through stakeholder education, cyber safety rules, supervised filters, and integration of cyber laws into training. By embedding cybersecurity lessons into curricula, modelling ethical digital behaviour, celebrating initiatives like Safer Internet Day, and collaborating with trusted cybersecurity organizations, schools can create a resilient, safe, and responsible digital ecosystem for students, teachers, and administrators.

Responsibilities of teachers:

Creating a secure digital environment requires combining technical, ethical, social, and legal measures. Technically, schools must enforce strong passwords, secure networks, regular updates, backups, and restricted access. Ethically, users should respect intellectual property, avoid plagiarism, and maintain authenticity online. Socially, safe digital behaviour is vital—protecting personal information, discouraging cyberbullying, and fostering respectful interactions. Legally, compliance means reporting cybercrimes, avoiding phishing, respecting privacy, and adhering to copyright and consent norms. Together, these practices protect systems, data, and people while promoting responsible digital citizenship.

Parents role in nurturing safe digital habits:

Parents are responsible for mentoring, monitoring, and modelling safe digital practices. Their role includes building trust, setting boundaries, securing devices, and educating children about online risks. By combining empathy, awareness, and technical safeguards, parents can create a safe and healthy cyber environment at home. They must also encourage open conversations so children feel confident to share their online experiences, guide them in responsible social media use, and instil the importance of privacy and strong passwords. In addition, parents should stay updated on emerging cyber threats, use parental controls wisely, and promote balanced screen time to ensure that technology supports learning and well-being rather than becoming a source of risk. Ultimately, their proactive involvement helps children grow into responsible, resilient, and digitally aware citizens.

DOI: 10.48175/IJARSCT-31539

PRACTICAL STRATEGIES FOR EMBEDDING CYBER SECURITY AWARENESS IN EDUCATION SYSYTEM

Classroom activities for students:

To embed cybersecurity awareness effectively, schools can organize **cyber hygiene workshops** that cover essentials like strong passwords, safe browsing, and spotting phishing attempts. **Role-play activities** help students practice responses to issues such as cyberbullying or suspicious emails, while **gamified learning** through quizzes and puzzles makes concepts engaging. **Digital citizenship projects**—posters, videos, or campaigns—encourage creative advocacy for safe online behaviour, and **peer-to-peer learning** allows older students to mentor younger ones in responsible digital practices.

Teacher training programs:

To strengthen cybersecurity awareness in education, teachers can engage in **professional development workshops** on cyber laws, ethical technology use, and classroom safety. **Simulation exercises** help them practice responses to incidents like data breaches or online harassment, while **curriculum integration training** guides the inclusion of cybersecurity topics across subjects. Collaboration with experts provides insights into emerging threats, and through **ethical digital modelling**, teachers set strong examples of responsible online behaviour for students.

Initiatives under educational institution:

Schools can strengthen digital citizenship through school-wide initiatives such as student-led **Cyber Safety Clubs** that promote awareness and peer support, **an Annual Cybersecurity Week** featuring activities, competitions, and expert talks, integration with national campaigns like **Safer Internet Day**, and consistent policy reinforcement with clear rules on device use, data protection, and incident reporting.

Cross- disciplinary approach:

Integrating cybersecurity across diverse subjects fosters a holistic educational approach that highlights its relevance beyond computer science. Embedding concepts into social studies, mathematics, and language arts allows students to explore ethical issues, cryptographic applications, and the societal impact of cyber laws, while also engaging with practical tools and real-world contexts. This multidisciplinary strategy underscores the interconnectedness of fields, encourages collaborative learning and critical thinking, and deepens students' understanding of how cybersecurity shapes everyday life and professional domains.

Collaborations with industry experts:

Partnerships with cybersecurity professionals and organizations can greatly strengthen cybersecurity education by bringing real-world expertise into the classroom. Guest lectures, workshops, and mentorship programs expose students to current industry trends, tools, and challenges, while offering practical, hands-on experiences and career guidance. Such collaborations enrich learning, provide valuable networking opportunities, and bridge the gap between theoretical knowledge and its application in practice

Comparative Chart: Foreign Cybercrime Initiatives vs India

Area	Initiative Abroad	Country/Region	Status in India	What India Lacks / Should Adopt
International law	Budapest Convention on Cybercrime	Europe	Not signed	Harmonized cybercrime laws, fast cross-border evidence sharing
Global Treaty	UN Convention on Cybercrime	UN member states	Not ratified	24×7 international cyber police coordination
Cybercrime Courts	Specialized internet Courts	China	Absent	Fast-track cybercrime judiciary

DOI: 10.48175/IJARSCT-31539

Deep fake law	Strict AI Manipulation Laws	EU (AI Act)	Absent	Legal control of deepfake misuse

SUGGESTIONS:

Embrace Artificial Intelligence (AI) and Machine Learning (ML) for Threat Detection and Response

Adopt a Zero Trust Security Framework

Prepare for Cloud-Native Security Challenges

Focus on Cyber Resilience, Not Just Prevention

Invest in Threat Intelligence and Collaboration

Integrate cybersecurity modules into all levels of teacher education programs to build foundational awareness and classroom readiness.

Mandate digital safety audits in schools and colleges to assess vulnerabilities and guide infrastructure upgrades.

Establish student-led cyber safety clubs to promote peer-to-peer learning and foster responsible digital behaviour.

Include cyber ethics and digital citizenship as cross-curricular themes in subjects like social science, computer studies, and language.

Develop multilingual cyber awareness content (including Odia and regional languages) to ensure inclusive outreach across diverse learner groups.

Create a centralized reporting system for educational institutions to log cyber incidents and receive expert guidance.

Encourage collaboration with cybersecurity agencies like CERT-In and I4C for real-time threat updates and training support.

Promote gamified learning tools to teach cybersecurity concepts in engaging formats for students aged 9–17.

Involve parents through digital parenting workshops that cover device safety, screen time balance, and emotional support strategies.

Celebrate Cybersecurity Week annually with competitions, expert talks, and student campaigns aligned with national initiatives.

II. CONCLUSION

In conclusion, cybersecurity is not merely a technical requirement but a fundamental pillar of Education 4.0. As digital learning environments expand, the rising tide of cyber threats underscores the urgency for schools and universities to adopt proactive safeguards. Embedding cyber safety into curricula and teaching practices empowers learners to navigate the digital world responsibly, while parents reinforce these habits at home. National and state initiatives provide a strong foundation, yet their true impact depends on deeper integration into everyday educational systems. By cultivating digital citizenship and awareness, institutions can foster secure ecosystems that uphold student safety, academic integrity, and holistic development. Ultimately, it is through the collective commitment of educators, parents, policymakers, and institutions that a resilient and trustworthy digital future for learners can be achieved.

REFERENCES

[1]. Data Security Council of India. (2020). National Cyber Security Strategy (Draft 2020). DSCI.

[2]. ET Edge Insights. (2025, May 7). Massive DDoS attack cripples government websites and telecom portals. ET Edge Insights.

[3]. Government of Odisha. (2021). Odisha Cyber Security Policy (OCSC 2021). Government of Odisha.

[4]. India Brand Equity Foundation. (2025, August 7). *Demand for generative artificial intelligence (GenAI) skills rises in India, with 2.6 million Coursera learners*. IBEF. (ibef.org in Bing)

[5]. India Today. (2024). Survey on social media and gaming addiction among Indian youth. India Today Group.

[6]. Ministry of Electronics and Information Technology. (2004). Indian Computer Emergency Response Team (CERT-In). Government of India.

[7]. Ministry of Home Affairs. (2018). Indian Cybercrime Coordination Centre (I4C). Government of India.

[8]. Odisha Higher Education Department. (2025, October–November). Cyber Security Awareness Campaign. Government of Odisha.

[9]. Odisha Legislative Assembly. (2024). *Report on financial fraud complaints in Odisha*. Government of Odisha. (odishaassembly.nic.in in Bing)

[10]. Press Information Bureau, Government of India. (2025, October 8). *Curbing cyber frauds in Digital India*. PIB. (pib.gov.in in Bing)

[11]. Sengupta, A. (2023, January 27). *Flaw in Diksha app exposed data of nearly 6 lakh students*. India Today. (indiatoday.in in Bing)

[12]. Times of India. (2025, June). Ransomware attack on Surya Shakti Infotech disrupts college admissions. Times of India.