ज्ञान-विज्ञान विमुक्तये

आचार्य मनिष र. जोशी
सचिव

Prof. Manish R. Joshi
Secretary

सत्यमेव जयते

आज़ादी का अमृत महोत्सव

विश्वविद्यालय अनुदान आयोग
University Grants Commission
(शिक्षा मंत्रालय, भारत सरकार)
(Ministry of Education, Govt. of India)

D.O.No.1-6/2025(e.Gov) **04 आषाढ़, 1974/25th June, 2025**

Subject: **Participation in Nationwide Forensics Hackathon on "CCTV Surveillance Security & Forensics Hackathon 2.0"- reg**

आदरणीय महोदया/महोदय,

The Bureau of Police Research & Development (BPR&D), Ministry of Home Affairs, Government of India, vide its letter No. M-13014/1/2024-AD (Admin)-HQ BPRD-Part-1 dated 20th June 2025 (copy enclosed), has informed regarding the launch of a Nationwide Forensics Hackathon titled "CCTV Surveillance Security & Forensics Hackathon 2.0". A curtain raiser for the event was held on 9th May 2025.

The objective of the Hackathon is to foster the development of indigenous, secure, scalable, and cost-effective CCTV-based technological solutions to address the operational and investigative needs of Law Enforcement Agencies (LEAs) across the country. The Hackathon encourages participation from academic institutions, students, faculty members, researchers, start-ups, and R&D organisations engaged in the areas of forensic science and surveillance technologies.

All Higher Education Institutions are requested to widely publicise this initiative through their institutional websites, notice boards, and official social media handles, and to encourage their stakeholders especially faculty members and students to register and actively participate in the Hackathon.

The last date for registration is **28th June 2025**. Further details, including problem statements, participation guidelines, and the registration process, are available on the official portal: https://www.cyberchallenge.in/bprd. A brochure containing comprehensive information is also enclosed for ready reference.

सादर,

भवदीय,

(मनिष जोशी)

संलग्नक : उपरोक्तानुसार

सेवा में,

सभी विश्वविद्यालयों के कुलपति
सभी महाविद्यालयों के प्राचार्य

M-13014/1/2024-AD (Admin)-HQ BPRD-Part(1)
Bureau of Police Research & Development
Government of India(MHA)

National Highway-48
Mahipalpur, New Delhi-110037
Date: 20th June, 25

To,

Shri Vineet Joshi, Chairman
University Grant Commission

Subject: National Hackathon on "CCTV Surveillance Security & Forensics Hackathon 2.0"-reg

Respected Sir,

The Bureau of Police Research & Development (BPR&D), Ministry of Home Affairs (MHA), in collaboration with NCRB and M/s CyberPeace, recently launched a Nationwide Forensics Hackathon "CCTV Surveillance Security & Forensics Hackathon 2.0" with a curtain raiser event on 9th May, 2025.

2. The aim of the hackathon is to encourage innovators, start-ups, and research institutions to develop indigenous, secure, scalable, and cost-effective CCTV solutions tailored to the specific needs of Law Enforcement Agencies of the nation.

3. In light of the above, you are requested to kindly disseminate this initiative through your website, networks, communication channels, and social media platforms and encourage startups, entrepreneurs, students, your teams and contacts to attend or participate. The last date for Registration is 28 Jun 25. Complete details of the hackathon are available at: **https://www.cyberchallenge.in/bprd**

(Gopesh Agrawal)
IG (Modernization)

CCTV Hackathon

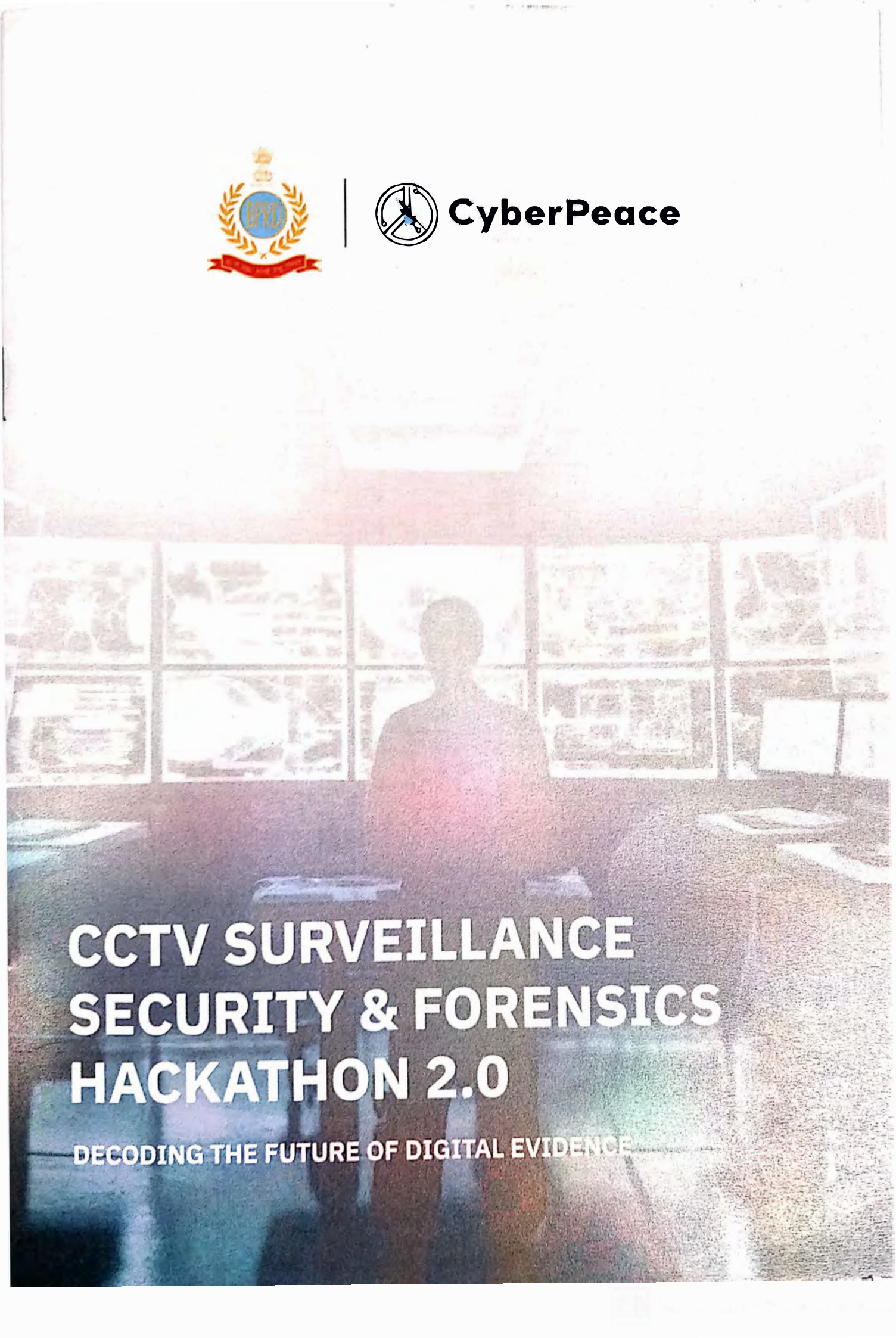
पुलिस अनुसंधान एवम् विकास ब्यूरो

BUREAU OF POLICE RESEARCH & DEVELOPMENT

Ministry of Home Affairs

Government of India

Promoting Good Practices & Standards



CyberPeace

CCTV SURVEILLANCE SECURITY & FORENSICS HACKATHON 2.0

DECODING THE FUTURE OF DIGITAL EVIDENCE

INTRODUCTION

The **CCTV Surveillance Security & Forensics Hackathon 2.0** unites cutting-edge technology with real-world challenges by bringing together innovators from academia, industry, and law enforcement. Participants are tasked with designing and developing indigenous surveillance systems that leverage AI for enhanced threat detection, facial recognition, and predictive analytics, while ensuring robust cybersecurity measures are in place to protect against data breaches and hacking attempts.

Through a rigorous, multi-phased competition—from the registration of teams and evaluation of detailed nomination packages to a 36-hour grand finale—participants will have ample opportunities to showcase their creativity and technical acumen. The hackathon not only challenges teams to create prototypes that are both innovative and practically viable but also provides a dynamic platform for mentorship, networking, and knowledge sharing with experts across multiple disciplines. This collaborative environment is designed to fuel breakthrough innovations in digital evidence gathering and surveillance.

At its core, the event is a call to action for transforming the future of digital security and forensic analysis. By encouraging cross-disciplinary collaboration and equipping law enforcement with state-of-the-art cyber defense tools, the hackathon aspires to empower a new generation of cybersecurity leaders. This approach ensures that innovative surveillance solutions are not only conceptualized but also effectively implemented, ultimately bolstering public safety and national security in an increasingly digital world.

OBJECTIVES

Develop Indigenous CCTV Solutions

Goal: Encourage the creation of locally manufactured surveillance hardware that caters specifically to the domestic market needs.

Focus: Emphasize innovation in the design and production of robust, secure, and reliable CCTV systems.

Integrate AI & Smart Analytics

Goal: Enhance traditional CCTV systems by incorporating state-of-the-art Artificial Intelligence.

Focus: Utilize AI for advanced threat detection, facial recognition, and the development of predictive models to support proactive security policies.

Strengthen Cybersecurity

Goal: Design security measures that safeguard against hacking, unauthorized access, and data breaches within CCTV networks.

Focus: Develop security protocols and features that ensure the integrity and confidentiality of surveillance data.

Deliver Cost-Effective Solutions

Goal: Create scalable, affordable surveillance systems that are adaptable for both densely populated urban environments and dispersed rural settings.

Focus: Prioritize cost efficiency without compromising on the technological robustness or security of the systems.

PROBLEM STATEMENTS & CHALLENGES

Challenge 1: Secure and Indigenous CCTV Design

Title: "Make in India Eyes: Building Secure, Tamper-Proof CCTV Hardware"

Background

India's dependence on imported surveillance hardware creates vulnerabilities like backdoors, insecure firmware, and lack of supply-chain transparency. A shift toward indigenous and secure-by-design CCTV systems is essential to enhance national security and self-reliance.

Overview:

This challenge focuses on designing and developing a next-generation CCTV system that is secure, tamper-proof, and manufactured using domestically sourced components and technologies. The goal is to reduce dependency on foreign surveillance infrastructure by fostering indigenous innovation in both hardware and firmware. Participants must take into account supply chain security, hardware integrity, and firmware-level protections while building a trustworthy surveillance solution that aligns with the "Make in India" initiative.

Objectives

- Design CCTV hardware using Indian or domestically available components.
- Incorporate **secure boot**, **chip-level encryption**, **tamper detection**, and **firmware integrity mechanisms.**
- Promote manufacturing feasibility and mass scalability.
- Address physical layer and supply-chain security threats.

Registration Requirements: During the registration participants need to share a deck in PPT/PDF format (10-12 slides) consisting of their proposed idea highlighting-

- Concept note and clearly defined problem.
- System block diagram/architecture.
- List of indigenous components to be used.
- Estimated cost and manufacturing feasibility.
- Proposed tech stack and security mechanisms.

PROBLEM STATEMENTS & CHALLENGES

Grand Finale Deliverables: The Grand finale will be a 36 hours in-person event.

- GitHub link to firmware/configuration code.
- Installation/setup instructions or emulator documentation.
- A **demo video** (max 5 mins) showing prototype/simulation.
- A **pitch deck** showcasing:
  - Problem & objectives
  - Indigenous innovation
  - Security design
  - Scalability and impact

BONUS POINTS

- **Supply chain transparency features**
- **Firmware signing or boot verification**
- **Manufacturing cost efficiency**

Challenge 2: AI and Smart Analytics Integration

Title: "Smart Eyes: Empowering CCTV with AI for Intelligent Surveillance"

Background

Standard CCTV systems are passive. With AI, they can become intelligent observers, detecting threats, unusual activity, or known faces autonomously and in real time.

PROBLEM STATEMENTS & CHALLENGES

Overview:

This challenge calls for the integration of artificial intelligence into CCTV systems to enable intelligent surveillance. Participants are expected to embed real-time analytics that can autonomously detect threats, recognize faces, analyze crowd behavior, and even predict incidents before they happen. The focus is on using AI to shift from passive video recording to proactive monitoring and response.

Objectives

- Apply AI/ML for real-time analytics
- Implement facial/vehicle recognition with anti-spoofing.
- Enable behavior classification, predictive threat alerts, and cross-camera tracking.
- Leverage **edge AI** for real-time processing.

Registration Requirements: During the registration participants need to share a deck in PPT/PDF format (10-12 slides) consisting of their proposed idea highlighting-

- Use-case scenarios and target environment.
- Model architecture and deployment workflow.
- Description of analytics features and data privacy considerations.
- Dataset plan, training/testing methodology.
- AI toolkits/frameworks to be used (such as: OpenCV, YOLO, TensorFlow).

Grand Finale Deliverables: The Grand finale will be a 36 hours in-person event.

- GitHub repository with AI model and scripts.
- Setup instructions and environment configuration.

PROBLEM STATEMENTS & CHALLENGES

- A **demo video** (max 5 mins) showing prototype/simulation.
- A **pitch deck** explaining:
  - The problem and detection goals
  - Model performance
  - Privacy ethics
  - Scalability and future use

BONUS POINTS

- **On-device (edge) AI implementation**
- **Anti-deepfake or spoofing defense**
- **Multi-camera correlation and real-time insights**

Challenge 3: Cybersecurity in CCTV Networks

Title: "Harden the Grid: Cyber Defense for CCTV Infrastructure"

Background

Networked CCTV systems are prime targets for cyberattacks. Once compromised, they can be used for lateral movement in networks or data exfiltration. A resilient cybersecurity layer is imperative.

Overview:

Modern CCTV systems are vulnerable to cyberattacks that can compromise data integrity, surveillance reliability, and public safety. This challenge asks participants to develop a comprehensive cybersecurity framework tailored to CCTV networks, incorporating robust encryption, secure transmission, user authentication, and intrusion detection to prevent unauthorized access or data breaches.

PROBLEM STATEMENTS & CHALLENGES

Objectives

- Implement secure data transmission (such as: VPN, TLS, DTLS).
- Enable **intruTsion detection/prevention systems (IDS/IPS).**
- Apply **RBAC**, **MFA**, and secure firmware management.
- Integrate **zero-trust** and threat intelligence capabilities.

Registration Requirements: During the registration participants need to share a deck in PPT/PDF format (10-12 slides) consisting of their proposed idea highlighting-

- Defined threat models and scenarios.
- Network architecture highlighting vulnerable areas.
- Cybersecurity layers and controls (encryption, auth, logging).
- Open-source frameworks and tools considered.
- Sample red/blue team test environments (mock attacks, if possible).

Grand Finale Deliverables: The Grand finale will be a 36 hours in-person event.

- GitHub repo with IDS/firewall/authentication tools.
- Deployment scripts and simulation instructions.
- A **demo video** (max 5 mins) of a threat scenario and its mitigation.
- A **pitch deck** that highlights:
  - Cyber risks addressed
  - Technical solution

PROBLEM STATEMENTS & CHALLENGES

- Real-time response
- Deployment scalability

BONUS POINTS

- **Zero-trust architecture**
- **Threat intelligence feed integration**
- **Advanced access control models**

Challenge 4: Cost-Effective Surveillance Solutions

Title: "Budget Watch: Scalable, Affordable Surveillance for All"

Background

Rural and low-income areas need effective surveillance without expensive infrastructure. The goal is to develop affordable yet efficient systems using open-source and low-power platforms.

Overview:

This challenge focuses on building affordable, scalable CCTV systems that can be deployed across diverse environments—including rural areas with limited resources. The idea is to innovate around cost-saving components, energy efficiency, minimal infrastructure dependency, and user-friendly deployment, all while retaining core surveillance capabilities.

Objectives

- Build CCTV systems using peripherals such as **Raspberry Pi**, **ESP32-CAM**, etc.
- Design solar-powered or battery-efficient models.

PROBLEM STATEMENTS & CHALLENGES

- Support basic analytics like motion detection or alerts.
- Enable offline capability with delayed cloud sync.

Registration Requirements: During the registration participants need to share a deck in PPT/PDF format (10-12 slides) consisting of their proposed idea highlighting-

- Defined use-case and problem setting.
- Architecture for rural or urban low-resource deployments.
- Cost analysis and bill of materials.
- Simplicity in deployment, scalability, and maintenance.
- Innovative features that reduce cost and enhance usability.

Grand Finale Deliverables: The Grand finale will be a 36 hours in-person event.

- GitHub repository with source code and documentation.
- Deployment guide and setup instructions.
- A **demo video** (max 5 mins) simulating field deployment.
- A **pitch deck** including:
  - Problem definition
  - System design
  - Cost analysis
  - Impact on rural/public safety

PROBLEM STATEMENTS & CHALLENGES

BONUS POINTS

- Offline sync or mobile alert dashboard
- Local language UI for community usage
- DIY setup models or training resources

COMPETITION PHASES

Phase 1 – Registration Phase (May 9 – June 30, 2025)

- Teams from academic institutions, industries, and research organizations begin registration.
- Institutions (colleges, universities, and companies) will nominate teams through the official hackathon portal.
- Registration details, guidelines, and nomination requirements are available on the event website.

Phase 2 – Shortlisting Phase (July 1 – July 12, 2025)

- After the registration deadline, submitted nomination packages undergo a stringent evaluation process.
- Participants will be shortlisted based on the quality of their proposals, team credentials, and alignment with hackathon objectives.

Phase 3 – Grand Finale (July 25 – July 26, 2025)

- Selected teams will compete in a 36-hour intensive challenge.
- The finale will focus on the creation of a working prototype, detailed presentation of the proof of concept (POC), and a dynamic interactive Q&A session with the panel of expert judges.

Phase 4 – Award Ceremony (July 27, 2025)

- The event will conclude with a formal award ceremony.
- Recognition and awards will be distributed to the top three teams from both Academia and Industry categories.

PARTICIPATION DETAILS

Eligibility & Registration

- **Team Format Only:**
  - Participation is exclusively on a team basis; individual entries are not permitted.
  - Each participating institution (academic or corporate) can nominate teams.

- **Who Can Participate:**
  - Open to teams comprising students, professionals, Ph.D. scholars, and researchers.
  - Institutions such as colleges, universities, and companies are invited to nominate teams.
  - Special emphasis is placed on multidisciplinary teams that can combine technical prowess with practical cybersecurity insights.

- **Registration Process:**
  - Registration must include comprehensive team details, member credentials, and a brief proposal outlining the team's vision.
  - Registrations can only be done through the official website of CCTV Surveillance Security & Forensics Hackathon.

Benefits of Participation

- **Expert Mentorship:**
  - Teams will have access to industry experts who provide guidance throughout the hackathon.

- **Networking Opportunities:**
  - Connect with peers, leading professionals, and law enforcement agencies, facilitating potential future collaborations.

- **Exposure & Recognition:**
  - Opportunity to showcase innovative ideas and secure recognition in both academic and industry circles.

- **Future Collaborations:**
  - Potential for partnerships, internships, or project sponsorships beyond the event.

JUDGING CRITERIA

Each project will be evaluated on several key dimensions to ensure that the winning proposals are both innovative and practical:

Innovation & Creativity:
Assessing originality, inventiveness, and the potential to disrupt traditional approaches. The solution must align well with the competition's theme and directly address the selected problem statement. The idea should demonstrate uniqueness, creativity, or innovation in its approach.

Technical Implementation and Feasibility:
Evaluating the feasibility, scalability, and robustness of the design and prototype. The solution should be practical and realistic to implement in real-world scenarios. It must be technically and economically viable, with resources or infrastructure being reasonably accessible. The potential challenges of implementing the solution should be identified, and appropriate strategies to address them must be outlined effectively.

Technical depth and Illustration of the idea:
The idea must be clearly presented, highlighting its key features, workflows, and functionality through effective use of visual aids such as diagrams, flowcharts, or lifecycle visualizations. Additionally, participants should demonstrate the technical depth of their solution by detailing the coding, technologies, frameworks, or libraries used. Any code samples provided should be well-commented and easy to understand, clearly explaining the purpose and usability of each component.

Impact on Security:
Measuring how effectively the solution enhances surveillance capabilities and fortifies cybersecurity measures.

Presentation & Clarity:
Examining the clarity of the project presentation, the ability to articulate the problem-solving approach, and the overall persuasive power of the demonstration. The PowerPoint presentation should be clear, organized, and comprehensive. It must effectively convey the idea using a balanced mix of visuals, text, and explanations to ensure the audience understands the solution.

JUDGING CRITERIA

AWARDS & RECOGNITION

Awards are distributed in both the Academia and Industry categories with identical prize structures to ensure balanced recognition:

- **First Prize: ₹5,00,000**
- **Second Prize: ₹3,00,000**
- **Third Prize: ₹1,00,000**

Winners will not only receive monetary awards but also gain invaluable industry recognition and potential opportunities for further development and collaboration.