National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

भारतीय विज्ञान संस्थान

CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security

DSCI
PROMOTING DATA PROTECTION

Ministry of Electronics & Information Technology
Government of India
सत्यमेव जयते

Cybersecurity R&D & Innovation Roadshow 2023

2 & 3 February

IISC Bangalore, Gulmohar Marg Mathikhere

AGENDA

DAY 1

10:00 - 10:15	Welcome Address	
10:15 TO 11:00	Session 1: Opportunities in Cyber Security Research	
11:00 TO 11:15	Tea Break	
11:15 TO 13:00	Presentation from Researchers	Innovation Challenge for Students (Closed Door)
13:00 TO 14:30	Lunch	
14:30 TO 15:30	Paper presentation Competition on below themes: 1. IoT and embedded security 2. Cloud security 3. SCADA/OT Security 4. Automotive Security 5. Overall cyber security 6. Digital Forensics Technology /Mac Forensics 7. Network/ Application Security	Break & Expo visit (Start-up / Researcher Industry interactions)
14:30 TO 17:00		
16:30		
17:00		

DAY 2

10:00 TO 10:45	Inauguration
10:45 TO 11:45	Masterclass on Research Productization and Commercialization
11:45 TO 12:00	Tea Break
12:00 TO 12:45	Session 1: Digitization & Emerging Technology: Agenda for Cyber Security Research
12:45 TO 13:30	Session 2: Case Studies of Industry Collaborations for Cybersecurity Research.
13:30 TO 14:30	Lunch
14:30 TO 15:15	IISc's Presentation: Covering researchers, research areas, and research works
15:15 TO 16:00	Session 4: Security Vision 2027 : Industry-Researcher Collaboration
16:00 TO 16:20	Tea Break
16:20 TO 16:30	Session 6: Resilient Cyber Security Ecosystem - Making Triple Helix work(Government, Industry and Academia)
16:30 TO 17:15	Prize Distribution for Paper Presentation Competition

Event Statistics

In-Person Event

Sector-wise participation stats:

97	7	4	8
Academia	Banking	Consulting Firm	Defence
27	28	206	91
Government Org	Research Bodies	Software & IT Companies	Other

EVENT SUMMARY

National Cybersecurity Centre of Excellence (NCoE), a joint initiative of the Data Security Council of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY), in collaboration with the Indian Institute of Science (IISc) – Bangalore and CySecK, hosted a Cybersecurity R&D & Innovation Roadshow 2023 at IISc campus on the 2nd - 3rd Feb, 2023, to provide a unique platform for academia, research institutes, start-ups, and PSUs to exhibit their cybersecurity research findings, prototypes, and products to further promote development and innovation within the cybersecurity industry.

Attendees of the roadshow included industry leaders, start-up founders, security professionals, security architects, and security professionals who had the opportunity to learn about distinguished cybersecurity research and innovative products, domain technology capabilities, prototypes, solutions, lab infrastructures, and tools. It attracted 150+ organisations and 30 exhibitors from National CoE-incubated Startups, Research bodies, Academia, and Government-owned enterprises. C-DAC (Centre for Development of Advanced Computing), C-DOT (Centre for Development of Telematics), SETS (Society for Electronic Transaction and Security) – Chennai, Chipspirit, EXPLIoT, SecneurX, SecOps Solution, Innspark Solutions, etc. are just a few of the notable organisations.

This informative event was a step towards achieving MeitY's objectives of fostering innovation and encouraging cyber security product entrepreneurship in the country. It also sought to investigate the potential for collaboration and co-creation among researchers and to expedite product development in the business sector.

Day 1

Session: Welcoming

Col. Vineet Madan
Director, Cybersecurity Technology, DSCI NCoE

Dr. Karthik Rao Bappanad
Centre Head, CySecK

Arpit Dubey
Senior Consultant - National CoE (Cyber Security), DSCI

Col. Vineet Madan, Director, National CoE,Arpit Dubey, Senior Consultant - National CoE (Cyber Security), Data Security Council of India, and Dr. Karthik Rao Bappanadu, Head, CySecK, gave the welcome address to launch the cybersecurity R&D & Innovation Roadshow in Bangalore. They provided the event's context and elaborated on the current cybersecurity landscape, recent developments, and challenges in cybersecurity. The panel thanked all attendees for participating in the roadshow and contributing to the advancement of cybersecurity.

Dr. Karthik B. elaborated on tech adoption and emphasised that digital adoption requires a solid cybersecurity foundation by stating: "As more and more people adopt IT, the need to secure IT soars, elevating the importance of cybersecurity. Therefore, a robust layer of cybersecurity must be implemented ". The panellists expressed their delight at seeing so many students eager to pursue careers in this field.

Col. Vineet M. addressed startups present at the event, urging them to view themselves as spearheads of cybersecurity in India rather than startups. He encouraged startups to reach out to the National CoE for use cases and to participate in the upcoming hands-on Azure ML workshop.

Session 1:

Opportunities in Cyber Security Research

Dr. SD Sudarshan
Executive Director,
CDAC

Dr. Dattatraya Kulkarni
McAfee Fellow

Prof. Urbasi Sinha
Professor,
Raman Research Institute

This panel discussion on "opportunities in cyber security research" was led by Dr. Sudarshan from C-DAC, Dr. Dattatraya Kulkarni from McAfee, and Prof. U Sinha from Raman Research Institute. They discussed various aspects of India's skilling initiatives, the shortage of skilled labour in the expanding market, and the need for quantum solutions to secure quantum threats. According to statistics, ransomware attacks are the leading type of cyberattack. Prof. Urbasi emphasised that quantum research is globally active at present. She discussed the disadvantages of quantum computers, including the fact that security is completely compromised. Working on solutions is crucial, and we want and require quantum solutions for quantum threats.

Dr. Dattatraya stated that success in both academia and business requires an innate understanding of opportunities and obstacles, which are equally essential. In addition to sharing his industry observations, he introduced the attendees to the 5Cs: Complexity, Connectivity, Closedness, Co-mingling, and Comprehension, which can assist us in analysing the surrounding challenges and opportunities. Dr. Sudarshan concluded the session by discussing DSCI's Cybershikshaa programme, designed specifically for women who wish to enter or transition into cybersecurity from other fields. In addition, he mentioned nasscom's quality matrix for assessing the skills and competencies required for a successful career in cybersecurity. The discussion centred on the government's targeted initiatives and incentives in place to ensure sufficient availability of skilled labour.

Presentations from researchers:

CDAC (Centre for Development of Advanced Computing), Bangalore

Gopinath from CDAC Bangalore elaborated on CDAC's cybersecurity-focused products and solutions. He stated that CDAC provides numerous cybersecurity solutions, such as script analysis, ATM fraud detection, video KYC solutions, and DNS security. AAGNEY, a client-based email security solution, and a secure document storage and access logging application are also provided. Additionally, CDAC has created a video KYC solution and a national blockchain framework.

Gopinath P

Joint Director, CDAC

In addition to offering specific cybersecurity products, the organisation focuses on capacity-building programmes, raising awareness about information security, and providing courses for graduates seeking IT careers. They offer Managed Security Services and Managed Detection and Response services 24 hours a day, seven days a week to businesses in a variety of industries. Mission-mode projects such as Exascale Computing, indigenous microprocessors, Quantum Computing, AI, Language Computing, and the Internet of Everything are a part of CDAC's broader work. Their popular PARAM Supercomputing facility operates 24 hours a day, seven days a week, 365 days a year, and they provide Internet of Things (IoT) products such as smart water distribution networks, smart energy metres, and air quality control devices.

C-DOT (Centre for Development of Telematics)

C-DOT elaborated on their work in post-quantum cryptography and quantum key distribution (QKD), as well as their preparedness to provide solutions in these areas. Quantum security is indispensable for protecting vital voice, video, and data transmissions and storage. Both legacy and modern networks must be protected. Time and cost constraints, as well as ensuring that solutions are standards-driven and in line with quantum-safe migration approaches recommended by standard bodies, are among the implementation challenges.

C-post-quantum DOT's cryptography product line includes a compact encryption module and a quantum-secure smart video IP phone. Both have been developed indigenously in India and are adaptable to any deployment and post-quantum algorithm selection. C-DOT is also involved in cybersecurity, addressing issues such as identifying nation- or state-sponsored threat actors, well-resourced attacker groups, and the increasing number of

attackers utilising open-source tools. They analyse big data in real-time to produce actionable intelligence and provide corrective measures against cyber threats like spyware, keyloggers, ransomware, and bots.

Nagarjuna College of Engineering and Technology, Bangalore

Dr. Sanju Kumaria, the head of the Information Science Engineering department at the Nagarjuna College of Engineering and Technology in Bangalore, elaborated on a project that employs emerging technologies such as machine learning to address cybersecurity threats in smart agriculture. The objective of the project is to create a secure smart farming environment in India by 2035, in which all agricultural activities are managed by IoT and other technological devices.

The objective of the project is to provide farmers with security and an advisory system to optimise crop production and market demand. To ensure security, the research team proposes creating an intrusion detection system to thwart cyber attacks that could result in production losses in agriculture. In intelligent farms, the system would be implemented at the physical, network, and storage layers of the IoT system. The team has also developed an approach to detect and monitor potential attacks based on machine learning. Initial experiments utilising existing datasets demonstrated an attack identification accuracy of 94-98%. The group is collaborating with two universities to create a testbed for smart farming experiments.

Cyberlabs from IIIT Kottayam

The IIIT Kottayam team includes Panchami, Mahima, Niranjan, Samhita, Gauri, and Aditya, who are all members of the Cybersecurity Research group (Cyberlabs). They presented four research papers on diverse cybersecurity and quantum technology topics. Niranjan discussed the significance of random number generation in cryptography as well as the team's technique for generating high-entropy random numbers using quantum machines. Mahima presented their findings regarding quantum cryptoanalysis and quantum-resistant authentication. It focuses on the security of classical cryptosystems currently in use. Aditya elaborated on their project to predict attacks using machine learning and self-supervision, which outperforms conventional methods in datasets of intrusion detection. He stated that the team is currently implementing this strategy on multiple other data sets in order to obtain more data and determine how this algorithm performs on various data sets.

Vellore Institute of Technology (VIT), Chennai

The Vellore Institute of Technology (VIT), Chennai campus team primarily presented their research on intrusion detection systems, malware detection, reversible data hiding schemes, steganography, DDOS detection in UAVs and wireless networks, and cancellable biometric systems. The team has also developed a tool called muraks to identify Android API vulnerabilities. Their malware detection research involves visualising executable code to identify malware patterns. Then, algorithms based on deep learning are used to detect the presence of malware. While machine learning has been successful in detecting malware on PCs, it has not been as effective in detecting malware on Android.

The team has also developed algorithms for intrusion detection systems in UAVs and wireless networks, in order to defend against attacks. They have worked on reversible data hiding algorithms for image-based applications, data leak prevention, and the security of private cloud infrastructure. The team at VIT Chennai is engaged in product development, real-time issue resolution, consulting services, and capacity building. They have collaborated with numerous entities, including K7 Computing, cybersecurity firms, and local law enforcement agencies. The team has received funding to establish a cyber threat intelligence lab and regularly hosts workshops, certification programmes, and hackathons to disseminate knowledge about cybersecurity.

The Society for Electronic Transaction and Security (SETS)

Society for Electronic Transaction and Security (SETS) centred its presentation on the organization's accomplishments. The SETS was founded under the direction of the late President, Dr. APJ Abdul Kalam. Currently, the organisation focuses on resolving and providing solutions for cybersecurity issues. SETS is composed of multiple research and development groups, including Cryptology and Computing, Hardware Security, Quantum Security, Network Security, and Service and Training.

SETS has partnered with a number of organisations, including DRDO and IIT Madras, to provide cybersecurity solutions. Quantum Security and ISC Bangalore have collaborated on post-quantum cryptography. The company has access to supercomputer facilities and has implemented cybersecurity solutions for various government agencies. SETS has signed Memorandums of Understanding (MoUs) with multiple agencies and has expanded into multiple cryptography and cybersecurity fields since its inception.

Cybersecurity R&D & Innovation Roadshow

Day 2

Session: Inauguration

Vinayak Godse
CEO,
DSCI

Karthik Rao Bappanad
Centre Head,
CySecK

Rajesh Sundaresan
Professor, IISC

Vinayak Godse, CEO of the Data Security Council of India, Karthik Rao Bappanad, Center Head of Cyseck, and Professor Rajesh Sundareshan from IISC set the stage for Day 2 of the Cybersecurity R&D & Innovation Roadshow - IISC Bangalore. Highlighting the growth of the cybersecurity startup ecosystem in the United States over the past ten to twelve years, they reported that startups are now solving problems across multiple industries, including those that are crucial to national security. They emphasised the significance of cybersecurity research intervention for sustaining the digitization narrative and developing innovative solutions to address challenges such as increased communication capability and infrastructure optimisation. They concluded by describing how the Data Security Council of India (DSCI) intends to bridge the gap between research and productization by partnering with leading academic institutions and organisations.

Masterclass on Research Productization and Commercialisation

Nishant Chandran
Principal Researcher,
Microsoft Research, India

Vinayak Godse
CEO, DSCI

The second day of sessions began with an engaging masterclass presented by Nishant Chandran, Principal Researcher at Microsoft Research, and Vinayak Godse, Chief Executive Officer of the Data Security Council of India. The masterclass examined the significance of research for economic development and national security. They emphasised the importance of research visibility and mentioned a tool on the website of the National CoE that tracks professors working in 13 areas of cybersecurity. This utility helps identify professors working in research-funding-relevant fields.

The masterclass emphasised the need for startups to comprehend cybersecurity research in order to productize and commercialise research. It highlighted the importance of collaborations between academia, industry, and startups to ensure that research is effectively applied and commercialised. In addition, speakers discussed the difficulties of transferring and storing large amounts of data and proposed collaborating with academic partners and diversifying areas of expertise in order to find solutions. The masterclass included a segment on the difficulties of commercialising research and the necessary legal arrangements for transferring intellectual property from academia to industry. They urged researchers to prioritise their research problems and work collaboratively to solve the last-mile problem.

Finally, the significance of international collaboration and concept demonstration prior to productization and commercialization was emphasised. On the necessity of collaborations to ensure the effective productization and commercialization of cybersecurity research, valuable insights were provided. The session concluded with a lively question-and-answer session, during which the speakers discussed bureaucracy and the necessity of a legal framework to support collaborative research efforts.

Session 1: Digitization & Emerging Technology: Agenda for Cyber Security Research

Dr. GK Patra
Scientist,
CSIR C-MMACS

Sandeep Tiwari
Director/Incharge - Infosec,
National Payments
Corporation Of India (NPCI)

Prof. Bhavana
Associate Professor,
IIS, Bengaluru,
Department of Computer
Science and Automation

Saikrishna BVS
Founder and CEO,
Pinaca Technologies

Day 2 began with an engaging session on Digitization & Emerging Technology: Agenda for Cyber Security Research with a panel consisting of Dr. Gopal Patra, Scientist, Council of Scientific and Industrial Research (CSIR) C-MMACS (CSIR Center for Mathematical Modelling and Computer Science), Sandeep Tiwari, In charge - Infosec National Payments Corporation of India (NPCI) Mumbai, Prof. Bhavana Kanukurthi, IISc, and SaiKrishna BVS, Pinaca Technologies.

The speakers highlighted that emerging technologies such as AI, ML, IoT, virtual reality, and drones are being integrated into cybersecurity research to tackle increasingly complex malicious cyber threats and attacks. Future solutions to cybersecurity threats are likely to rely on these technologies. Nonetheless, security is frequently neglected during the initial phases of system development, resulting in potential system vulnerabilities. To avoid creating exploitable vulnerabilities, it was emphasised that security and privacy must be considered from the start. The prevalence of cyber-physical systems is on the rise, increasing the attack surface for malicious actors. Therefore, proactively addressing cybersecurity challenges and adapting to new threats is essential.

In addition, the panel emphasised that interdisciplinary research, such as the intersection of cryptography and game theory, can provide valuable insights to assist in addressing security issues. By fostering collaboration between various fields and leveraging their combined expertise, more robust and secure systems can be created, thereby mitigating the risks associated with the advancement of digital technology.

Session 2: Case Studies of Industry Collaborations for Cybersecurity Research

Abilash Soundararajan
Founder & CEO,
PrivaSapien

Amarnath Choudhary
Chief Executive Officer,
Mode Finserver Pvt. Ltd.

Abilash Soundarajan, founder and CEO of PrivaSapien, and Amarnath Choudhary, founder and CEO of Mode Finserver Pvt. Ltd., participated in this session. Abilash discussed the challenges of privacy and security in the context of AI during the session. He discussed AI-related issues and countermeasures. He emphasised the importance of addressing privacy concerns, describing neural network capabilities, and removing bias from data sets used to train AI. The focus was on visualising and mitigating privacy risks to safeguard human consciousness, as well as controlling data. He also discussed the efforts of PrivaSapien to develop a new alternative for humanity.

CEO of Mode Finserver Pvt. Ltd. Amarnath Choudhary described the company's efforts to address offline payments and connectivity issues in regions with low bank penetration and poor internet. Moreover, he discussed the company's partnership with IISC Bangalore to develop AI-enabled risk assessment and customer-behavioral solutions. Participants, including students, were encouraged to attempt the international challenges and projects.

IISc's Presentation: Covering researchers, research areas, and research works

Vinod Ganapathy
Professor,
Department of Computer Science and Automation

Professor Vinod Ganapathy of the Department of Computer Science and Automation at IISC led the presentation. He discussed power grid security and explained that the power grid is increasingly a cyber-physical system and that the security properties of individual systems are poorly understood. He elaborated on IISC's new initiative, a cluster-wide effort with the Power Grid Corporation of India to secure power grids. The organization's mission is to serve as a hub and think tank for all infrastructure and security issues that arise in the power grid.

Prof. Vinod centred one of his group's projects on privacy in the age of drones. The issue is how to protect citizens' privacy when delivery drones equipped with cameras fly above us. Using a cryptographic method known as secure multi-party computation, two parties, the regulatory authority and the privacy-conscious citizen, can communicate

without revealing their own inputs, while still producing a meaningful result of the computation.

This solution enables citizens to identify which drones have them in their field of view, and then communicate with these drones either through the regulatory authority or by establishing a connection with these drones in order to audit their regulatory compliance. The drones are equipped with trusted hardware, which attests the software stack running on the drone and demonstrates to the citizen on the ground that the software stack is a privacy-enhancing software stack.

Session 4: Security Vision 2027: Industry-Researcher Collaboration

Geetha Hari
Practice Director,
Wipro Limited

Dr. Kapali
Siemens

Vaidyanath R Iyer
Chief of Operation, IBM
security command centre

Dr. Harish Ramani
IIIT

The panel for this session featured Geetha Hari, Practice Director, Wipro Limited, Dr. Kapali, Siemens, Vaidyanath R Iyer, Chief of Operation, IBM security command centre and Dr. Harish Ramani, IIIT. The session dealt with security vision for India for 2027. The issue of CCTV deployment in India, where the government, private citizens, and traffic police all have CCTV cameras was discussed. The panel suggested approaching the problem of CCTV deployment vertically with regulations and methods in place to address privacy concerns. They also discussed alternative solutions such as anonymity networks and information-theoretic security, as well as the impact of quantum computing on cryptography and possible solutions.

Furthermore they discussed industry research collaboration and their visions for security in 2027. They emphasised on importance of collaboration, co-innovation, and co-creation in driving innovation and scaling up startups. They stated that India has the potential to drive innovation in this field. Additionally, they added that the Indian government's concept of data embassies can help address the challenge of sovereignty of data while allowing foreign organizations to operate within the country with diplomatic immunity.

Session 5: Resilient Cyber Security Ecosystem - Making Triple Helix Work (Government, Industry, and Academia)

KPM Das
National Cyber Security Officer at Cisco

Madhesh V
Centre for e-governance, Government of Karnataka

Prof. Virendra Singh
Professor of Computer Science & Electrical Engineering, Indian Institute of Technology, Bombay

KPM Das, National Cyber Security Officer at Cisco, Madhesh V., Centre for e-governance, Government of Karnataka and Prof.Virendra Singh, Professor of Computer Science and Electrical Engineering, steered the session titled "Resilient Cybersecurity Ecosystem - Making Triple Helix Work." They discussed the triple helix strategy, which has been identified as an effective method for addressing complex problems in the cybersecurity ecosystem. The panel emphasised the importance of a unified vision and coordinated efforts to protect our critical infrastructure and personal information. Attendees witnessed a comprehensive discussion on the evolving threat landscape and integrated cybersecurity solutions to combat them, taking into account the three core domains of academia, industry, and startups.

Cybersecurity challenges and opportunities in an increasingly technologically dependent world were discussed. The speakers emphasised the significance of considering security and privacy from the outset of development, highlighting the interdependence of disciplines and the need for interdisciplinary research to create more secure systems.

In addition, they discussed the significance of cybersecurity literacy and the role of government, industry, and academia in assisting startups in this field. Also discussed was the difficulty of scaling cybersecurity solutions for a large population, such as India's, and the significance of user-friendly design in cybersecurity products. The speakers acknowledged the need for incentives to encourage users to adopt secure practises when interacting with digital systems and suggested that the government could offer incentives for products that promote mass cybersecurity awareness.

Prize Distribution for Paper Presentation Competition

Cybersecurity industry, academic institutions, and government organisations participated in the Cybersecurity R&D & Innovation Roadshow to promote cybersecurity research and entrepreneurship. IISc Bangalore's version concluded with the announcement of the winners of the Paper Presentation Competition. The first prize was secured by two teams,

Team 1: Hemant Rathore, BITS Pilani – Goa (Team leader), Adarsh Nandanwar, BITS Pilani – Goa, Sanjay Sahay BITS Pilani – Goa and Mohit Sevak, Microsoft, Hyderabad.

Hemant Rathore
BITS Pilani,
Goa Campus

Adarsh Nandanwar
BITS Pilani,
Goa Campus

Sanjay K. Sahay
BITS Pilani,
Goa Campus

Mohit Sewak
Microsoft,
Hyderabad

Our research paper on *Adversarial Superiority in Android Malware Detection: Lessons from Reinforcement Learning based Evasion Attacks and Defenses*

Has won the ***first prize*** at the **Paper Presentation Competition**

Team 2: Pradeep Kumar Duraisamy Soundrapandian VIT, Chennai (Team Leader) and Geetha S.

Pradeep Kumar D S

Geetha S

Our research paper on *"Android Communication Security: Protecting Apps from Leaking Privileges"*

Has won the ***first prize*** at the **Paper Presentation Competition**

The second prize was secured by Mohit Sevak from BITS Pilani – Goa (Team leader), Sanjay K. Sahay, BITS Pilani – Goa and Hemant Rathore, BITS Pilani – Goa.

Mohit Sewak
Microsoft,
Hyderabad

Sanjay K. Sahay
BITS Pilani,
Goa Campus

Hemant Rathore
BITS Pilani,
Goa Campus

Our research paper on ***Green Forensics: Deep Hybrid Edge-Cloud Detection and Forensics System for Battery-Performance-Balance Conscious Devices***

Has won the ***second prize*** at the **Paper Presentation Competition**

The third prize was secured by Dr. K R Ramkumar, Chitkara University, Punjab (Team leader), Taniya Hasija, Chitkara University, Punjab, Dr. Bhupendra Singh, CAIR, DRDO, Banglore, Dr. Amanpreet Kaur, Chitkara University, Punjab and Dr. Sudesh Mittal, Chitkara University, Punjab.

Dr. K. R. Ramkumar
Chitkara University,
Punjab

Ms. Taniya Hasija
Chitkara University,
Punjab

Dr. Bhupendra Singh
CAIR, DRDO,
Banglore

Dr. Amanpreet Kaur
Chitkara University,
Punjab

Dr. Sudesh Mittal
Chitkara University,
Punjab

Our research paper on ***"A Novel Polynomial based Symmetric Key Cryptography using Polynomial Interpolation Methods"***

Has won the ***third prize*** at the **Paper Presentation Competition**

The segment came to an end with the organisers expressing gratitude to everyone who contributed to the success of the roadshow. By bringing together experts from various fields, the event successfully promoted cybersecurity research and entrepreneurship.

Azure/ML Workshop - Security Challenge Winners

Bhagawankripa Mehta
ECE Department
MS Ramaiah Institute of Technology

1st

Amogh M Babu
ECE Department
MS Ramaiah Institute of Technology

2nd

Ravi N
ECE Department
MS Ramaiah Institute of Technology

3rd

Event Gallery

GET IN TOUCH WITH US

Address: 4th Floor, nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP - 201303

Email: ncoe@dsci.in