ભક્તકવિ નરસિંહ મહેતા યુનિવર્સિટી, જુનાગઢ

(ગુજરાત પબ્લિક યુનિવર્સિટીઝ અધિનિયમ નં. ૧૫/૨૦૨૩)

સરકારી પોલીટેકનીક કેમ્પસ, ભક્તકવિ નરસિંહ મહેતા યુનિવર્સિટી રોડ, ખડીયા, જુનાગઢ–૩૬૨ ૨૬૩, ગુજરાત(ભારત)

BHAKTA KAVI NARSINH MEHTA UNIVERSITY, JUNAGADH

[Gujarat Public Universities Act No. 15/2023]

Government Polytechnic Campus, Bhakta Kavi Narsinh Mehta University Road, Khadiya, Junagadh-362263 (Gujarat)

Ph: 0285-2681400 || : www.bknmu.edu.in || itcell@bknmu.edu.in

---

Ref. No./BKNMU/IT CELL/042/2026 **Date : 09/06/2026**

વિષય : "Invitation for Students : KANAD S.H.I.E.L.D. Cybersecurity Hackathon 2026" By Cyber Crime Branch, Ahmedabad City Police અંગે વધુમાં વધુ પ્રચાર કરવા બાબત.

સંદર્ભ : Assistant Commissioner of Police, Cyber Cell, Crime Branch, Ahmedabad (Email)

:: પરિપત્ર ::

ઉક્ત વિષય અન્વયે તથા સંદર્ભ E-Mail પત્રથી, ભક્તકવિ નરસિંહ મહેતા યુનિવર્સિટી જૂનાગઢ સંલગ્ન તમામ કોલેજોના આચાર્યશ્રીઓ, માન્ય સંસ્થોના વડાઓ તેમજ યુનિવર્સિટી સ્થિત અનુસ્નાતક ભવનોના અધ્યક્ષશ્રીઓને જણાવવામાં આવે છે કે, Cyber Crime Branch, Ahmedabad City Police દ્વારા નેશનલ લેવલની "**KANAD S.H.I.E.L.D. Cybersecurity Hackathon 2026**" સ્પર્ધાનું આયોજન કરવામાં આવેલ છે. સંદર્ભ પરિપત્રમાં જણાવ્યા મુજબ ભાગ લેનાર વિદ્યાર્થીઓ માટે કુલ "10 Problem Statements" દર્શાવેલ છે, જેના Innovative Solution વિદ્યાર્થીઓ દ્વારા શોધવાના રહેશે. સ્પર્ધામાં ભાગ લેનાર વિદ્યાર્થીઓ માટે રોકડ ઇનામ, સર્ટીફિકેટ, કારકિર્દી વૃદ્ધિ, ટેકનીકલ એક્સપર્ટ સાથે કામ કરવાની તક તથા માર્ગદર્શન, તેમજ આ સ્પર્ધાનો મુખ્ય હેતુ યુનિવર્સીટી સંલગ્ન તમામ વિદ્યાર્થીઓને સાયબર સુરક્ષા અંગેની આ સ્પર્ધામાં ભાગ લેવા તથા આ સ્પર્ધાની માહિતીનો વિસ્તૃત અને વોટ્સએપના માધ્યમથી અસરકારક પ્રચાર કરવા જણાવવામાં આવે છે.

Benefits for Students :

- Grand Cash Prizes : **1st Prize** : ₹1 Lakh | **2nd Prize** : ₹75,000 | **3rd Prize** : ₹25,000
- Certificates : Participating Certificates.
- Opportunities : Networking and career growth prospects with law enforcement and tech experts.

Registration Link : https://forms.gle/g2SDtNunU6DVEFiGA
વધુ માહિતી દર્શાવેલ વેબસાઈટ પરથી મળશે. : www.kanadshield.com

સંપર્ક તથા સપોર્ટ (નોડલ ઓફિસર)

સ્પર્ધા અંગેની કોઇપણ ક્વેરી, માહિતી તથા માર્ગદર્શન અંગે સંપર્ક કરવો

ઓફિસરનું નામ : ડી. જે. જાડેજા (પોલીસ ઇન્સ્પેકટર) | **સંપર્ક નંબર** : 9624251798

સંદર્ભ પત્ર :

- Students_Problem statements_10_Category_2

કુલસચિવ

પ્રતિ,

ભક્તકવિ નરસિંહ મહેતા યુનિવર્સિટી સંલગ્ન (1) તમામ કોલેજોના આચાર્યશ્રીઓ, (2) માન્ય સંસ્થોના વડાઓ, (3) અનુસ્નાતક ભવનોના અધ્યક્ષશ્રીઓ તેમજ (4) વિદ્યાર્થીઓ તરફ...

- નકલ સાદર રવાના :
  1) માનનીય કુલપતિશ્રીના અંગત સચિવશ્રી / માનનીય કુલસચિવશ્રીના અંગત સચિવશ્રી.
  2) આસિસ્ટન્ટ કમિશ્નરશ્રી, સાયબર સેલ, ક્રાઈમ બ્રાંચ, અમદાવાદ.
- વેબસાઈટ પર પ્રસિદ્ધ તથા યોગ્ય કાર્યવાહી અર્થે : આઈ.ટી. સેલ

Office of the Deputy Commissioner of Police,
Cyber Crime Police Station,
Dafnala, Shahibaug, Ahmedabad city, Gujarat, India.
Telephone No. – +91 79 22861917

Outward No.DCP/CYBER CRIME/970/2026
DATE:- 1/06/2026

To
The Director/Principle

Subject: Official Invitation for Students: KANAD S.H.I.E.L.D. Cybersecurity Hackathon 2026 by Cyber Crime Branch, Ahmedabad City Police

Dear Sir / Madam,

Greetings from the Cyber Crime Branch, Ahmedabad City Police, Gujarat

We are proud to introduce the KANAD S.H.I.E.L.D. Cyber Security Hackathon 2026, a visionary initiative by the Cyber Crime Branch, Ahmedabad City Police. The core objective of this hackathon is to strengthen Cyber Space World through the power of advanced technology. We are bringing together the brightest minds from the country's top universities on a single platform to develop cutting-edge solutions for modern cyber threats. This event is more than just a competition; it is a collaborative ecosystem designed to bridge the gap between students, academia, and the police department to build a safer digital future.

We have curated 10 crucial Problem Statements specifically for university students. These problem statements are live and can be viewed under the Category-2 box in the Problem Statements tab on our official website: www.kanadshield.com. We warmly welcome the students of your esteemed university to participate and propose innovative solutions for these 10 problem statements.

Benefits for Students:

By participating in this collaborative ecosystem, your students will get cash prizes, participation certificates, incentives of networking, and career growth opportunities with law enforcement and tech experts.

Contact & Support (Nodal Officer):

For any queries, information, or guidance regarding this event, the following officer has been designated as the point of contact:

Name of the Officer: D.J. Jadeja
Designation: Police Inspector
Contact Number: 9624251798

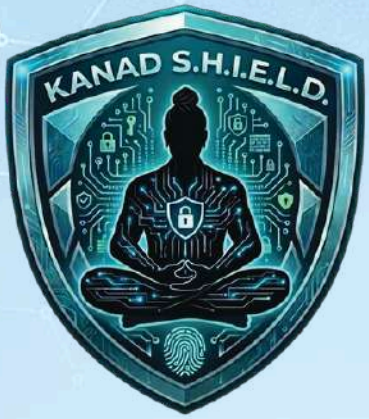
For Detailed Information: www.kanadshield.com
(Registration and more details are given in this mail body)

We highly recommend and request you to take active initiatives to inform, motivate, and invite your students to join this national-level event at the earliest. Let's collaborate to empower the next generation of cyber warriors! We look forward to maximum participation from your university.

Warm regards,

Thanking you,

(Dr. Lavina Sinha, IPS)
Deputy Commissioner of Police
Cyber Crime Branch,
Ahmedabad City



KANAD S.H.I.E.L.D.

2026

Security Hackathon for Intelligence, Encryption, Law enforcement & Defence

Organised by Cyber Crime Branch, Ahmedabad City Police

Intelligence | Encryption | Law Enforcement | Defence

i-Hub (A Gujarat Government Enterprise)

KARNAVATI UNIVERSITY

Problem Statements for KANAD S.H.I.E.L.D. 2026
Category-II

Domain Name	No. of Problem Statements
Cybersecurity & Digital Forensics	2
AI-Driven Smart Policing & Predictive Analytics	2
Legal Intelligence & Automation	2
Health, Welfare & Human-Centric Monitoring	4

Sr. No	Problem Statement ID	Definition	Domain
1	KANADSHIELD26_P2_01	Cyber-Integrated Safety Platform for Women	Health, Welfare & Human-Centric Monitoring
2	KANADSHIELD26_P2_02	Cyber Safety and Protection Platform for Children	Health, Welfare & Human-Centric Monitoring
3	KANADSHIELD26_P2_03	Cyber-Aware Safety and Welfare Platform for Senior Citizens	Health, Welfare & Human-Centric Monitoring
4	KANADSHIELD26_P2_04	Unified Legal & Government Intelligence Platform for Central and Gujarat State	Legal Intelligence & Automation
5	KANADSHIELD26_P2_05	Integrated Health & Wellness Monitoring System for Gujarat Police Personnel	Health, Welfare & Human-Centric Monitoring
6	KANADSHIELD26_P2_06	CrimeGPT – AI-Powered Automation for Crime Documentation and Legal Intelligence	Legal Intelligence & Automation
7	KANADSHIELD26_P2_07	Crime Hotspot Mapping & Predictive Patrol Routing System (Cyber-Integrated)	AI-Driven Smart Policing & Predictive Analytics
8	KANADSHIELD26_P2_08	Network & Packet Forensics Platform (Cyber Crime Investigation System)	Cybersecurity & Digital Forensics
9	KANADSHIELD26_P2_09	Real-Time Data Breach Alert System for Legal & Government Ecosystem	Cybersecurity & Digital Forensics
10	KANADSHIELD26_P2_10	Open-Ended Innovation Platform for Smart Policing (Cyber Crime Branch, Ahmedabad City)	AI-Driven Smart Policing & Predictive Analytics

Sr. No	Problem Statement ID	Definition	Domain
1	KANADSHIELD26_P2_01	Cyber-Integrated Safety Platform for Women	Health, Welfare & Human-Centric Monitoring

Background

With the rapid growth of digital platforms, women face increasing risks not only in physical spaces but also in cyberspace, including cyberstalking, online harassment, deepfake misuse, identity theft, financial fraud, and blackmail. While emergency response systems exist, there is limited integration between cybercrime reporting, digital evidence handling, and real-time police intervention.

The Cyber Crime Branch, Ahmedabad City, requires a unified system that bridges physical safety and cyber safety, enabling rapid reporting, digital evidence capture, and coordinated law enforcement response.

Problem Statement

Design and develop a Unified Cyber-Physical Safety Platform for Women that acts as a Single Point of Contact (SPOC) integrating emergency response, cybercrime reporting, and proactive digital safety mechanisms. The platform should allow women to trigger SOS alerts, report cyber incidents (harassment, stalking, blackmail), and securely upload digital evidence (screenshots, chat logs, URLs) directly to the Cyber Crime Branch and police control rooms.

It must integrate with emergency systems (112), cybercrime portals, and police databases to enable real-time intervention, digital investigation, and legal evidence handling, ensuring both immediate safety and long-term justice.

Key Objectives

- Provide unified cyber + physical safety platform for women
- Enable real-time SOS alerts and cybercrime reporting
- Support secure digital evidence submission
- Integrate with ERSS (112) and cybercrime investigation systems
- Enable AI-based detection of cyber threats (fake profiles, phishing links)
- Provide preventive awareness and alerts
- Ensure privacy and secure handling of sensitive data

Functional Requirements

1. Emergency & Cyber Response System
    a. One-touch SOS alert to police + cyber cell
    b. Cybercrime reporting (stalking, harassment, fraud)
    c. Upload screenshots, links, chat logs
    d. Silent SOS and panic mode

2. Real-Time Tracking & Monitoring
    a. Live location tracking during emergencies
    b. Incident tracking (physical + cyber complaints)
    c. Threat-level monitoring
3. Evidence Collection Module
    a. Secure upload of digital evidence
    b. Tamper-proof storage with timestamps
    c. Chain-of-custody tracking for legal admissibility
4. Cyber Crime Integration
    a. Integration with Cyber Crime Branch systems
    b. Automated FIR/complaint drafting assistance
    c. AI-based phishing and fake profile detection
5. User & Guardian Connectivity
    a. Alerts to trusted contacts
    b. Incident status updates
    c. Emergency communication channels
6. Preventive Cyber Safety Features
    a. Alerts for suspicious links/messages
    b. Awareness modules on cyber safety
    c. Social media risk scanning (optional AI feature)
7. Dashboard & Analytics
    a. Cybercrime dashboard for police
    b. Pattern analysis of online crimes
    c. Repeat offender tracking
8. Data Security & Compliance
    a. Encryption of sensitive media
    b. Privacy-preserving architecture
    c. Legal compliance for digital evidence

Evaluation Criteria

- Effectiveness of police integration and real-time response
- Accuracy of location tracking and alert mechanisms
- Quality and admissibility of digital evidence
- Scalability and performance
- User interface and accessibility
- Innovation in preventive safety features
- Data privacy and security compliance
- Real-world applicability

Suggested Tools/Technologies

- Backend: Node.js / Python (Django/Flask)
- Frontend: React.js / Flutter
- Database: PostgreSQL / MongoDB
- Real-time communication: WebSockets / Firebase
- GIS: Google Maps API / OpenStreetMap

- AI/ML: TensorFlow / PyTorch
- Integration APIs for ERSS / CCTNS (simulated if required)

Bonus Points

- AI-based unsafe zone prediction
- Voice-activated SOS trigger
- Offline/SMS-based alert system
- Multilingual support (Gujarati, Hindi, English)
- Wearable device integration
- Facial recognition for missing persons (optional)

Deliverables

- Working prototype/demo
- Police dashboard demonstration
- Documentation (architecture, workflow, integrations)
- Deployment instructions or containerized setup (optional)

Sr. No	Problem Statement ID	Definition	Domain
2	KANADSHIELD26_P2_02	Cyber Safety and Protection Platform for Children	Health, Welfare & Human-Centric Monitoring

Background

Children are increasingly exposed to online threats such as cyberbullying, online grooming, gaming frauds, exposure to harmful content, and identity exploitation. Traditional safety solutions lack integration with cybercrime monitoring and parental control mechanisms.
The Cyber Crime Branch, Ahmedabad City, aims to establish a child-centric safety ecosystem that combines parental supervision, AI-based threat detection, and direct law enforcement connectivity.

Problem Statement

Design and develop a Child Cyber Safety and Protection Platform that integrates real-time safety monitoring, parental controls, and cybercrime detection into a single unified system. The platform should enable parents and authorities to monitor children's digital and physical safety, detect suspicious online behaviour, and report incidents directly to the Cyber Crime Branch.

It should proactively identify risks such as online predators, cyberbullying, and unsafe content, while enabling quick intervention and evidence collection.

Key Objectives

• Ensure holistic safety (online + offline) for children
• Enable parental monitoring and alerts
• Detect cyber threats using AI
• Integrate with cybercrime reporting systems
• Provide safe digital environment tools
• Enable missing child and emergency alerts

Functional Requirements

1. Emergency & Alert System
    e. SOS button for children
    f. Alerts to parents and police
    g. Missing child reporting integration
2. Real-Time Tracking & Geo-Fencing
    a. Live location tracking
    b. Safe zone / restricted zone alerts
    c. School-to-home journey monitoring
3. Cyber Monitoring Module
    a. Detection of cyberbullying and abusive language
    b. Identification of suspicious contacts (grooming detection)
    c. Monitoring of harmful content exposure

4. Evidence Collection
    a. Capture chat logs and suspicious interactions
    b. Secure evidence storage for police use
5. Cyber Crime Integration
    a. Direct reporting to Cyber Crime Branch
    b. Automated alerts for high-risk activity
    c. Integration with missing child databases
6. Parental Control & Connectivity
    a. Screen time management
    b. App usage monitoring
    c. Parent-child communication alerts
7. Preventive Safety Features
    a. AI-based risk scoring
    b. Educational modules for children
    c. Gaming fraud and scam detection
8. Dashboard & Analytics
    a. Police dashboard for child-related cybercrime
    b. Risk heatmaps
    c. Trend analysis
9. Data Security & Compliance
    a. Child data protection compliance
    b. Encrypted communication
    c. Consent-based monitoring

Evaluation Criteria

- Effectiveness of police integration and real-time response
- Accuracy of location tracking and alert mechanisms
- Quality and admissibility of digital evidence
- Scalability and performance
- User interface and accessibility
- Innovation in preventive safety features
- Data privacy and security compliance
- Real-world applicability

Suggested Tools/Technologies

- Backend: Node.js / Python (Django/Flask)
- Frontend: React.js / Flutter
- Database: PostgreSQL / MongoDB
- Real-time communication: WebSockets / Firebase
- GIS: Google Maps API / OpenStreetMap
- AI/ML: TensorFlow / PyTorch
- Integration APIs for ERSS / CCTNS (simulated if required)

Bonus Points

- AI-based unsafe zone prediction
- Voice-activated SOS trigger
- Offline/SMS-based alert system
- Multilingual support (Gujarati, Hindi, English)
- Wearable device integration
- Facial recognition for missing persons (optional)

Deliverables

- Working prototype/demo
- Police dashboard demonstration
- Documentation (architecture, workflow, integrations)
- Deployment instructions or containerized setup (optional)

Sr. No	Problem Statement ID	Definition	Domain
3	KANADSHIELD26_P2_03	Cyber-Aware Safety and Welfare Platform for Senior Citizens	Health, Welfare & Human-Centric Monitoring

Background

Senior citizens are particularly vulnerable to cyber frauds such as phishing, OTP scams, fake investment schemes, and identity theft, along with physical risks like medical emergencies and isolation.

Existing systems do not adequately combine cyber fraud prevention, emergency response, and welfare monitoring into a unified platform.

The Cyber Crime Branch, Ahmedabad City, seeks a system that ensures digital trust, financial safety, and physical well-being for senior citizens.

Problem Statement

Design and develop a Cyber-Aware Safety and Welfare Platform for Senior Citizens that integrates emergency response, cyber fraud prevention, and continuous welfare monitoring. The platform should allow seniors to report fraud attempts, receive real-time scam alerts, and connect directly with law enforcement and family members. It should also support medical alerts and routine well-being checks.

Key Objectives

- Protect seniors from cyber fraud and scams
- Provide easy-to-use emergency response system
- Enable welfare and health monitoring
- Integrate with Cyber Crime Branch and police
- Offer proactive fraud detection and alerts
- Ensure accessibility and simplicity

Functional Requirements

1. Emergency Response System
    a. One-touch SOS (large, simple UI)
    b. Voice-enabled SOS trigger
    c. Medical emergency alerts
2. Real-Time Monitoring
    a. Location tracking during emergencies
    b. Daily safety check-ins
    c. Inactivity alerts

3. Cyber Fraud Protection Module
    a. Detection of scam calls/messages
    b. Alerts for phishing and fraudulent links
    c. Transaction anomaly alerts (optional integration)
4. Evidence Collection
    a. Record scam calls/messages
    b. Secure upload of fraud evidence
    c. Timestamped logs for investigation
5. Cyber Crime Integration
    a. Direct reporting to Cyber Crime Branch
    b. Fraud case tracking
    c. Integration with banking fraud reporting systems
6. Family & Caregiver Connectivity
    a. Alerts to family members
    b. Shared monitoring dashboard
    c. Emergency contact network
7. Preventive Safety Features
    a. Awareness modules (fraud prevention)
    b. AI-based scam detection
    c. Voice assistant for guidance
8. Welfare Monitoring Module
    a. Scheduled health check reminders
    b. Police-assisted welfare visits
    c. Integration with wearable health devices
9. Dashboard & Analytics
    a. Fraud trend analysis
    b. Senior citizen risk mapping
    c. Response tracking
10. Data Security & Compliance
    a. Simplified secure authentication
    b. Privacy-focused design
    c. Legal compliance for cybercrime evidence

Evaluation Criteria

- Effectiveness of police integration and real-time response
- Accuracy of location tracking and alert mechanisms
- Quality and admissibility of digital evidence
- Scalability and performance
- User interface and accessibility
- Innovation in preventive safety features
- Data privacy and security compliance
- Real-world applicability

Suggested Tools/Technologies

- Backend: Node.js / Python (Django/Flask)
- Frontend: React.js / Flutter
- Database: PostgreSQL / MongoDB
- Real-time communication: WebSockets / Firebase
- GIS: Google Maps API / OpenStreetMap
- AI/ML: TensorFlow / PyTorch
- Integration APIs for ERSS / CCTNS (simulated if required)

Bonus Points

- AI-based unsafe zone prediction
- Voice-activated SOS trigger
- Offline/SMS-based alert system
- Multilingual support (Gujarati, Hindi, English)
- Wearable device integration
- Facial recognition for missing persons (optional)

Deliverables

- Working prototype/demo
- Police dashboard demonstration
- Documentation (architecture, workflow, integrations)
- Deployment instructions or containerized setup (optional)

Sr. No	Problem Statement ID	Definition	Domain
4	KANADSHIELD26_P2_04	Unified Legal & Government Intelligence Platform for Central and Gujarat State	Legal Intelligence & Automation

Background

In India, legal and government-related information such as Government Resolutions (GRs), notifications, circulars, Acts, rules, and court judgments are published across multiple independent platforms maintained by various departments at both Central and State (e.g., Gujarat) levels. These include ministry websites, state GR portals, gazette publications, and judicial platforms.

However, this information ecosystem is highly fragmented, unstructured, and difficult to navigate, especially for citizens, law enforcement agencies, legal professionals, and researchers. Users often need to manually search across multiple portals to gather complete information on a single topic (e.g., pension, land laws, welfare schemes), resulting in inefficiency, lack of awareness, and delayed decision-making.

Existing platforms such as India Code and Indian Kanoon provide partial access to laws and judgments but lack integration with government resolutions, notifications, and department-level circulars. There is currently no single unified system that aggregates and intelligently organizes legal and administrative information across departments and jurisdictions.

Problem Statement

Design and develop a Unified Legal & Government Intelligence Platform that acts as a Single Point of Access (SPA) for retrieving, aggregating, and analysing government resolutions, notifications, laws, circulars, and court judgments from both Central Government and Gujarat State departments.

The platform should allow users to search using keywords (e.g., “pension”) and automatically fetch relevant documents from multiple government and judicial sources. The system must intelligently categorize results (e.g., GRs, Acts, judgments, schemes), provide direct source links, and present structured summaries for ease of understanding.

The solution should incorporate advanced search capabilities, metadata extraction, and AI-based document processing to enable efficient discovery, cross-referencing, and analysis of legal and administrative information. The goal is to build a scalable, user-friendly, and intelligent system that enhances accessibility, transparency, and usability of government and legal data for all stakeholders.

Key Objectives

- Provide a single unified platform for accessing legal and government documents
- Enable keyword-based and intelligent semantic search across multiple sources
- Aggregate data from Central Government and Gujarat State departments
- Automatically categorize documents (GRs, notifications, Acts, judgments, etc.)
- Extract and display relevant metadata (department, date, category)
- Provide AI-based summaries for lengthy documents
- Enable cross-linking of related documents (e.g., GR ↔ Act ↔ Judgment)
- Support multilingual access (English, Hindi, Gujarati)
- Ensure data authenticity by linking to official sources

Functional Requirements

1. Smart Search Engine
    a. Keyword-based search (e.g., pension, land, education)
    b. Semantic/AI-based search for contextual results
    c. Auto-suggestions and query refinement
2. Data Aggregation Module
    a. Fetch data from:
        i. *Government portals (Home department, Central & Gujarat)*
        ii. *Gazette notifications*
        iii. *Judicial* platforms
    b. Support ingestion of:
        i. *PDF documents*
        ii. HTML pages
3. Document Categorization Module
    a. Automatically classify documents into:
        i. *Government Resolutions (GRs)*
        ii. *Notifications / Circulars*
        iii. *Acts / Rules*
        iv. *Court Judgments*
        v. *Schemes*
4. Metadata Extraction Module
    a. Extract:
        i. *Department name*
        ii. *Date of issue*
        iii. *Document type*
        iv. *Keywords / subject*
        v. *Applicable* region
5. Advanced Filtering Module
    a. Filter by:
        i. *Department*
        ii. *Date range*
        iii. *Document type*
        iv. *State /* Central

6. AI-Based Summarization Module
    a. Generate concise summaries of documents
    b. Highlight key provisions, eligibility, and conditions

7. Cross-Linking Engine
    a. Link related documents:
        i. *GRs with amendments*
        ii. *Laws with relevant judgments*
        iii. *Notifications* with parent Acts
8. User Personalization Module
    a. Save searches and bookmarks
    b. Create alerts for new updates
    c. Maintain search history
9. Notification & Alert System
    a. Notify users about:
        i. *New GRs or notifications*
        ii. *Updates* in laws or judgments
10. Dashboard & Analytics Module
    a. Display:
        i. *Trending searches*
        ii. *Frequently accessed documents*
        iii. *Department*-wise data insights
11. Download & Sharing Module
    a. Provide:
        i. *Direct access to original documents*
        ii. *Sharing options*
        iii. *Export of* summaries
12. Security & Compliance
    a. Ensure secure access and data handling
    b. Maintain audit logs
    c. Provide role-based access (user/admin)

Evaluation Criteria

- Accuracy and relevance of search results
- Effectiveness of document categorization and filtering
- Performance and scalability of the system
- Quality of AI-based summarization
- User interface and ease of navigation
- Integration across multiple data sources
- Innovation in cross-linking and legal intelligence
- Real-world usability and impact

Suggested Tools/Technologies

- Backend: Python (Django/Flask) / Node.js
- Frontend: React.js / Angular
- Database: MongoDB / PostgreSQL
- Search Engine: Elasticsearch
- NLP/AI: spaCy, BERT, TensorFlow
- Web Scraping: Scrapy / BeautifulSoup
- APIs for government/judicial data (if available)

Bonus Points

- Voice-based search (multilingual)
- AI chatbot for legal queries
- Offline access for key documents
- Document comparison (old vs new GRs)
- Regional language NLP support
- Integration with other platforms for extended datasets

Deliverables

- Working prototype/demo of the platform
- Documentation (architecture, modules, usage guide)
- Deployment instructions or container setup
- Sample dataset and demonstration of search, categorization, and summarization

Sr. No	Problem Statement ID	Definition	Domain
5	KANADSHIELD26_P2_05	Integrated Health & Wellness Monitoring System for Gujarat Police Personnel	Health, Welfare & Human-Centric Monitoring

Background

Police personnel operate in highly demanding environments involving long duty hours, irregular shifts, high stress, and physically intensive tasks. These conditions often lead to fatigue, stress-related disorders, sleep deprivation, and long-term health issues, which can impact both individual well-being and overall operational efficiency.

While consumer health platforms like Apple Health and wearable-based systems such as WHOOP Strap provide insights into personal health metrics like activity, sleep, and recovery, they are not tailored to the unique operational requirements of police forces.

There is a critical need for a police-specific, integrated health monitoring system that combines physical and mental health tracking, predictive analytics, and supervisory oversight, enabling proactive intervention and improved workforce management.

Problem Statement

Design and develop an Integrated Health & Wellness Monitoring System for police personnel that acts as a centralized platform for tracking, analysing, and improving physical and mental health.

The system should collect data related to activity levels, sleep patterns, stress indicators, and medical records, either through manual input or integration with wearable devices. Based on this data, it should generate a comprehensive health score, identify potential risks such as fatigue, burnout, or health deterioration, and provide personalized recommendations for diet, exercise, and recovery.

The platform must also include a supervisory dashboard for senior police officers, enabling them to monitor unit-level health trends, identify at-risk personnel, and take preventive actions such as duty reassignment or medical intervention. Additionally, the system should allow personnel to upload medical reports (health cards, lab reports, etc.), maintain a secure health history, and support confidential counselling and wellness programs.

The objective is to create a scalable, secure, and intelligent system that enhances well-being, operational readiness, and long-term health outcomes of police personnel.

Key Objectives

- Provide a centralized platform for health monitoring of police personnel
- Track physical activity, sleep, stress, and recovery metrics
- Generate daily/weekly health scores and wellness indices
- Enable early detection of fatigue, stress, and health risks
- Provide AI-based personalized recommendations
- Support medical record management and health history tracking
- Enable supervisory monitoring and intervention by senior officers
- Improve duty allocation based on health conditions
- Ensure data privacy, security, and role-based access control

Functional Requirements

1. Health Monitoring Module
    a. Capture:
        i. Activity levels (steps, movement)
        ii. Sleep duration and quality
        iii. Stress indicators (manual/AI-based)
    b. Integration with wearable devices (optional)
2. Health Score Engine
    a. Generate:
        i. Daily health score
        ii. Weekly wellness index
    b. Categorize:
        i. Fit / Moderate / At Risk
3. Activity & Fitness Tracking
    a. Monitor physical activity levels
    b. Track duty-related exertion
    c. Maintain fitness benchmarks
4. Sleep & Recovery Module
    a. Track sleep duration and patterns
    b. Detect sleep deprivation
    c. Provide recovery scores
5. Stress & Mental Health Monitoring
    a. Self-assessment tools
    b. Behavioural analysis for stress detection
    c. Mood tracking (optional)
6. AI Recommendation Engine
    a. Provide suggestions for:
        i. Diet
        ii. Exercise
        iii. Sleep improvement
    b. Adaptive recommendations based on user behaviour

7. Medical Records Management
    a. Upload and store:
        i. Health cards
        ii. Lab reports
        iii. Medical history
    b. Maintain secure digital health profiles
8. Supervisory Dashboard (Police Integration)
    a. Unit-wise health overview
    b. Identify:
        i. High-risk personnel
        ii. Unfit-for-duty officers
    c. Enable intervention and monitoring
9. Risk Alert System
    a. Generate alerts for:
        i. High stress
        ii. Fatigue
        iii. Health deterioration
    b. Escalation to supervisors/medical units
10. Duty vs Health Correlation Module
    a. Map duty hours with health indicators
    b. Identify high-stress assignments
    c. Support optimized duty allocation
11. Counselling & Wellness Support
    a. Provide access to:
        i. Mental health professionals
        ii. Wellness programs
    b. Optional anonymous support system
12. Notification & Reminder System
    a. Reminders for:
        i. Sleep
        ii. Exercise
        iii. Medical checkups
13. Analytics & Reporting
    a. Individual health trends
    b. Unit-level analytics
    c. Monthly wellness reports
14. Security & Privacy
    a. Role-based access (individual, supervisor, medical officer)
    b. Secure storage of sensitive health data
    c. Audit logs for access and changes

Evaluation Criteria

- Accuracy and reliability of health monitoring
- Effectiveness of risk detection and alerts
- Quality of AI-based recommendations
- Usability and accessibility of the platform

- Performance and scalability
- Innovation in police-specific health features
- Data privacy and security compliance
- Real-world applicability and impact

Suggested Tools/Technologies

- Backend: Node.js / Python (Django/Flask)
- Frontend: Flutter / React Native
- Database: PostgreSQL / MongoDB
- AI/ML: TensorFlow / PyTorch
- APIs for wearable integration
- Cloud: AWS / Azure / GCP

Bonus Points

- AI-based burnout prediction
- Voice-based health input
- Wearable device integration (real-time monitoring)
- Multilingual support (Gujarati, Hindi, English)
- Gamification of fitness scores
- Offline functionality for field personnel

Deliverables

- Working prototype/demo (mobile/web application)
- Supervisory dashboard demonstration
- Documentation (architecture, modules, usage guide)
- Deployment instructions or containerized setup (optional)

Sr. No	Problem Statement ID	Definition	Domain
6	KANADSHIELD26_P2_06	CrimeGPT – AI-Powered Automation for Crime Documentation and Legal Intelligence	Legal Intelligence & Automation

Background

Law enforcement agencies spend a significant amount of time preparing repetitive and detail-heavy documentation throughout the lifecycle of a criminal case. From the moment a victim applies at the police station to the eventual arrest and remand of the accused, various documents such as charge sheets, remand requests, seizure receipts, medical letters, court custody letters, and face identification forms must be created. Much of the content in these documents overlaps, yet officers must manually re-enter and verify the same information across different forms, increasing the risk of errors, omissions, and inefficiencies. Additionally, officers often struggle to immediately determine applicable legal provisions or landmark judgments based on the narrative of the incident, slowing investigation and prosecution.

Problem Statement

Develop a smart AI-driven platform, CrimeGPT, that automates and accelerates the creation of crime-related documentation by eliminating duplication of information and intelligently extracting and mapping legal sections and relevant case laws based on incident narratives. The platform should assist officers from the first victim report to arrest, helping generate all required documents dynamically and maintain a case diary over time.

Key Objectives

- Reduce redundant data entry across legal documents.
- Dynamically generate all required documents for a criminal case using a shared pool of case data.
- Maintain a digital Case Diary from FIR to arrest.
- Recommend relevant legal sections and case laws/judgments based on crime descriptions.
- Ensure document format compliance with Indian criminal procedure standards (BNSS/BNS/BSA).

Functional Requirements

1. Unified Case Data Pool:
    a. Single entry of names, addresses, sections, items seized, statements, etc., used across documents.
    b. Editable and traceable entries.

2. Document Generation Engine:
    a. Automatically generate the following documents:
        i. Purvani Chargesheet
        ii. Medical Treatment Letter
        iii. Remand Request Letter (Police Custody)
        iv. Seizure Receipt
        v. Court Custody Letter
        vi. Accused Panchanama
        vii. Accused Face Identification Form
3. Case Diary Automation:
    a. Maintain a timeline-based case diary from initial complaint to arrest.
    b. Log investigative steps, witness interaction, evidence seizure, etc.
4. Legal Section Intelligence:
    a. NLP-based module to analyse the case summary and suggest:
        i. Relevant sections under BNS, BNSS, BSA
        ii. Applicable landmark judgments
        iii. Cross-referenced IPC/CrPC/Evidence Act provisions where needed.
5. Multilingual Interface:
    a. Input/output support in Gujarati, Hindi, and English.
    b. Search & Audit:
    c. Officers can retrieve old entries/documents using keywords or case numbers.
    d. Version history and audit trail for all document edits.

Evaluation Criteria

- Accuracy of Document Generation: The solution will be evaluated based on how accurately and consistently it generates various crime-related documents using shared input data, minimizing duplication and errors.
- Intelligence in Legal Section Mapping: The platform should effectively analyse incident descriptions and suggest appropriate legal sections under BNS, BNSS, and BSA, along with relevant landmark case laws or judgments.
- User Experience and Interface Design: The usability of the interface, especially for non-technical law enforcement officers, will be assessed, including clarity of workflow, ease of navigation, and multilingual support.
- Integration and Management of Case Diary: The system's ability to maintain a structured and chronological case diary that records all investigative activities from the first report to the arrest will be considered.
- Language Support and Localization: The extent and quality of multilingual input/output support—especially in Gujarati, Hindi, and English—will be reviewed for real-world deployment readiness.
- Completeness and Quality of Deliverables: The overall completeness of the working solution, including documentation, code structure, dataset use, and demo materials, will be evaluated.
- Innovation and Additional Features: Extra credit will be given for innovative or additional features such as offline mode, integration with other systems like BharatPol or CCTNS, face recognition support, or evidence tracking.

Suggested Tools/Technologies

- Frontend: React.js / Angular
- Backend: Node.js / Django / Flask
- Database: PostgreSQL / MongoDB
- NLP & AI: OpenAI GPT, spaCy, BERT (for legal text classification)
- OCR (for scanned documents): Tesseract or Google Vision
- Localization: Google Translate API / Indic NLP Library
- Document Templates: Docx templating (e.g., docxtpl, pdfplumber)
- Legal Dataset: Indian Kanoon, BNS/BNSS/BSA datasets, SCC Online (mocked or public)

Bonus Points

- Integration with Meta/Facebook/Instagram/WhatsApp LERS compliant request templates.
- Offline-first support for low-network police stations.
- Role-based access (IO, SHO, Legal Advisor).
- Evidence image upload and tagging.
- Linkage to CCTNS or BharatPol mock API.

Deliverables

1. A working prototype of CrimeGPT with at least 4 autogenerated documents.
2. A demo showing:
    a. Case creation from FIR to arrest.
    b. Real-time generation of at least two documents.
    c. Legal section and judgment suggestions.
3. Documentation (README, user guide, and code).
4. Dataset used (including anonymized legal texts, FIR samples).

Sr. No	Problem Statement ID	Definition	Domain
7	KANADSHIELD26_P2_07	Crime Hotspot Mapping & Predictive Patrol Routing System (Cyber-Integrated)	AI-Driven Smart Policing & Predictive Analytics

Background

With the rapid increase in both physical and cyber-enabled crimes, law enforcement agencies face challenges in efficiently allocating limited resources and responding proactively to emerging threats. Traditional policing methods rely heavily on reactive responses rather than predictive intelligence.

The Cyber Crime Branch, Ahmedabad City, along with city police units, generates vast amounts of data through FIRs, complaints, cyber reports, surveillance systems, and patrol logs. However, this data often remains underutilized due to lack of integration, advanced analytics, and visualization tools.

A unified GIS-enabled predictive system can transform policing by identifying crime hotspots, forecasting risk zones, and optimizing patrol deployment, thereby enhancing preventive policing and rapid response capabilities.

Problem Statement

Design and develop a GIS-enabled Crime Hotspot Mapping and Predictive Patrol Routing Platform that integrates crime data from multiple sources (FIRs, complaints, cybercrime reports, and patrol logs) to identify high-risk areas and predict future crime-prone zones.

The system should leverage spatial and temporal analytics to generate actionable insights and recommend optimized patrol routes and resource allocation strategies. It must support integration with police databases and cybercrime systems, enabling real-time monitoring, predictive intelligence, and efficient decision-making.

The objective is to create a data-driven, scalable, and intelligent policing platform that enhances situational awareness, improves crime prevention, and optimizes field operations.

Key Objectives

- Identify and visualize crime hotspots using GIS mapping
- Predict future crime-prone areas using AI/ML models
- Integrate cybercrime and physical crime datasets
- Optimize patrol routes and resource deployment
- Enable real-time monitoring and alerts for high-risk zones
- Support data-driven decision-making for police authorities
- Improve response time and preventive policing
- Ensure secure handling of sensitive law enforcement data

Functional Requirements

1. Crime Data Integration System
    a. Integration with FIR databases, complaint systems, and patrol logs
    b. Inclusion of cybercrime data from Cyber Crime Branch
    c. Real-time data ingestion and updates
    d. Data normalization and categorization
2. GIS-Based Crime Mapping
    a. Interactive map displaying crime incidents
    b. Layer-based visualization (crime type, severity, time)
    c. Heatmaps for hotspot identification
    d. Drill-down capabilities (area → street-level insights)
3. Predictive Analytics Module
    a. Temporal analysis (hourly, daily, seasonal trends)
    b. Spatial clustering of crime patterns
    c. AI/ML models for hotspot prediction
    d. Risk scoring for zones based on historical data
4. Patrol Route Optimization
    a. AI-based route generation for patrol units
    b. Dynamic route adjustment based on real-time incidents
    c. Resource allocation recommendations
    d. Integration with GPS-enabled patrol vehicles
5. Cybercrime Intelligence Layer
    a. Mapping of cybercrime origins and affected regions
    b. Detection of digital fraud clusters and phishing hotspots
    c. Correlation between cyber and physical crime patterns
    d. Alerts for emerging cyber threat zones
6. Real-Time Monitoring & Alerts
    a. Live dashboard for ongoing incidents
    b. Alerts for high-risk zones and unusual activity spikes
    c. Incident escalation system
    d. Integration with emergency response systems (e.g., 112)
7. Dashboard & Visualization
    a. Command centre dashboard for police officials
    b. Crime trend graphs and analytics
    c. Predictive heatmaps and risk indicators
    d. Custom reports and data export features
8. Decision Support System
    a. Suggested deployment of patrol units
    b. Scenario simulation (e.g., festival, public events)
    c. Resource planning tools
    d. Performance metrics for patrol efficiency
9. Data Security & Compliance
    a. Role-based access control
    b. Secure handling of sensitive crime data
    c. Audit logs for accountability
    d. Compliance with legal and data protection standards

Evaluation Criteria

- Accuracy of hotspot detection and predictions
- Effectiveness of patrol route optimization
- Integration of cyber and physical crime data
- Performance and scalability of the system
- Usability of GIS dashboard and visualizations
- Innovation in predictive policing techniques
- Data security and compliance

Practical applicability for real-world policing

- Suggested Tools/Technologies
- Backend: Python (Django/Flask) / Node.js
- Frontend: React.js / Angular
- GIS: Google Maps API / OpenStreetMap / Leaflet
- Database: PostgreSQL (PostGIS) / MongoDB
- AI/ML: TensorFlow / PyTorch / Scikit-learn
- Real-time: WebSockets / Kafka
- Data Processing: Apache Spark (optional)

Bonus Points

- AI-based anomaly detection in crime patterns
- Integration with CCTV and surveillance systems
- Predictive alerts before crime spikes
- Mobile app for patrol officers
- Voice-assisted analytics queries
- Integration with smart city infrastructure

Deliverables

- Working prototype/demo with GIS dashboard
- Predictive model demonstration
- Patrol routing simulation
- Documentation (architecture, workflows, models)
- Deployment setup (cloud/containerized preferred)

Sr. No	Problem Statement ID	Definition	Domain
8	KANADSHIELD26_P2_08	Network & Packet Forensics Platform (Cyber Crime Investigation System)	Cybersecurity & Digital Forensics

Background

With the increasing sophistication of cyber threats such as Advanced Persistent Threats (APTs), ransomware, insider attacks, and data exfiltration, malicious activities are often concealed within legitimate network traffic. Traditional security systems struggle to detect such stealthy attacks in real time.

Law enforcement agencies, including the Cyber Crime Branch, Ahmedabad City, require advanced forensic tools capable of deep packet inspection, traffic analysis, and evidence generation to investigate cyber incidents effectively.

A centralized platform for capturing, analysing, and visualizing network traffic can significantly enhance the ability to detect hidden threats, reconstruct attack patterns, and generate legally admissible digital evidence.

Problem Statement

Design and develop a Network & Packet Forensics Platform capable of capturing, storing, and analysing live as well as historical network traffic to detect anomalies such as data exfiltration, covert communication channels, insider threats, and malware activity.

The system should provide deep packet inspection, protocol decoding, signature-based detection, and AI-driven anomaly detection, along with visualization tools for traffic flows and attack patterns. It must support forensic investigation workflows and enable secure export of evidence for legal proceedings.

The objective is to equip the Cyber Crime Branch with a robust, scalable, and intelligent network forensic system for proactive threat detection and post-incident investigation.

Key Objectives

- Capture and analyse live and stored network traffic
- Detect anomalies including APTs, exfiltration, and hidden tunnels
- Provide deep packet inspection and protocol decoding
- Enable signature-based and AI-based threat detection
- Visualize network flows and suspicious activities
- Support forensic investigation and evidence generation
- Integrate with cybercrime investigation systems
- Ensure secure and legally compliant data handling

Functional Requirements

1. Packet Capture & Ingestion System
    a. Capture live network traffic (PCAP format support)
    b. Import and analyse stored packet capture files
    c. High-throughput packet processing
    d. Filtering based on IP, protocol, port, etc.
2. Deep Packet Inspection (DPI)
    a. Protocol decoding (HTTP, HTTPS, DNS, FTP, SMTP, etc.
    b. Payload inspection for hidden data
    c. Detection of encrypted and obfuscated traffic patterns
    d. Session reconstruction
3. Threat Detection Module
    a. Signature-based detection (known attack patterns)
    b. Detection of malware communication and botnets
    c. Identification of data exfiltration attempts
    d. Detection of covert channels and tunnelling (DNS, ICMP, etc.)
4. AI-Based Anomaly Detection
    a. Behavioural analysis of network traffic
    b. Detection of unusual traffic spikes and patterns
    c. Insider threat detection
    d. Identification of zero-day or unknown attacks
5. Traffic Flow Visualization
    a. Graph-based visualization of network communication
    b. Flow diagrams (source → destination mapping)
    c. Timeline-based activity tracking
    d. Highlighting suspicious nodes and connections
6. Forensic Investigation Module
    a. Search and filter historical traffic
    b. Reconstruction of attack scenarios
    c. Timeline correlation of events
    d. Case management for investigators
7. Evidence Collection & Reporting
    a. Export of forensic data (PCAP, logs, reports)
    b. Tamper-proof storage with timestamps
    c. Chain-of-custody tracking
    d. Automated report generation for legal use
8. Integration with Cyber Crime Systems
    a. Integration with Cyber Crime Branch databases
    b. Linking network evidence with reported cases
    c. Support for digital forensic workflows
    d. API-based integration with other investigation tools
9. Dashboard & Analytics
    a. Real-time monitoring dashboard
    b. Alerts for suspicious activities
    c. Traffic statistics and trends
    d. Investigator-friendly UI

10. Data Security & Compliance
    a. Encryption of captured data
    b. Role-based access control
    c. Secure storage and access logs
    d. Compliance with digital evidence standards

Evaluation Criteria

- Accuracy of anomaly and threat detection
- Efficiency of packet capture and processing
- Quality of traffic visualization and insights
- Effectiveness in forensic investigation workflows
- Scalability and system performance
- Data security and legal compliance
- Usability for law enforcement personnel
- Real-world applicability in cybercrime investigations

Suggested Tools/Technologies

- Backend: Python (Django/Flask), Node.js
- Packet Processing: Wireshark libraries, Scapy, Zeek
- Frontend: React.js / Angular
- Database: Elasticsearch / PostgreSQL / MongoDB
- AI/ML: TensorFlow / PyTorch / Scikit-learn
- Streaming: Apache Kafka
- Visualization: D3.js / Kibana

Bonus Points

- Real-time alerting system for active threats
- Integration with SIEM systems
- Encrypted traffic analysis without decryption (metadata-based)
- Automated attack classification
- Multi-language support for reports
- Cloud-based scalable deployment

Deliverables

- Working prototype/demo (live or simulated traffic)
- Packet analysis and visualization dashboard
- Threat detection demonstration
- Forensic report generation sample
- Documentation (architecture, workflows, detection methods)
- Deployment setup (containerized/cloud-ready preferred)

Sr. No	Problem Statement ID	Definition	Domain
9	KANADSHIELD26_P2_09	Real-Time Data Breach Alert System for Legal & Government Ecosystem	Cybersecurity & Digital Forensics

Background

In today's digital governance ecosystem, sensitive data such as citizen records, legal documents, email credentials, and organizational information is increasingly stored and shared across multiple online platforms. With the rise in cyber threats and data leaks, both individuals and government organizations are at constant risk of exposure through data breaches originating from compromised databases, unsecured systems, or malicious actors on the dark web.

Currently, there is no unified system within the legal and government intelligence ecosystem that proactively monitors and alerts users when their sensitive information is exposed. Legal professionals, government officials, and citizens often become aware of breaches only after significant damage has occurred, leading to identity theft, financial loss, or misuse of confidential data. A real-time, intelligent breach detection and alert mechanism integrated into a unified platform can significantly enhance cybersecurity awareness, enable rapid response, and strengthen trust in digital governance systems.

Problem Statement

Design and develop a Real-Time Data Breach Alert System integrated within the Unified Legal & Government Intelligence Platform. The system should continuously monitor multiple data breach sources (including public breach repositories and dark web intelligence feeds) to detect exposure of sensitive user or organizational data. The platform must allow individuals, legal professionals, and government organizations to register identifiers such as email addresses, phone numbers, or domain names for monitoring.

Upon detecting a breach, the system should instantly notify users, provide details of the compromised data, and recommend actionable steps to mitigate risks. The goal is to build a secure, scalable, and intelligent alert system that enhances proactive cybersecurity, minimizes damage from breaches, and promotes data protection awareness across the legal and governance ecosystem.

Key Objectives

- Enable continuous monitoring of data breach sources
- Provide real-time alerts for compromised data
- Support monitoring for individuals and organizations
- Deliver actionable recommendations for risk mitigation
- Ensure secure handling of sensitive user data
- Increase awareness of cybersecurity best practices
- Integrate seamlessly with the unified legal intelligence platform

Functional Requirements

1. Data Breach Monitoring Engine
    a. Continuously scan:
        i. Public breach databases
        ii. Dark web sources (via APIs or threat intelligence feeds)
        iii. Security forums and leak repositories
2. User Registration & Monitoring Module
    a. Allow users to register:
        i. Email addresses
        ii. Phone numbers
        iii. Domains (for organizations)
    b. Enable bulk upload for enterprise users
3. Real-Time Alert System
    a. Notify users via:
        i. Email
        ii. SMS / Push notifications
    b. Include breach details:
        i. Type of data leaked (passwords, emails, financial info)
        ii. Source of breach
        iii. Date and severity
4. Risk Mitigation Recommendation Engine
    a. Suggest actions such as:
        i. Password reset
        ii. Enabling Two-Factor Authentication (2FA)
        iii. Account monitoring or freezing
    b. Provide severity-based guidance
5. Data Privacy & Security Module
    a. Encrypt user data
    b. Ensure anonymized storage where possible
    c. Comply with data protection standards
    d. Prevent misuse of monitored data
6. Organizational Dashboard
    a. Monitor multiple accounts/domains
    b. View breach history and trends
    c. Generate reports on exposure risks
7. Integration with Legal Intelligence Platform
    a. Link breaches with:
        i. Relevant IT laws and regulations
        ii. Government cybersecurity advisories
    b. Provide legal guidance on data protection compliance
8. Analytics & Insights Module
    a. Display:
        i. Number of breaches detected
        ii. Most common data types leaked
        iii. Trends over time

9. Notification & Subscription System
    a. Allow users to:
        i. Subscribe to alerts
        ii. Customize alert frequency
        iii. Track past notifications
10. User Interface & Experience
    a. Simple and intuitive dashboard
    b. Clear alert visualization
    c. Easy on boarding and monitoring setup

Expected Results

1. Timely Notifications
    - Immediate alerts when user data is found in breaches
2. Damage Mitigation
    - Users can take quick actions to secure accounts
3. Increased Awareness
    - Improved understanding of cybersecurity risks and practices
4. Enhanced Security Posture
    - Reduced risk of identity theft and financial fraud
5. Organizational Readiness
    - Businesses and government entities can respond proactively to breaches

Evaluation Criteria

- Accuracy and speed of breach detection
- Effectiveness of real-time alert system
- Security and privacy of user data
- Quality of mitigation recommendations
- Scalability and system performance
- User interface and usability
- Integration with legal/government intelligence platform
- Innovation in threat detection and alerting mechanisms

Suggested Tools/Technologies

- Backend: Python (Django/Flask) / Node.js
- Frontend: React.js / Angular
- Database: MongoDB / PostgreSQL
- APIs: Have I Been Pwned API, threat intelligence feeds
- Web Scraping: Scrapy / BeautifulSoup
- AI/ML: Anomaly detection, NLP for breach analysis
- Messaging: Twilio, Firebase Notifications
- Security: Encryption libraries, OAuth

Bonus Points

- Dark web monitoring enhancements
- AI-based breach severity scoring
- Integration with CERT-In advisories
- Browser extension for real-time alerts
- Automated password strength checker
- Multilingual alert system (English, Hindi, Gujarati)

Deliverables

- Working prototype/demo
- System architecture documentation
- API integration details
- Deployment guide
- Sample dataset and breach detection demonstration

Sr. No	Problem Statement ID	Definition	Domain
10	KANADSHIELD26_P2_10	Open-Ended Innovation Platform for Smart Policing (Cyber Crime Branch, Ahmedabad City)	AI-Driven Smart Policing & Predictive Analytics

Background

With the rapid evolution of technology and the rise in cybercrime, traditional policing methods are increasingly challenged by complex digital threats, high data volumes, and the need for faster, transparent, and citizen-centric services.

Law enforcement agencies such as the Cyber Crime Branch, Ahmedabad City, require innovative, technology-driven solutions that enhance operational efficiency, streamline investigations, improve public engagement, and ensure accountability.

There is a growing need for platforms that leverage AI, data analytics, automation, and digital evidence systems to modernize policing and bridge the gap between citizens and law enforcement.

Problem Statement

Design and develop an Innovative Smart Policing Solution that enhances the efficiency, transparency, and responsiveness of law enforcement operations. The solution can address any critical policing challenge such as AI-driven case management, predictive crime analytics, digital evidence management, cybercrime investigation support, or citizen-police interaction systems.

The platform should demonstrate a clear use case, measurable impact, and seamless integration with existing law enforcement workflows, particularly within the Cyber Crime Branch ecosystem. It should enable smarter decision-making, faster response times, and improved service delivery.

Key Objectives

- Develop an innovative solution addressing a real policing challenge
- Enhance efficiency and reduce manual workload
- Improve transparency and accountability in processes
- Enable faster response and decision-making
- Integrate cybercrime investigation capabilities
- Support data-driven policing using AI/analytics
- Improve citizen engagement and trust
- Ensure scalability and adaptability for real-world deployment

Functional Requirements

1. Core Innovation Module
    a. Unique solution addressing a specific policing problem
    b. Clearly defined use case (e.g., case management, analytics, citizen app)
    c. Configurable workflows based on police processes
    d. Modular and scalable architecture
2. AI & Data Intelligence (if applicable)
    a. Predictive analytics or recommendation engine
    b. AI-based automation (case prioritization, anomaly detection, etc.)
    c. Natural Language Processing for complaint analysis (optional)
    d. Data-driven insights and decision support
3. Cyber Crime Integration
    a. Support for cybercrime reporting or investigation
    b. Integration with Cyber Crime Branch systems
    c. Handling of digital evidence (logs, media, metadata)
    d. Threat intelligence or fraud detection (if applicable)
4. Workflow Automation
    a. Automation of repetitive police tasks
    b. Case tracking and status management
    c. Notifications and escalation mechanisms
    d. Reduced paperwork and manual intervention
5. Citizen Engagement Interface (if applicable)
    a. Mobile/web interface for public interaction
    b. Complaint registration and tracking
    c. Feedback and grievance system
    d. Awareness and alert notifications
6. Dashboard & Analytics
    a. Real-time dashboard for officials
    b. Visualization of key metrics (cases, response time, trends)
    c. Performance monitoring
    d. Customizable reports
7. Evidence Management (if applicable)
    a. Secure upload and storage of digital evidence
    b. Tamper-proof logging and audit trails
    c. Chain-of-custody tracking
    d. Easy retrieval for investigation
8. Integration & Interoperability
    a. Integration with police databases (e.g., FIR systems)
    b. API-based architecture for extensibility
    c. Compatibility with existing tools and platforms
    d. Support for future smart city integrations
9. Data Security & Compliance
    a. End-to-end encryption
    b. Role-based access control
    c. Secure authentication mechanisms
    d. Compliance with legal and data protection standards

Evaluation Criteria

- Level of innovation and originality
- Real-world relevance and problem-solution fit
- Measurable impact on policing efficiency
- Ease of use and adoption by law enforcement
- Scalability and performance
- Integration capability with existing systems
- Data security and compliance
- Quality of implementation and demonstration

Suggested Tools/Technologies

- Backend: Node.js / Python (Django/Flask)
- Frontend: React.js / Flutter
- Database: PostgreSQL / MongoDB
- AI/ML: TensorFlow / PyTorch
- Real-time: WebSockets / Firebase
- Cloud: AWS / Azure / GCP

Bonus Points

- Highly innovative or first-of-its-kind solution
- AI-driven automation with measurable outcomes
- Multilingual support (Gujarati, Hindi, English)
- Mobile-first or field-usable solution
- Integration with IoT / surveillance systems
- Offline capability for low-connectivity areas

Deliverables

- Working prototype/demo
- Clear use-case explanation and impact metrics
- Demonstration of efficiency improvement
- Documentation (architecture, workflow, innovation details)
- Deployment setup (optional, containerized/cloud-ready preferred)

Get In Touch

Phone
+91-9624251798

Mail
support@kanadshield.com

Website
www.kanadshield.com

KANAD S.H.I.E.L.D.

Organised by

i-Hub
(A Gujarat Government Enterprise)

Academic Partner

KARNAVATI UNIVERSITY

NAAC GRADE A+
ACCREDITED UNIVERSITY