KAVACH 2023 (Cybersecurity Hackathon)

(https://kavach.mic.gov.in)

(National Hackathon)

1. Working toward empowering these imperative notions of our society, MoE's Innovation Cell,**AICTE** along with **Bureau of Police Research and Development (BPR&D)(MHA) and Indian Cybercrime Coordination Centre (I4C)(MHA)** have launched '**KAVACH-2023'** a unique national Hackathon to identify innovative concepts and technology solutions for addressing the security challenges of the 21st century faced by our intelligence agencies.
2. KAVACH-2023 is conceived to challenge India's innovative minds to conceptualize ideas and framework in the domain of **cyber security using artificial intelligence, deep learning, machine learning, automation, big data and cloud computing.**
3. KAVACH-2023 is a unique opportunity for higher institutional Students and Startups in India to submit their innovative ideas/concepts under the different problem statements.
4. This event is going to be conducted in **physical mode in two phase's viz. Initial Phase/Idea screening round and Grand Finale round.**
5. In the Initial round the initially **submitted ideas will be thoroughly screened and scrutinized and the selected ones will be moved for the Grand Finale that will be held in the month of July-2023.**
6. **KAVACH 2023 will have two phases**. The submitted ideas will be evaluated by **a group of experts** in the field and only **the innovative ideas will be selected for the Grand Finale or 2nd round.**
7. During the **Grand Finale,** selected participants are expected to **build the solution to demonstrate their concepts and prove to the juries that their ideas are technically feasible** and more importantly implementable. Best ideas will be declared winners.
8. **During this 36 hours hackathon, scheduled in the month of July-23,** selected youths from education institutions across the country will participate to offer strong, safe and effective technology solutions using their technical expertise and innovative skills.
9. Total **Prize money worth Rs. 20,00,000** is announced for the winning teams.
10. This **hackathon has 20 Problem statements** related to the cyber security domain against which the innovative minds will be able to submit their ideas and compete against each other.

S No.	Task and Activities	Tentative Timeline
1	Launch of Kavach Hackathon	16th Feb 2023
2	Idea Submission	1st March 2023 – 15th April 2023
3	Idea Evaluation	16th April 2023 – 15th May 2023
4	Announcement of Finalist (in Batches)	16th May 2023 – 31st May 2023
5	Training of Finalist	1st June 2023 – 1st July 2023
6	Grand Finale of the Hackathon	12th July 2023 – 14th July 2023

KEC Cyber Security- Hackathon:2023

In order to select the best **10 teams** from Katihar Engineering College, Katihar for **Kavach Hackathon 2023(Cyber Security Hackathon)**. The Department of Computer Science & Engineering of Katihar Engineering College Katihar will conduct an internal Hackathon for all of the branches (CSE/MECH/CIVIL/EEE/FOOD Technologies) to shortlist the best team from KEC, Katihar. The tentative date for KEC Cyber Security Hackathon is **3rd April 2023**.

TEAM FORMATION RULES:

1) All team members should be from KEC, Katihar. However, **members from different branches of the KEC Katihar** are encouraged to form a team.

2) Each team would mandatorily **comprise of 6 members** including the **team leader**.

3) Each team must have **AT LEAST ONE GIRL CANDIDATE**.

4) As this edition of the hackathon is digital product development competition, majority of the team members MUST be well versed with **programming skills.**

5. Last date to submit the Team member names along with the ideas towards the problem statements listed below is 14th March 2023.

6. This hackathon has **20 Problem statements** related to the cyber security domain against which the innovative minds will be able to submit their ideas and compete against each other.

SELECTION CRITERIA:

The selection of 10 best teams would be done by the experts. Each team's performance will be judged and then selected based on the following criteria such as:

1. MCQ Test Round on Cyber Security

2. Oral Question Answer Round(Related to Solution of the problem)

3. Novelty & Accuracy Check

4. Feasibility, Practicability, user experience and potential for future work.

5. Power Point Presentation (Each member of team is required to present PPT slides)

Competent authorities's decisions will be final for shortlisting the team. **Selected best 10 teams from KEC Katihar will be nominated for Kavach Cyber Security Hackathon-2023.**

For more Details Contact to:
Dr. Dharmveer Kr. Yadav
Asst. Prof. (CSE Dept.)

Cybersecurity Hackathon-2023

20- Problem Statement (Choose one of the problem and find solution)

1.No.: KVH-001

PS ID:	KVH-001
Title of PS:	New age women safety app
Domain Bucket:	Mobile App/Women safety
Description:	Design and develop a Women safety app that automatically senses the danger to a mobile user and triggers an SOS alert with location details based on multimodal data from a mobile device such as audio, video, image, motion detection etc., given a situation that the user is not able to operate the mobile.

2. **KVH-002**

S No.:	2
	KVH-002
Title of PS:	Obscenity blocker solution
Domain Bucket:	Obscene Content Detection/ AI
Description:	Design and develop a technological solution for identifying and blocking any obscene media (image/video/audio) at the user's end. The solution should be able to send alerts to the concerned nodal agency in case of the spread of such content. The solution may be in the form of a desktop/mobile application or a web browser plugin.

3. KVH-003

S No.:	3
PS ID:	KVH-003
Title of PS:	Advanced fake news detection system
Domain Bucket:	Fake News/social media
Video URL:	
Description:	Design and develop a technological solution/software tool for Tracking & Tracing Fake News and its origin using official sources as the input

filter. The solution should have a mechanism to mitigate the impact of the spread of Fake News by auto-populating the fake news spreaders' inboxes with the official/authenticated news content.

4. KVH-004

S No.:	4
PS ID:	KVH-004
Title of PS:	Phishing Detection Solution
Domain Bucket:	Phishing Detection/AI
Video URL:	
Description:	Design and develop a technological solution for AI-enabled Phishing Links Detection and Alert System. The solution should be able to identify the source of phishing attacks in web pages, email apps, social media, instant messenger apps, text messages etc. The solution may be in the form of a desktop/mobile application or a web browser plugin.

5. KVH-005

S No.:	5
PS ID:	KVH-005
Title of PS:	Advanced ANPR & FRS solution
Domain Bucket:	Video analytics/CCTV
Video URL:	
Description:	Design and develop a technological solution that can accurately perform the Automatic Number Plate Recognition (ANPR) along with Facial Recognition from the available CCTV feeds. The solution should be able to recognize number plates that are written in typical non-standard ways using varying font styles, sizes, designs, symbols, languages etc., i.e. difficult to recognize by existing ANPR Systems.

6. KVH-006

S No.:	6
PS ID:	KVH-006

Title of PS:	Dark web crawler
Domain Bucket:	Dark web
Video URL:	
Description:	Design and develop an AI-enabled technological solution for actionable Crime Intelligence from the Deep and Dark Web including but not limited to child pornography, weapons, drugs etc. The solution should have the capability to raise demands for additional information from clear-net and proprietary databases viz. TSPs/ISPs for attempting correlation and attribution.

7. KVH-007

S No.:	7
PS ID:	KVH-007
Title of PS:	Spam alert system
Domain Bucket:	Spam Alert/AI
Video URL:	
Description:	Design and develop a crowd-sourcing based solution that can analyse and verify the

	source of any incoming call, SMS and Email based on the inputs from the end-users. The solution should be able to classify, whether the source is genuine or spam. Also, the solution should be able to generate a risk score for incoming calls, SMS and Emails, based on the crowd-sourced input.

8. KVH-008

S No.:	8
PS ID:	KVH-008
Title of PS:	Malware analysis tool
Domain Bucket:	Malware Analysis/Digital Forensics
Video URL:	
Description:	Design and develop a technological solution for the detection and prevention of Fileless Malware (a type of malicious software that uses legitimate programs to infect a computer). The solution may be in the

	form of a desktop or mobile application.

9. KVH-009

S No.:	9
PS ID:	KVH-009
Title of PS:	Advanced CCTV analytics solution
Domain Bucket:	Video Analytics/CCTV
Video URL:	
Description:	Design and develop a technological solution based on live CCTV feeds, that can automatically detect incidents related to street crime, violence, burglary, theft, infiltration, unauthorized access etc. and generate alerts to the nearest Police Station. The solution should also be able to generate a report and maintain a database that includes the nature of incident/crime, location, time, level of alert (i.e., low,

	medium, high risk alert) etc.

10. KVH-010

S No.:	10
PS ID:	KVH-010
Title of PS:	RAM dump collection tool
Domain Bucket:	Digital Forensics
Video URL:	
Description:	Design and develop a technological solution that can collect RAM Dump from any Windows, Linux or Mac based operating system. The solution may be in the form of an Auto-Executable/Lite Version that can be run/executed from any USB storage device without installation at the target computer system.

11. KVH-011

S No.:	11
PS ID:	KVH-011
Title of PS:	Citizen safety app for protection against cyber crimes
Domain Bucket:	Citizen Safety Mobile App
Video URL:	
Description:	Developing an App to flag malicious/ fraud indicators in real-time. a) Mobile Number b) SMS Headers c) URL Links. d) UPI addresses e) Bit coin Wallet Address etc. f) SMS Templates

12. KVH-012

S No.:	12
PS ID:	KVH-012
Title of PS:	Fund trail analysis tool

Domain Bucket:	Financial Data Analysis
Video URL:	
Description:	Fund Trail Analysis Tool (Financial Statements in various Formats- pdf, csv etc).

13. KVH-013

S No.:	13
PS ID:	KVH-013
Title of PS:	Tool for monitoring ground personnel
Domain Bucket:	Asset Tracking
Video URL:	
Description:	Platform/tool to remotely track police officers deployed to bandobast duty using NFC(Near Field Communication)to ensure that they stay where they are posted.

14. KVH-014

S No.:	14
PS ID:	KVH-014
Title of PS:	Chat messenger decryption tool
Domain Bucket:	Cyber Crime Investigation & Forensics
Video URL:	

Description:	Utility to decrypt We Chat, and Ding Talk from cloud / local storage from evidence.

15. KVH-015

S No.:	15
PS ID:	KVH-015
Title of PS:	Mesh network app detection
Domain Bucket:	Cyber Intelligence
Video URL:	
Description:	Design and develop a technological solution for detecting apps like Fire chat that use Mesh Networking to connect users without cell service in a given area. The solution should be man-portable and should be able to scan an area corresponding to a relatable TSP-BTS

16. KVH-016

S No.:	16
PS ID:	KVH-016
Title of PS:	Detecting usage of LoRa

Domain Bucket:	Signal Intelligence
Video URL:	
Description:	Design and develop a technological solution for detecting usage of LoRa (low-power wide-area network modulation derived from chirp spread spectrum) in a given area.

17. KVH-017

S No.:	17
PS ID:	KVH-017
Title of PS:	Hardware forensic suite
Domain Bucket:	Digital Forensics
Video URL:	
Description:	Hardware Forensic Suite- Disk, memory, and Network Traffic (windows, Linux, Mac) with On-Prem and Cloud options.

18. KVH-018

S No.:	18
PS ID:	KVH-018
Title of PS:	Plug & play system security audit tool

Domain Bucket:	Cyber Security Audit
Video URL:	
Description:	Plug and Play System Security Audit Tool for Windows, and Linux. Agent-based with a centralized dashboard.

19. KVH-019

S No.:	19
PS ID:	KVH-019
Title of PS:	Solution for auditing propriety cellular/portable electronic device hardware
Domain Bucket:	Cyber Security Audit
Video URL:	
Description:	Design and develop a technological solution for auditing proprietary cellular/portable electronic device hardware for backdoors and vulnerabilities. The solution should have the capability to audit OEM embedded as well as third-party integrated hardware.

20. KVH-020

S No.:	20
PS ID:	KVH-020
Title of PS:	Indigenous Crypto Currency Investigation Tool
Domain Bucket:	Crypto Analysis
Video URL:	
Description:	Indigenous technological Crypto Currency Investigation Tools with multi-blockchain platform support.