

<http://apisinnovationchallenges.ap.gov.in/#/cybersecurity>



CYBER SECURITY INNOVATION CHALLENGE 2023

Jointly organised by APIS, APTS, NCoE DSCI & VIT AP University



Scan the QR CODE



BACKGROUND

In a world where **cybercrime** continues to escalate at an exponential rate, the need for innovation in cybersecurity has never been more critical. As technology advances, so do the tactics of cybercriminals. We've all felt the vulnerabilities - from Zoom class disruptions to scam emails - and it's evident that our reliance on technology has made cyber security a paramount concern.

Cybersecurity refers to the practice of protecting computer systems, networks, and digital assets from theft, damage, unauthorized access, or other cyber threats. It encompasses a wide range of technologies, processes, and practices designed to safeguard information and ensure the **confidentiality, integrity, and availability of data and systems**.

Cybersecurity is essential in today's digital age, where the volume and sophistication of cyber threats continue to grow. Effective cybersecurity measures are crucial for **protecting individuals, organizations, and governments from cyberattacks, data breaches, and other forms of cybercrime**. Cybersecurity professionals and experts play a vital role in identifying vulnerabilities, implementing safeguards, and responding to security incidents to maintain the security and privacy of digital systems and data.





ABOUT CYBER SECURITY CHALLENGE 2023

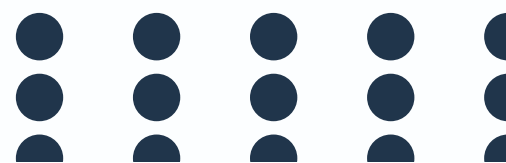
AP Innovation Society (APIS) is proud to join hands with Andhra Pradesh Technology Services (APTS), National Centre of Excellence (NCoE), Data Security Council of India (DSCI), and VIT-AP University to unveil the "Cyber Security Innovation Challenge 2023". This ground-breaking initiative is set to scout for remarkable innovations and startups in the realm of cybersecurity

The goal of this challenge is to bring together stakeholders from the Indian start-up ecosystem, such as entrepreneurs, industrialists, investors, experts, government, and aspiring start-ups, to test, refine, and validate their solutions.

The problem statements are devised in close communication with the State Government Departments and industry partners for the start-ups to showcase their capabilities in these emerging technologies.

Apart from cash incentives of up to INR 30 Lakh distributed among Winners, First Runners and Second Runners. The selected start-ups will also get a chance to get incubation space, mentoring, access to funding schemes & procurement support for prototyping as well as piloting opportunities in the state.

Sounds exciting then let's jump into the problem statements to be addressed!





PROBLEM STATEMENTS

Problem Statement 01:-

Detecting and Mitigating Monitoring and Alteration of Duplicate Websites

Description:

The prevalence of duplicate websites poses a significant threat to user security and privacy. Malicious actors often create duplicate versions of legitimate websites to trick users into disclosing sensitive information or downloading malware. This cyber security challenge aims to assess the effectiveness of monitoring mechanisms and propose innovative solutions to detect and mitigate the risks associated with the monitoring and alteration of duplicate websites.

Expected Outcomes:

- In-depth analysis of duplicate website creation techniques and monitoring mechanisms.
- Development of innovative solutions to detect and mitigate duplicate website risks.
- Successful testing and validation of the developed solutions using a comprehensive dataset.
- Development of an effective AI-based malware detection system for websites.
- Integration strategies for website servers or hosting platforms.
- Real-time monitoring and response mechanisms.
- Comprehensive documentation and reporting on the system's design, implementation, and evaluation.

Problem Statement 02:

Detecting and Mitigating Phishing Emails Luring Users to Pay False Claims

Description:

Phishing emails continue to be a prevalent cyber threat, with attackers using deceptive techniques to trick users into paying false claims or providing sensitive information. This cyber security challenge aims to assess the effectiveness of email security measures and propose innovative solutions to detect and mitigate phishing emails luring users to pay fraudulent amounts.





PROBLEM STATEMENTS

Expected Outcomes:

- In-depth analysis of phishing email techniques and characteristics.
- Development of innovative solutions to detect and mitigate phishing emails luring users to pay false claims.
- Implementation of awareness and education initiatives to enhance user knowledge and vigilance against phishing attacks.


Problem Statement 03:-

Enhancing Cybersecurity for Remote 3D Printing Operations to Prevent Intellectual Property (IP) Theft

Description:

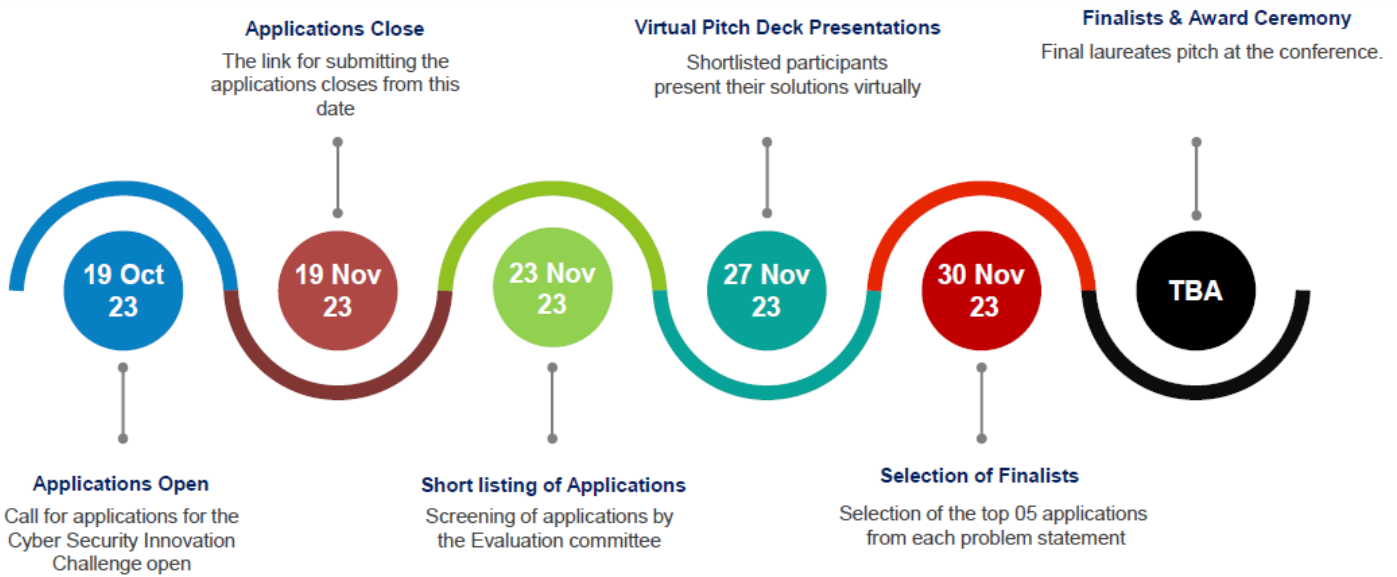
The use of remote 3D printing operations has become increasingly popular, offering convenience and efficiency. However, this convenience also introduces security risks, as attackers may attempt to hack into the communication protocols to steal intellectual property (IP) or disrupt 3D printing processes. This cybersecurity challenge aims to design and implement robust communication protocols for remote 3D printing operations, ensuring the integrity of the commands and preventing IP theft.

Expected Outcomes:

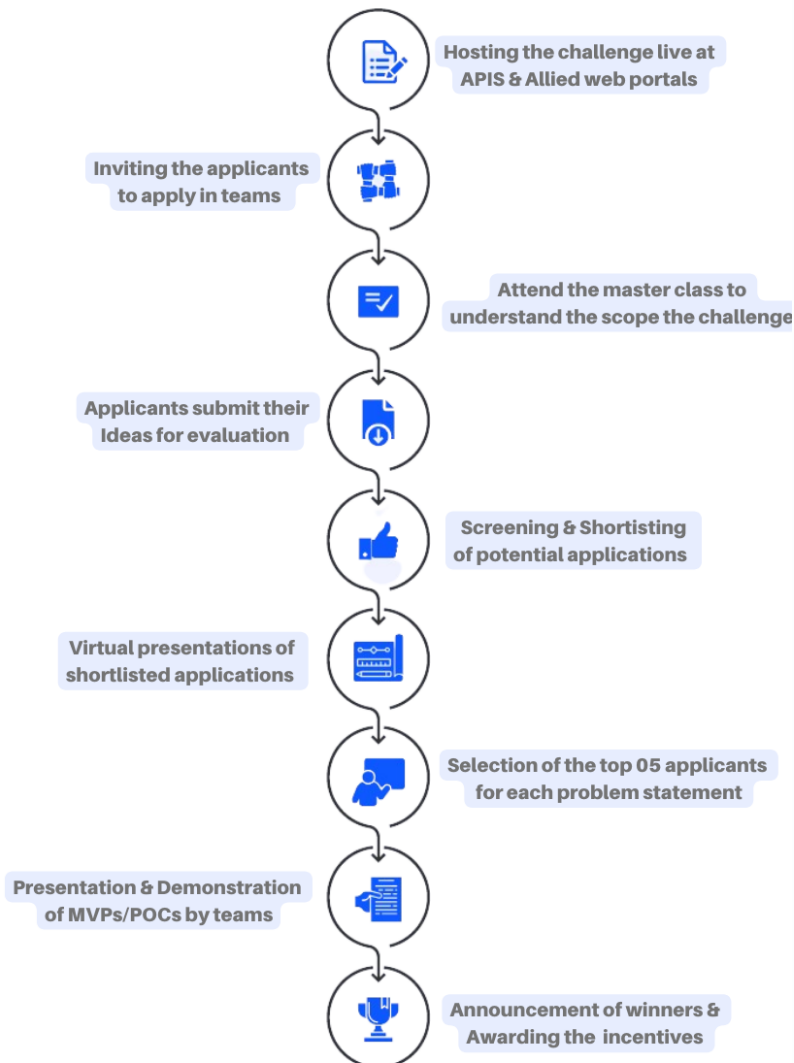
- Secure communication protocols for remote 3D printing operations.
 - Integration of AI for real-time detection and response to anomalous or malicious commands.
 - Effective command validation mechanisms.
 - User authentication and authorization procedures.
 - Comprehensive documentation and reporting.
 - Demonstrated functionality of the system in detecting and responding to security threats.
- 

PROCESSES AND TIMELINES

All the applications received should be strictly adhered to the dead lines and no further entries will be accepted beyond them.



PROCESS FLOW CHART OF CYBERSECURITY INNOVATION CHALLENGE 2023





WHO CAN APPLY


If you are a **start-up, an early stage organization or working in collaboration** to solve problems in the **Cyber Security Space**, you are eligible to apply meeting the following requirements:-

- Demonstrating the existence of a legal structure: Company should comply with the start-up definition as defined by DPIIT at <http://startupindia.gov.in>
- Products/ Services should not violate/ breach/ copy any product already launched and/or copyrighted or patented.
- IPR/ Patent registered for the product(if any) should be owned by the nominating Indian company.
- The product/ Prototype/ MVP submitted should have been designed and developed in India.

Participants will have to come up with solutions that can be called 'innovative', 'radical', 'unconventional' or 'out-of-the-box'. The solutions provided should be thoroughly researched, must not include any sort of plagiarism, carried out as a student effort with a feasible work plan and should be presented with required deliverables

INCENTIVES

The selected start ups will be felicitated with a financial reward of **upto INR 30 Lakh** for creating impact at a scale.

- **Winner - INR 5.00 lakh (Per each problem statement)**
 - **First Runner-up - INR 3.00 lakh (Per each problem statement)**
 - **Second Runner-up - INR 2.00 lakh (Per each problem statement)**
- 



SELECTION CRITERIA

Applicants will be **selected on the basis of the novelty and utility** for any new concept or idea or design or solution to the proposed problem statements. The concept of Innovation should have been proved through a **Model, Prototype, Minimal Viable Product (MVP), Tool and Technology**. The parameters that will be considered in selecting the applications are as follows:

Innovation & Creativity

Higher scores will be given to entries that skip a generation of existing solutions and give **out-of-the-box approaches** to solve the problem.

Relevance & Accuracy


Submission of the solution should have reference to the theme of competition and should provide an innovative, efficient, sustainable and rapid solution to the problem. The submission will receive higher scores if it **addresses big problems with large beneficiaries or cost and/or time savings** in methodology and receive lower scores for just nice-to-have solutions.

Efficiency & Feasibility

The competition doesn't want the participant to just come up with an innovative solution but one that is technically and practically feasible. Lower scoring will be given if the innovation does not appear to be a realistic success. Higher points will be given if the **innovative solutions are cost effective** and try to prove the same with a well-thought-out plan by considering market size, expenditure, socio-political and economic impact.

Communication

Communication plays a vital role to portray ideas and put them to action. A good submission should not only include **a critically-thought, innovative and feasible solution** but should also be effectively demonstrated and communicated.






ETHICS & CODE OF CONDUCT

All participants are required to act in a professional and ethical manner throughout the competition. Failure to act as per the code of conduct can result in disqualification at any stage of the competition. In this regard, any **'means of unfair competition'**, as stated below, will lead to immediate disqualification:

- Any means of plagiarism in the materials and ideas used in the competition
- Failure to provide credit for any sources referred to as aid in the development of solutions
- Any false or malicious statements about other contestants, organizers of the competition, panel of judges or others involved in the competition

PATENTS & INTELLECTUAL PROPERTY RIGHTS

- By submitting an entry to the Innovation Challenge, participants are acknowledging that their ideas/research will be made publicly accessible and shared with industry professionals.
 - The Existing Rights and the Proprietary Rights remain the exclusive property of the Participants who own them. Moreover, the Participants alone shall decide whether or not to protect any know-how of their own and to register or protect or defend any Proprietary Rights or Existing Rights. If required APIS would also support protecting the IPR/ Copyright/ Patent of the innovators based on the expert opinion report from NRDC, Vishakapatnam.
 - However, if the innovator receives a request from the concerned government department, it should be granted to the organizer/ the provider, free of charge, on the deliverables, i.e., within the sole framework of the Challenge.
 - Participants agree not to abuse the rights that may be granted to them by law, any abuse entitling the Organizer to disqualify the participant concerned.
- 

ESTEEMED COMMITTEE MEMBERS

Patron-In-Chief



Sh. Kona Sasidhar IAS

Secretary, ITE&C Department (GOAP)

Honorary Chairman



Sh. Vinayak Godse

CEO, Data Security Council of India

Member Co-Convenor



Sh. M. Ramana Reddy, IRS

MD, APTS

Member Co Convener

Patron



Dr. S. V. Kota Reddy

VC, VIT AP University

Member Convener



Sh. M. Vineet

Director Cyber security Technology NCoE - DSCI



Anil Kumar Tentu

CEO, APIS

KEY PARTNERS

AP Innovation Society:



Andhra Pradesh Innovation Society (APIS) was set up in the year 2015 functioning under the administrative control of the ITE & C Department, the state nodal agency for spearheading the promotion of Innovations, Startups, and Entrepreneurship among first-generation entrepreneurs, researchers, students, citizens, and the government.



APTS:

Andhra Pradesh Technology Services (APTS) is a wholly-owned Government Company incorporated in the year 1986. Under the administrative control of Information Technology, Electronics & Communication Department (ITE&C) Department, APTS is a self sustained company, offering wide-ranging of services including Implementation of IT and Infrastructure Projects, IT Consultancy Services, Information Security Assurance Services & Procurement of Infrastructure for Departments.

NCoE, DSCI:



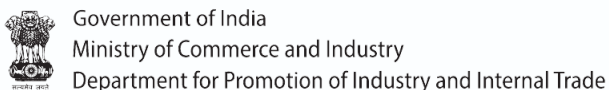
National Centre of Excellence for Cyber Security Technology Development and Product Entrepreneurship, a joint initiative of the Data Security Council of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY), works as a multiplier for cybersecurity research, innovation, and product development.

VIT AP University:



With a history of 37 years of innovation in educational and research domain, VIT has been a forerunner in delivering quality education. Consistently ranked among the top educational institutes in the country, the VIT group of institutions have had a proud tradition of pursuing knowledge and excellence.

ECOSYSTEM PARTNERS





FOR MORE DETAILS

If you have any questions or need advice with any aspect of the **Cyber Security Innovation Challenge 2023**, please contact us

Singamala Sreedhar

Joint Director- Challenges & Hackathons

 jd-startup-apis@ap.gov.in

 +91 9052108526

AP Innovation Society (APIS)

Sunrise Incubation Hub, Hill-3, IT SEZ, Madhurawada, Visakhapatnam - 530048 (AP)