C3iHub
भारतीय प्रौद्योगिकी संस्थान कानपुर
Indian Institute of Technology Kanpur

CYBER RAKSHAK

Newsletter from C3iHub, IIT Kanpur

VOLUME 4 ISSUE 1
JANUARY EDITION 2026

Message from CEO

Dear Readers,

I am delighted to present the January 2026 edition of our Newsletter **CYBER RAKSHAK** reflecting another productive and impactful quarter for C3iHub. Over the past few months, we have continued to strengthen India's cybersecurity ecosystem through strategic collaborations, technology deployments, research advancements, and focused capacity-building initiatives.

A key milestone this quarter has been the successful deployment of our indigenous IT-OT Security Operations Center at Bhilai Steel Plant, SAIL, enhancing the protection of critical industrial infrastructure. We also launched a blockchain-based Agriculture Seed Licensing System for the Government of Rajasthan, improving transparency and efficiency in public service delivery. In addition, the introduction of C3iHub Arena, our in-house secure platform for hackathons and cybersecurity challenges, marks an important step toward nurturing innovation and talent.

Our research and innovation efforts continued to gain momentum through vulnerability discoveries, CVE publications, and publication of paper in conference. We are also proud that IIT Kanpur received the 'Special Jury Recognition for Consistent Performance' at the DSCI Excellence Awards 2025, reinforcing the collective impact of our work in cybersecurity education and innovation.

This quarter also witnessed strong collaboration through MoUs with the Indian Army's Central Command, NMDC, DMRC, Maharashtra Metro, and ARAI, supporting cybersecurity readiness across critical sectors. Alongside this, we conducted specialized training programs for officials from the Indian Ports Association, NIC, and the Ministry of Power, further strengthening national cyber resilience.

These achievements reflect the dedication of our researchers, partners, and startups. As we move forward into 2026, we remain committed to driving indigenous innovation, strengthening digital trust, and building a Cyber secure future for the nation.

Dr. Tanima Hajra

About C3iHub

C3iHub is a Technology Innovation Hub (Section 8 Company) established at IIT Kanpur (in 2020) funded by Department of Science and Technology, Government of India, under the National Mission on Interdisciplinary Cyber-Physical Systems. As the name (C3iHub, i.e., Cybersecurity and Cybersecurity for Cyber-Physical Systems Innovation Hub) implies, C3iHub addresses cybersecurity issues of cyber-physical systems in its entirety.

From analysing security vulnerabilities and developing tools to address them at various levels of critical cyber-physical system architectures, to nucleating start-ups developing such tools at scale, to partnering with industries for co-development and technology transfer, to training the next generation of cybersecurity researchers, C3iHub works on every level that facilitates country's adoption and advancement of cyber-physical systems. C3iHub has been upgraded to prestigious Technology Translation Research Park status by DST, GoI in 2025.

Our hub management team is headed by Prof. Manindra Agrawal as the Chairman, Prof. Somitra Sanadhya as the Project Director, and Dr. Tanima Hajra as the CEO.

News Highlights

- C3iHub Deploys IT-OT SOC at Bhilai Steel Plant, SAIL
- MoUs signed with Indian Army HQCC, NMDC, DMRC, Maharashtra Metro, and Automotive Research Association of India
- Specialized Training Programs Conducted for Indian Ports Association, National Informatics Centre, and Ministry of Power Officials
- C3iHub Deploys Blockchain-based Agriculture Seed Licensing System for Rajasthan Government
- Launch of C3iHub Arena - A Secure Platform for Hackathons and Cybersecurity Challenges
- Received 'Special Jury Recognition for Consistent Performance' in Best Practices in Cybersecurity Education and Research at DSCI Excellence Awards 2025

Technology Innovations

C3iHub Deploys IT-OT SOC at Bhilai Steel Plant, SAIL

C3iHub, IIT Kanpur has successfully deployed and gone live with a state-of-the-art Security Operations Center (SOC) at Bhilai Steel Plant (BSP), Steel Authority of India Limited. This milestone marks a significant step toward strengthening the cybersecurity posture of one of India's most critical industrial infrastructures.

The newly established SOC facility was formally inaugurated by Prof. Manindra Agrawal, Director, Indian Institute of Technology Kanpur, and Shri C. R. Mahapatra, Director In-Charge, SAIL Bhilai Steel Plant. Dr. Tanima Hajra, CEO of C3iHub, Shri M. P. Singh, GM (IT) of BSP, along with senior officers from C3iHub and BSP were also present during the inauguration ceremony.

The IT-OT SOC allows monitoring of cyber threats on an organization's IT and OT assets 24x7 and provides timely alerts with remediation workflow, ensuring vulnerability fixation after detection

Salient Features:

- Code-based scalable customizable SOC
- 100% indigenous SIEM (Security Information and Event Management)
- Custom integration of indigenously developed platforms: Asset Management, Vulnerability Management, Log Aggregation & Analysis, Threat Intel & Management, Rule Management, Ticket Management, Alert Management, Incident Management, File Analysis, and Compliance Management
- Solutions compatible with both IT & OT assets
- Compatible across sectors (power, manufacturing, refinery) and OEMs
- Homegrown security data lake

Benefits:

- IT-OT SOC maximizes organization safety
- High-efficiency reporting, notifications, and threat analysis significantly reduce security breaches
- Cost-effective than big companies' SOC

C3iHub Deploys Blockchain-based Agriculture Seed Licensing System for Department of Agriculture, Government of Rajasthan

C3iHub has developed a blockchain-based tamper-proof and transparent system for seed license issuance and verification, ensuring accountability across the agricultural supply chain. The platform utilizes Hyperledger Besu to record and manage seed licensing data securely. The platform integrates seamlessly with the existing Raj Kisan portal via APIs, enabling automatic license creation, renewal, and verification.

Salient Features:

- Immutable blockchain ledger ensures complete data integrity
- Real-time auditability promotes confidence
- Reduces manual effort and processing time by up to 90%

Benefits:

- Each license is cryptographically secured and stored immutably, preventing unauthorized modification or duplication
- Smart contracts automate workflows and create transparent, auditable trails accessible to regulators and citizens

Launch of C3iHub Arena - A Secure Platform for Hackathons and Cybersecurity Challenges

C3iHub announces the launch of C3iHub Arena, a secure, in-house platform developed to streamline the hosting of hackathons and cybersecurity challenges. Designed with a cybersecurity-first architecture, C3iHub Arena enables the organization of a wide range of technology-driven events, including hackathons, coding competitions, quizzes, and Capture The

Flag (CTF) challenges, within a controlled and secure environment. Indigenously developed, the platform provides a reliable solution for conducting technical evaluations and innovation-focused challenges. C3iHub Arena is built to support a diverse user base, including government organizations, academic institutions, and corporate partners seeking secure event-hosting capabilities, as well as students and professionals participating in competitive cybersecurity and technology events.

The platform is being introduced with the launch of HACK IITK 2026, a national-level cybersecurity hackathon, marking the beginning of its use for large-scale technical competitions and talent development initiatives.

Scan QR to see full product video: C3iHub Arena - A Secure Platform for Hackathons and Cybersecurity Challenges

Common Vulnerabilities and Exposures (CVEs)

CNA: Indian Computer Emergency Response Team (CERT-In)

Contributors: Deven Lunkad, Swaroop Dora, Nazia Aslam, and S. Venkatesan (IoT Security Research Lab funded by C3iHub and IIIT Allahabad)

Published: 2026-01-09

CVE-2026-22079

Title: Cleartext Transmission Vulnerability in Tenda Wireless Routers

Description
This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the plaintext transmission of login credentials during the initial login or post-factory reset setup through the web-based administrative interface. An attacker on the same network could exploit this vulnerability by intercepting network traffic and capturing the credentials transmitted in plaintext. Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information and gain unauthorized access to the targeted device.

CVE-2026-22080

Title: Insecure Transmission Vulnerability in Tenda Wireless Routers

Description
This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the transmission of credentials encoded using reversible Base64 encoding through the web-based administrative interface. An attacker on the same network could exploit this vulnerability by intercepting network traffic and capturing the Base64-encoded credentials. Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information and gain unauthorized access to the targeted device.

CVE-2026-22081

Title: Cookie without HTTPOnly Flag Vulnerability in Tenda Wireless Routers

Description
This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the missing HTTPOnly flag for session cookies associated with the web-based administrative interface. A remote at-tacker could exploit this vulnerability by capturing session cookies transmitted over an insecure HTTP connection. Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information and gain unauthorized access to the targeted device.

CVE-2026-22082

Title: Insecure Session ID Management Vulnerability in Tenda Wireless Routers

Description
This vulnerability exists in Tenda wireless routers (300Mbps Wireless Router F3 and N300 Easy Setup Router) due to the use of login credentials as the session ID through its web-based administrative interface. A remote attacker could exploit this vulnerability by intercepting network traffic and capturing the session ID during insecure transmission. Successful exploitation of this vulnerability could allow the attacker to hijack an authenticated session and compromise sensitive configuration information on the targeted device.

Tutorial Session Delivered by C3iHub Representatives

Dr. Anand Handa, Chief Strategy Officer and Mr. Aman Raj, Cybersecurity Instructor delivered a two-hour technical tutorial session at BuildSec 2025, hosted at the Indian Institute of Technology, Patna, supported by International partners including UNSW Sydney.

The tutorial, titled “Next-Gen Cyber Defense in the Cloud: Leveraging AWS Security Tools,” was selected and conducted as part of the conference programme. The session focused on practical and real-world approaches to modern cloud security, covering cloud-native threat detection and incident response, AWS security architecture and automation, and case-based exercises for proactive cyber defence

Research Work

The paper “Unmasking Malicious Actors: Tracing Scammers on the Ethereum Blockchain” was presented by C3iHub researchers Tanmay Thapliyal, Aman Gupta, and Dr. Rachit Agarwal at the 7th International Conference on Blockchain Computing and Applications (BCCA 2025) in Dubrovnik, Croatia.

The study proposed an efficient algorithm to identify Ethereum addresses linked to scam activities, analyzing over 1.8 billion transactions. The approach identified 32,272 scam-associated accounts, achieved detection in 0.024 seconds per address, and revealed recurring transaction patterns to support blockchain forensics and law enforcement investigations. This work is published in IEEE Xplore.

https://ieeexplore.ieee.org/abstract/document/11227181

Workshops Organized

Ideas Matter Most - Talk Show

C3iHub, IIT Kanpur hosted Ideas Matter Most – Talk Show, the flagship platform under the aegis of Ideas Matter Most Ventures Private Limited, in association with Hindustan Times and Dainik Jagran INEXT, at IIT Kanpur.

The event brought together innovators, thought leaders, members of FICCI FLO (Kanpur Chapter), and experts from corporate, government, and civil society for an exchange of perspectives on emerging digital challenges. Prof. Manindra Agrawal, Director, IIT Kanpur, inaugurated the talk show as the Chief Guest. The central theme, “Digital Trust in the Age of AI: Navigating Cybersecurity, Deepfakes, and the New Reality,” addressed critical issues shaping the evolving digital landscape.

The program featured keynote addresses and panel discussions by distinguished speakers from technology, policy, defence, law enforcement, entrepreneurship, and social advocacy, covering topics related to cybersecurity, artificial intelligence, governance, digital ethics, and societal impact.

The talk show facilitated meaningful dialogue and knowledge exchange, offering insights that bridged technology, public policy, and human-centric considerations in the context of digital trust

Hands-on Workshop Conducted at c0c0n 2025

C3iHub conducted a hands-on workshop at c0c0n 2025 as part of the IoT Security Village. The workshop, titled “From Sensors to Security: A Practical Workshop on IoT Systems and Protocol Vulnerabilities,” focused on practical aspects of securing connected systems.

The two-day program provided participants with an immersive learning experience bridging embedded IoT development and cybersecurity. The sessions covered foundational electronics, IoT protocol design, actuator integration, and real-world vulnerabilities affecting connected devices.

Participants received hands-on exposure to real-world IoT vulnerabilities, cyber-attack simulations, and defensive strategies for connected devices. Key focus areas included IoT systems and protocol vulnerabilities, firmware and bootlog analysis, and securing communication in IoT environments.

Cybersecurity Workshop Conducted for CSJM University Faculty Across Seven Districts

C3iHub, IIT Kanpur, in collaboration with Chhatrapati Shahu Ji Maharaj University (CSJMU), Kanpur, and the CSJM Innovation Foundation, Kanpur, conducted a Cybersecurity Workshop for faculty members representing degree colleges across seven districts under CSJM University's jurisdiction—Kanpur Nagar, Kanpur Dehat, Unnao, Etawah, Auraiya, Kannauj, and Farrukhabad.

The workshop was organized at multiple colleges across seven districts as part of C3iHub's cybersecurity outreach program. The initiative focused on enhancing cybersecurity awareness among faculty members and strengthening the effective implementation of the Cybersecurity Vocational Course jointly offered by C3iHub, CSJM University, and CSJM Innovation Foundation.

The Cybersecurity Vocational Course is a semester-long, fully online program delivered in Hindi, designed to equip students with essential cybersecurity knowledge and hands-on skills. The program aims to improve accessibility, practical learning, and inclusivity in cybersecurity education for students across the region.

2nd Workshop on CSCMM Development

C3iHub conducted the 2nd Workshop on Cyber Security Capability Maturity Model (CSCMM) Development in collaboration with NCIIPC, bringing together experts from critical sectors of BFSI, Power & Energy, Telecom, Government, Health , and Transport to validate and seek sector-specific feedback on the 6-sector-specific CSCM Model based on (i) actual evaluation responses of the participants, (ii) AI-based CSCMM solution as demonstrated on the tool.

Overall feedback was taken on the CSCMM Project and tech/policy perspectives on maturity assessment at organizational, sectoral and national level. Created an offline repository of participant specific feedback from focus group discussions (FGDs) on the solution itself to be addressed after the workshop.

Specialized Training Program

Maritime Cybersecurity Training for Indian Ports Association Officials

C3iHub conducted a two-day specialized training program on Maritime Cybersecurity for officials of the Indian Ports Association (IPA) at the IIT Kanpur – Noida Extension Centre from 16 December 2025 to 17 December 2025. The program was designed to enhance cybersecurity preparedness across the maritime and port ecosystem. It included focused sessions on compliance and regulatory requirements, social media threat profiling and dark web analysis, Open-Source Intelligence (OSINT) investigations and suspect profiling, digital forensics and incident response (DFIR), network security assessment, and cloud security.

The program featured the presence of Dr. Arvind Bhisikar, Executive Director (IT), Indian Ports Association; Prof. Manindra Agrawal, Director, IIT Kanpur; Mr. Akhilesh Variar, IPS, National Critical Information Infrastructure Protection Centre (NCIIPC), NTRO; and Dr. Tanima Hajra, CEO, C3iHub. The sessions provided insights on strengthening and future-proofing cybersecurity frameworks to safeguard critical maritime infrastructure.

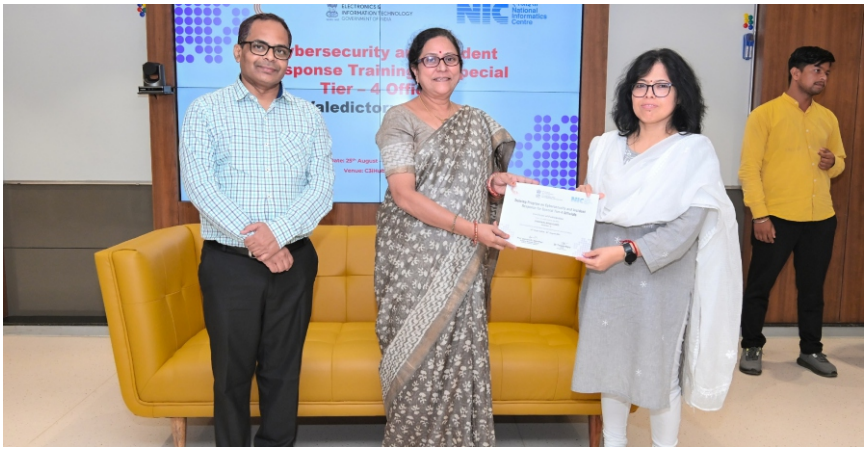
Through such initiatives, C3iHub continues to support cybersecurity capacity building across critical sectors, contributing to enhanced digital and maritime resilience.

Specialized Cybersecurity Training Program for National Informatics Centre Officials

C3iHub conducted an exclusive cybersecurity training program for Special Tier 4 Officers of the National Informatics Centre (NIC), with a focus on the practical application of cybersecurity techniques relevant to e-governance systems, secure digital infrastructure, and national information systems. The program was structured to provide advanced, hands-on exposure to key cybersecurity domains, including digital forensics, offensive cybersecurity techniques, threat intelligence, and malware analysis, enabling participants to address real-world cyber threats effectively.

The objective of the program was to strengthen the cyber defense capabilities of officials responsible for managing critical government IT infrastructure and to equip them with advanced operational skills for detecting, analyzing, and responding to cyber incidents.

To date, the program has trained over 85 officers across six cohorts, contributing to capacity building within India's government cybersecurity ecosystem.



Successful Completion of Cybersecurity Training Program for Ministry of Power Professionals

C3iHub conducted an intensive and highly specialized cybersecurity training program for the 8th batch of professionals from organizations under the Ministry of Power, Government of India. The batch comprised 30 professionals representing various power sector entities. The training program was designed to address the cybersecurity requirements of critical power infrastructure by combining foundational concepts with advanced, sector-specific modules. The curriculum focused on practical and contextual cybersecurity challenges relevant to the power and energy ecosystem.

The objective of the program was to equip power sector professionals with the skills to detect, assess, and respond to cyber threats targeting critical infrastructure, thereby supporting the development of a resilient and secure digital energy ecosystem. To date, the program has been delivered across eight cohorts, training over 200 professionals from the power sector.

New Partnerships

HQ Central Command, Indian Army

C3iHub, IIT Kanpur, and Headquarters Central Command, Indian Army, signed a Memorandum of Understanding (MoU) in November 2025 to initiate an advanced cybersecurity training program for military personnel. The program, to be delivered by C3iHub, comprises two structured modules of three months each, designed to equip military units and formations with advanced cyber defence competencies. The training framework focuses on developing a comprehensive understanding of emerging and evolving cyber threats, strengthening incident response and mitigation capabilities, and enhancing overall operational preparedness. By integrating contemporary cyber defence frameworks into formal training structures, the initiative aims to strengthen the digital security posture across the operational theatre and contribute to a more resilient cyber defence ecosystem.

The MoU was formalized in the presence of Lt General Naveen Sachdeva, Chief of Staff, Headquarters Surya Command, and Prof. Somitra Sandhya, Program Director, C3iHub. The MoU was signed on behalf of C3iHub by Dr. Tanima Hajra, CEO, C3iHub.

National Mineral Development Corporation (NMDC)

IIT Kanpur and the National Mineral Development Corporation (NMDC), a Navratna Public Sector Enterprise under the Ministry of Steel, Government of India, signed a Memorandum of Understanding (MoU) to strengthen collaboration in cybersecurity, information security, artificial intelligence (AI), machine learning (ML), digital transformation, and next-generation technological applications across NMDC's IT and operational technology (OT) ecosystems.

The MoU was signed by Mr. Satyendra Rai, Executive Director (Digital Transformation), NMDC Limited, and the Dean of Research and Development, IIT Kanpur, in the presence of the Project Director, Project Leaders, and officials from NMDC and the I-Hub NTIHAC Foundation, C3iHub, IIT Kanpur.

Under the MoU, C3iHub will support NMDC in areas including cyber risk assessment, vulnerability analysis, security governance, incident response planning, and benchmarking of Security Operations Centre (SOC) models. The collaboration will also explore the application of AI/ML-driven solutions, digital twins, predictive maintenance frameworks, and advanced data analytics to enhance operational efficiency and resilience across NMDC's mining ecosystem.

Delhi Metro Rail Corporation (DMRC)

C3iHub, IIT Kanpur, and the Delhi Metro Rail Corporation (DMRC) signed a Memorandum of Understanding (MoU) to strengthen collaboration in the field of cybersecurity and other areas of mutual interest. The partnership focuses on integrating advanced research and innovation into DMRC's operational and digital ecosystem.

The MoU aims to facilitate joint research, capacity building, and technology development initiatives, with a particular emphasis on strengthening cybersecurity frameworks across critical infrastructure systems. Through this collaboration, advanced cybersecurity research is expected to be translated into practical, real-world applications, enhancing the resilience and security of essential urban infrastructure such as metro networks. The MoU was signed in the presence of Dr. Vikas Kumar, Managing Director, DMRC, and Prof. Manindra Agrawal, Director, IIT Kanpur. The MoU was signed on behalf of C3iHub by Dr. Tanima Hajra, CEO, C3iHub.

Maharashtra Metro Rail Corporation

The Maharashtra Metro Rail Corporation Limited (Maha Metro) signed a Memorandum of Understanding (MoU) with C3iHub to strengthen cybersecurity across its metro rail operations. The agreement was formalized at Metro Bhavan, with Mr. Shravan Hardikar, Managing Director, Maha Metro, and Dr. Tanima Hajra, CEO, C3iHub, signing the MoU.

The collaboration focuses on strengthening IT systems, enhancing cybersecurity awareness among officials, and ensuring compliance with international and national cybersecurity standards, including ISO/IEC 27001:2022, NIST Cybersecurity Framework (NIST-CSF), and CERT-In guidelines.

Key Focus Areas of the MoU

- Cybersecurity gap assessment, including Vulnerability Assessment and Penetration Testing (VAPT)
- Development of policy and governance frameworks
- Roadmap for risk mitigation
- Continuous security monitoring

The cybersecurity evaluation under the MoU covers metro operations in Nagpur (Zero Mile OCC, Hingna Depot, Sitabuldi, Airport South, Khapri, and Metro Bhavan) and Pune (OCC, Range Hills Depot, Civil Court, PCMC, Swargate, and Metro Bhavan). The scope includes critical systems such as operations control, signalling, telecommunications, power supply, automatic fare collection, building and tunnel management systems, and train onboard systems.

Automotive Research Association of India (ARAI)

C3iHub has signed a MoU with the Automotive Research Association of India (ARAI) to advance research, innovation, and collaboration in the field of automotive security. The MoU was formally signed by Dr. Reji Mathai, Director, ARAI, Prof. Tarun Gupta, Dean of R&D, IIT Kanpur, and Dr. Tanima Hajra, CEO, C3iHub, in the presence of Prof. Manindra Agrawal, Director, IIT Kanpur.
This strategic collaboration will focus on developing innovative solutions, advancing joint

research, and addressing emerging challenges in automotive cybersecurity. With the rapid adoption of connected and autonomous vehicles, ensuring safe, secure, and resilient mobility systems has become a global priority. Through this partnership, C3iHub and ARAI aim to create impactful technologies that enhance the safety of future transportation systems.

Webinars Organized

Understanding India's Digital Personal Data Protection (DPDP) Act

C3iHub conducted a webinar titled “Understanding India's Digital Personal Data Protection (DPDP) Act” on 10 December 2025, as part of the HACK IITK 2026 engagement activities. The webinar focused on key aspects of the DPDP Act, including its core provisions, implications for organizations, compliance requirements, and the broader benefits and future outlook for India's digital ecosystem.

The session featured an expert panel comprising Dr. Bharat Panchal, Chief Risk and Regulatory Officer (APAC & Middle East), Capital One, and Commander Vivek Yadav, Director (IT and Cybersecurity), Ministry of Defence. The discussion was moderated by Dr. Ras Dwivedi, Chief Technology Officer, C3iHub, IIT Kanpur.

The webinar provided participants with practical insights into data protection regulations and their implementation within India's evolving digital landscape.

SCAN QR to watch:
https://www.linkedin.com/event/manage/7404396355189706752/

Careers in Cybersecurity: Skills, Roles, and Roadmaps for the Digital Future

C3iHub conducted a webinar titled “Careers in Cybersecurity: Skills, Roles, and Roadmaps for the Digital Future” on 13 January 2026 as part of the HACK IITK 2026 webinar series.

The session focused on emerging career pathways in cybersecurity, required skills, evolving professional roles, and learning roadmaps for students and early-career professionals navigating the digital security landscape. The webinar featured expert speakers Mr. Rajiv Swarup, Former President, Shiv Nadar University and Senior Corporate Vice President, HCLTech, and Prof. Somitra Sanadhya, Program Director, C3iHub, IIT Kanpur, and Professor, Wadhwani School of AI and Intelligent Systems, IIT Kanpur. The session was moderated by Commander (Retd.) Bheem Reddy, Vice President, Cybersecurity Operations, C3iHub.

The discussion provided participants with practical insights and guidance on building sustainable careers in the cybersecurity domain.

SCAN QR to Watch:
https://www.linkedin.com/feed/update/urn:li:activity:7416382665056022528

Eminent Visitors

Shri Adil Zainulbhai Chairman, Network18 Media & Investments Limited

C3iHub hosted Shri Adil Zainulbhai, Chairman, Network18 Media & Investments Limited, and Chairperson of the Board of Governors, Indian Institute of Technology Ropar and Indian Institute of Technology (IIT) Goa, during his visit to IIT Kanpur.

During the visit, Shri Zainulbhai was received by Dr. Tanima Hajra, CEO, C3iHub; Dr. Anindita Gayen, AVP (R&D); and Dr. Anand Handa, CSO, C3iHub. The leadership team briefed him on C3iHub's ongoing projects, research initiatives, and the cybersecurity solutions being developed at the Hub. The visit coincided with the 66th Foundation Day celebrations of IIT Kanpur, where Shri Zainulbhai also served as the Chief Guest, marking a significant occasion for the institute and its associated initiatives.

Dr. Harrick Vin, CTO at Tata Consultancy Services

Dr. Harrick Vin, Chief Technology Officer (CTO) at Tata Consultancy Services (TCS), visited C3iHub, on the sidelines of Samanvay 2025. He was welcomed by Prof. Somitra Sanadhya, Project Director, C3iHub, and Dr. Ras Dwivedi, Chief Technology Officer, C3iHub.

During the visit, Dr. Vin was briefed on the indigenous cybersecurity technologies developed at C3iHub and was given an overview of ongoing research, innovation, and deployment initiatives. He also visited the Security Operations Center (SOC), where he gained insights into real-time monitoring capabilities and applied cybersecurity operations.

A Delegation of 29 Government Officers Visited C3iHub

A delegation of 29 officers, including Directors, Deputy Secretaries, Deputy Directors, Assistant General Managers (AGMs), Deputy General Managers (DGMs), and Scientists from various ministries and organizations—such as the Ministry of New and Renewable Energy, Central Public Works Department, Indian Cyber Crime Coordination Centre (I4C), Food Corporation of India, Department of Financial Services, National Highways Authority of India, Ministry of Minority Affairs, Ministry of AYUSH, Ministry of Labour and Employment, and Central Water Commission—visited C3iHub, IIT Kanpur as part of a campus tour. The visit was organized under the Special Capacity Building Programme on Technology, Economics and Public Policy: A Training on Data-Driven Governance, conducted by the National Centre for Good Governance.

Brig MS Jamwal Station Commander, Kanpur Cantonment

Brigadier M.S. Jamwal, Station Commander, Kanpur Cantonment, accompanied by a team of senior officers, visited C3iHub, IIT Kanpur to gain first-hand insights into the cybersecurity initiatives being undertaken at the Hub. The visit focused on exploring avenues for deeper collaboration and further strengthening the ongoing working relationship between the Indian Army and C3iHub, IIT Kanpur.

Awards and Accolades

IIT Kanpur Receives Special Jury Recognition at DSCI Excellence Awards 2025

The Indian Institute of Technology Kanpur was conferred with the 'Special Jury Recognition for Consistent Performance' in Best Practices in Cybersecurity Education and Research at the DSCI Excellence Awards 2025. The award was presented by Shri Navin Kumar Singh, National Cybersecurity Coordinator of India, during the DSCI Annual Information Security Summit (AISS) 2025, held in New Delhi.

This recognition reflects IIT Kanpur's sustained efforts in strengthening India's cybersecurity ecosystem through education, research, and innovation. C3iHub continues to work closely with IIT Kanpur to advance indigenous cybersecurity capabilities, promote innovation, support startups, and enable advanced research and skill development.

IIT Kanpur has previously received the DSCI Excellence Award for Best Security Practices for Cybersecurity Evangelists in Academic Research and Education in 2023 and 2024, with the continued recognition underscoring its leadership and impact in the domain of cybersecurity education and research.d to enhance security capabilities and address the evolving challenges in cybersecurity.

Annual Day Celebration 2025

GLIMPSES


ANNUAL DINNER 2025
AN EVENING OF EXCELLENCE


3i Hub
INDIAN INSTITUTE OF TECHNOLOGY


TRAINING
FOR
PORT OFFICIA
3iHub, IIT Kanpur

Editorial Team

Dr. Anindita Gayen
AVP (R&D)

Dr. Madhusree Kole
Manager (R&D Programs)

Mr. Aditya Singh Gaur
Deputy Manager (Research & Media)

Ms. Shivangi Agnihotri
Technical Writer

Contact us

2nd Floor, TECHNOPARK@IITK Phase I,
IIT Kanpur, Kanpur-208016, U.P., India

info@c3ihub.org

0512 259 2120/2273

www.c3ihub.org

Follow Us

/C3iHub.org

@HubC3i

@c3ihub

/company/c3i-hub