Problem statements

Problem Statement 1: Airborne Threat Detection in Surveillance Videos

Introduction:

In modern security and defense operations, timely and accurate detection of airborne threats is crucial. Traditional surveillance methods often rely on manual monitoring, which is inefficient, prone to human error, and struggles with differentiating between harmless objects like birds and potential threats such as drones or missiles.

Our solution aims to revolutionize airborne threat detection using advanced object detection frameworks. By leveraging AI-driven classification and trajectory prediction, we enhance threat identification while minimizing false alarms. This automated approach ensures rapid response and improved security in diverse operational environments, including low-light and night-vision conditions.

Solution Expected:

Our solution provides a cutting-edge airborne threat detection system that integrates advanced AI capabilities to enhance surveillance effectiveness and security.

Objective:

The primary goal of this phase is to train an AI model that can automatically detect and classify airborne objects, such as birds, drones, and missiles, from surveillance video footage. The challenge is to accurately distinguish between real threats (drones/missiles) and non-threatening objects (birds) while ensuring high-speed performance to avoid unnecessary delays in detection.

Key Steps in Round 1:

1️⃣ Training an AI Model on Surveillance Footage

- The AI model will be trained using 30-minute video clips containing instances of birds, drones, and missiles.
- The dataset should include diverse conditions (e.g., different backgrounds, lighting scenarios, object speeds) to improve generalization.

2️⃣ Implementing Object Detection Frameworks

- The model will be trained to detect, classify, and count the airborne objects detected in the surveillance footage.

3️⃣ Prioritizing High-Speed Inference to Reduce False Alarms

- One of the biggest challenges in airborne threat detection is the high rate of false alarms caused by birds.

4️⃣ **Employing Optimized Detection Models for Accuracy**

- Fine-tune the AI model using transfer learning from pre-trained models on object detection tasks.
- Apply data augmentation techniques to improve accuracy in different scenarios (e.g., changing background, lighting variations, motion blur).

Key Steps in Round 2

Round 2: Enhancing Airborne Threat Detection

Objective

Teams will refine their airborne threat detection system by improving accuracy, analytics, and real-time performance. The focus is on enhancing the existing model and making it more effective for real-world deployment.

Key Focus Areas

✅ **1. Improving Model Accuracy**

- **Optimize detection algorithms to reduce false positives (e.g., distinguishing birds from drones).**
- **Fine-tune classification and tracking models for better precision.**

✅ **2. Advanced Threat Analytics**

- **Provide detailed analytics on detection accuracy, accuracy over time, evaluation time, system utilization and more.**

✅ **3. Real-Time Threat Detection**

- **Improve detection speed to minimize delays in identifying airborne threats.**
- **Ensure the system can process live video feeds efficiently.**

Judging Criteria

Criteria	Description
Innovation	**Novelty, creativity, feasibility, and impact of product**
Accuracy	**Improved threat classification and false alarm reduction.**

Efficiency	**Faster evaluation time and real-time detection capabilities.**
Analytics & Insights	**Quality of threat data visualization and reporting.**
Technical Execution	**Integration of model and system responsiveness**

Problem Statement2: UI Component Designer with AI Integration

Introduction:

Designing user interfaces (UI) is a critical aspect of software development, but traditional methods often involve repetitive tasks, limited customization, and lack of collaboration. Developers and designers face challenges in creating responsive, visually appealing, and functional UIs efficiently. To address these issues, we introduce an innovative UI Component Designer Platform that leverages AI to revolutionize the way UIs are designed, customized, and deployed.

Solution Expected:

Our platform is a web or desktop-based tool that enables users to create, customize, and preview user interfaces through an intuitive drag-and-drop interface. With AI-powered suggestions, the platform ensures efficiency and collaboration. It caters to designers, developers, and businesses seeking to streamline UI development while maintaining high-quality standards.

Unique Selling Points and Features:

Round 1: Core Features

Drag-and-Drop UI Editor:

- Users can add, arrange, and resize elements like buttons, text fields, images, and forms.
- Components support basic styling options (e.g., color, font size, borders) and advanced customization.

Real-Time Preview Mode:

- Instantly preview and interact with the designed interface within the platform.
- Ensure all component functionalities work as intended in the preview.

AI-Powered Design Suggestions:

- AI analyzes user designs and suggests improvements for layout, color schemes, and accessibility.
- Automatically generate responsive designs for different screen sizes (desktop, tablet, mobile).

Component Library:

- A library of pre-made components (e.g., modals, navigation bars, input forms) that users can drag into their designs.
- Allow users to customize or extend these components.

Round 2: UI Component designer

Objective

Teams will develop an **AI-powered UI design platform** with real-time collaboration, automated code generation, and project management capabilities. The focus is on **building a functional, marketable product** with innovative enhancements.

Key Focus Areas

✅ 1. AI-Powered Code Generation

- **Automatically generate code** based on user's design
- Allow user to preview the built website and export the code
- Bonus: Generate a shareable link to the web page

✅ 2. Design language

- Allow user to define a custom UI design theme for their project
- All generated components should follow the given theme

✅ 3. Project Management System

- Allow users to **save, load, and edit UI projects** efficiently.
- Implement **version control** for tracking and reverting changes.

Judging Criteria

Criteria	Description
Innovation	Novelty, creativity, and scalability of the implemented features.
Functionality	Seamless collaboration, code generation, and project management.
Automation	Effectiveness and accuracy of generative AI.
User Experience	Intuitive UI and workflow efficiency.

Technical Execution	Stability, responsiveness, and real-time performance.

.

ps3:Enhancing Clinical Decision Support Systems with Retrieval-Augmented Generation (RAG) Model

Problem Statement:

Healthcare professionals often struggle to access accurate, real-time, and relevant medical information for critical decision-making. Traditional Clinical Decision Support Systems (CDSS) rely on static databases and predefined rules, limiting their adaptability to evolving medical research and treatment protocols. Key challenges include:

- Difficulty in retrieving patient-specific insights from vast structured and unstructured medical data.
- Lack of real-time integration with the latest research papers, guidelines, and case studies.
- Cognitive overload due to excessive medical literature.
- Inconsistent accuracy in diagnosis recommendations, leading to medical inefficiencies.

Solution Expected:

Our system leverages Retrieval-Augmented Generation (RAG) to combine retrieval models for fetching relevant medical information with generative AI for context-aware clinical recommendations. This system will:

- Retrieve up-to-date research papers, clinical guidelines, and case studies.
- Integrate structured EHR data with retrieved insights for patient-specific recommendations.
- Provide real-time, evidence-based suggestions to healthcare professionals.
- Improve diagnostic accuracy while reducing cognitive load.

Unique Selling Points and Features:

Round 1: Core Features

Data Collection & Processing:

- Extract structured patient data from Electronic Health Records (EHRs).
- Scrape and preprocess unstructured data from medical research repositories (PubMed, WHO, FDA).
- Store and retrieve data efficiently using vector databases.

AI-Powered Clinical Decision Support:

- Fine-tuned retrieval models to fetch relevant medical information.
- Generative AI (e.g., GPT-4) to contextualize and summarize retrieved data.
- Named Entity Recognition (NER) to extract medical conditions, drugs, and treatment suggestions.

Round 2: Enhancing Clinical Decision Support Systems with Retrieval-Augmented Generation (RAG) Model

✅ 1. Clinical Decision Transparency & Explainability

- Display **why** a diagnosis or treatment was suggested.
- Show supporting **research papers, case studies, and medical guidelines** linked to the recommendation.
- Provide **confidence scores** for AI-generated insights to improve trust.

✅ 2. Risk Assessment & Alert System

- Implement a **risk scoring mechanism** based on medical history.
- Display **color-coded risk levels** for different conditions.
- Generate **real-time alerts** for high-risk diagnoses requiring urgent attention.

✅ 3. Smart Medical Knowledge Retrieval

- Allow doctors to **search for case studies, research papers, and treatment guidelines** using natural language queries.
- Implement **keyword filtering** to refine search results.

Criteria	Description
Innovation	Novelty, real-world applicability, and market readiness of the solution.
Clinical Decision Transparency	Clarity and explainability of AI-generated insights, confidence scores, and supporting references.
Risk Assessment & Alerts	Effectiveness of risk scoring, accuracy of alerts, and usability of the alert system.
Smart Medical Knowledge Retrieval	Accuracy and relevance of retrieved medical knowledge, efficiency of search and filtering.

Technical Execution & User Experience	Seamless integration, UI/UX quality, responsiveness, and overall system performance.

Problem statement 4: Deepfake & Social Engineering Attack Detector

Introduction:

Deepfake technology is increasingly being exploited for social engineering attacks such as voice phishing, business email compromise (BEC), and fake video authentication. These threats pose significant risks to individuals and organizations, making it crucial to develop an AI-powered fraud detection system to identify and prevent deepfake-based attacks effectively.

Solution Expected:

Our platform is a browser/desktop extension that scans and detects deepfake content in real-time across various communication channels, including video calls, emails, and social media. By leveraging AI-driven media analysis, the system ensures accurate detection and provides users with actionable insights to mitigate security risks.

Unique Selling Points and Features:

Round 1: Core Features

Client-Side Detection:

- Monitor and analyze audio/video calls on platforms like Zoom, Teams, and WhatsApp.
- Scan emails for impersonation attempts and phishing attacks.
- Detect fake profiles and fraudulent messages on social media.

AI-Powered Media Analysis:

- Facial Landmarks & Lip Sync Analysis to identify video tampering.
- Voice Biometrics & MFCC Analysis to detect synthetic speech.
- NLP-based Linguistic Analysis to recognize phishing patterns in emails.

Round 2: Deepfake & Social Engineering Attack Detector

✅ **1. Deepfake Detection Accuracy & Performance**

- Optimize AI models for **low-latency deepfake detection** to ensure real-time scanning.
- Reduce **false positives** while maintaining high detection precision.

✅ **2. Real-Time User Alerts & Confidence Scoring**

- Implement a **security dashboard** displaying **confidence scores** for detected deepfakes.
- Provide **actionable alerts** with recommendations to mitigate risks.

✅ **3. Integration & Usability**

- Ensure smooth integration into **browsers plugins, messaging apps, and video call platforms**.
- Focus on **seamless user experience** with minimal system performance impact.

Scoring Criteria

Criteria	Description
Innovation	Novelty, real-world applicability, and market readiness of the solution.
Detection Accuracy & Performance	Effectiveness of AI models in detecting deepfake media with minimal false positives.
Real-Time Alerts & Explainability	Clarity of security alerts, confidence scoring, and user guidance on mitigating threats.
Integration & Usability	Ease of implementation in real-world communication platforms.
Technical Execution & Efficiency	Optimization, speed, and reliability of deepfake detection.

Problem statement 5: Ransomware Early Detection & Response System

Introduction:

Ransomware is one of the most damaging cyber threats, leading to encrypted files and financial extortion. Traditional security measures often fail to detect ransomware attacks before encryption completes, making early detection crucial. This project aims to build an AI-driven ransomware detection and prevention system that identifies attacks in real-time and mitigates their impact.

Solution Expected:

Our system is a real-time monitoring agent designed to detect and respond to ransomware threats before they cause significant damage. By analyzing file and process behavior, it provides proactive alerts and automated responses to neutralize potential attacks before encryption completes.

Unique Selling Points and Features:

Round 1: Core Features

Client-Side Monitoring:

- Detect unusual file encryption patterns and mass renaming/deletion of files.
- Monitor unauthorized process execution, including PowerShell, cmd, and wmic abuse.
- Analyze system behavior to detect potential ransomware activity in real-time.

AI-Powered Threat Detection:

- Identify file entropy changes, which indicate ransomware modifying file structures.
- Track process API calls related to cryptographic operations and shadow copy deletion.
- Detect registry modifications commonly associated with ransomware attacks.

Round 2: Advanced Features

Behavior-Based ML Threat Classification:

- LSTMs/Transformers to detect long-term behavioral anomalies in system activity.
- Isolation Forests & One-Class SVM to identify deviations from normal process behavior.

Database & Machine Learning:

- Maintain a database of known ransomware families and Indicators of Compromise (IOC) from security firms like VirusTotal and AnyRun.

- Utilize ensemble models combining signature-based and anomaly detection techniques.
- Train deep learning models to recognize encryption patterns using RNNs and LSTMs.

Automated Response System:

- Provide real-time alerts when ransomware activity is detected.
- Automatically kill malicious processes, block network access, and quarantine infected files.
- Display risk scores and recommended mitigation strategies for affected users.

Scoring Criteria

Criteria	Description
Innovation	**Novelty, real-world applicability, and scalability of the solution.**
Detection Accuracy & Performance	**Effectiveness in identifying ransomware attacks with minimal false positives.**
Automated Response & Risk Scoring	**Speed and efficiency in stopping ransomware and preventing damage.**
Integration & System Impact	**Compatibility with real-world IT environments without high system overhead.**
Technical Execution & Efficiency	**Optimization, reliability, and practical implementation of security mechanisms.**

Problem statement 6: OSINT-Based Dark Web Threat Intelligence Platform

Introduction:

Organizations struggle to monitor leaked credentials, vulnerabilities, and cyberattack planning on the dark web. Traditional security measures fail to track hidden threats in underground forums and encrypted networks. This project focuses on building an OSINT-based intelligence tool that crawls hacker forums, TOR websites, and data leak dumps to provide actionable threat intelligence.

Solution Expected:

Our system is a web-based intelligence platform that continuously monitors and analyzes dark web activities. By leveraging advanced NLP and graph-based analytics, it detects leaked credentials, cyberattack discussions, and emerging threats in real-time, helping security teams stay ahead of potential risks.

Unique Selling Points and Features:

Round 1: Core Features

Dark Web Crawling & Data Collection:

- Scrape and analyze TOR-based hacker forums, breach databases, and underground marketplaces.
- Monitor paste sites for leaked credentials and stolen data.
- Track cybercrime discussions in real-time to detect emerging threats.

AI-Powered Threat Intelligence:

- Named Entity Recognition (NER) to extract sensitive information such as usernames, passwords, and emails.
- BERT-based Topic Modeling to classify discussions into categories like hacking, exploits, and scams.
- Sentiment Analysis on hacker conversations to detect planned cyberattacks.

Round 2: Advanced Features

Graph-Based Threat Actor Analysis:

- Utilize Graph Neural Networks (GNNs) to map relationships between threat actors.
- Identify key influencers and their roles in cybercrime networks.
- Detect connections between multiple data breaches and emerging attack trends.

Database & Machine Learning:

- Maintain a historical database of leaked credentials and hacker activities.
- Use transformer-based NLP models like BERT and RoBERTa for advanced text classification.

- Implement anomaly detection to identify new and evolving cyber threats.

Automated Risk Scoring & Alerts:

- Assign risk scores to detected threats based on their impact level.
- Provide real-time alerts to security teams for immediate response.
- Integrate with security platforms for automated incident response and threat mitigation.

Expectation:

By implementing this OSINT-based Dark Web Threat Intelligence Platform, organizations can proactively detect and respond to cyber threats before they escalate. This system provides deep insights into hacker activities, helping security teams prevent data breaches, financial fraud, and cyberattacks.

Conclusion:

In conclusion, our AI-powered dark web monitoring system revolutionizes cybersecurity by delivering real-time intelligence and risk analysis. By combining NLP, machine learning, and OSINT techniques, we empower organizations to safeguard their assets from hidden cyber threats effectively.

Problem Statement 7: Blood Donation & Emergency Help

Introduction:

During medical emergencies, finding a compatible blood donor or receiving immediate assistance can be a life-or-death situation. Many patients struggle to access blood due to shortages, delays, or reliance on middlemen. This platform aims to directly connect blood donors with recipients based on location, ensuring timely donations and emergency support without unnecessary delays.

Solution Expected:

Our platform is a mobile and web-based application that facilitates real-time blood donation matching and emergency assistance. By leveraging location-based services, donor availability tracking, and real-time notifications, the system ensures rapid response times, directly linking donors, recipients, and emergency responders.

Unique Selling Points and Features:

Round 1: Core Features

1. Blood Request System:

- Users can request blood by specifying blood type, urgency level, and hospital location.
- Requests are broadcasted to nearby potential donors, increasing response rates.
- A request tracking system allows real-time monitoring of request status.

2. Location-Based Donor Matching:

- The system finds and notifies nearby registered donors matching the required blood type.
- Donors can accept or decline requests based on availability.
- Prioritization of closest available donors ensures minimal travel time.

3. Emergency SOS Alerts:

- An SOS button allows users to instantly notify nearby volunteers, emergency contacts, or responders.
- Alerts include live location and details about the emergency.
- Responders can accept SOS requests and provide assistance.

4. Blood Bank Inventory Integration:

- Integration with hospitals and blood banks provides real-time blood stock availability.
- If no direct donors are available, users can check nearby blood banks for required blood types.

5. Donor Availability Status:

- Donors can update their status (Available/Unavailable) at any time.
- Only active donors receive urgent blood requests, reducing unnecessary notifications.

Round 2: Advanced Features

1. Live Donor Tracking:

- Allow Recipient and donor to track live location via maps api and sockets
- Helps recipients plan their arrival at the hospital or donation center.

2. AI-Based Urgency Prioritization:

- Requests are ranked based on blood type rarity, distance, and urgency.
- The system prioritizes critical cases to ensure faster response times.
- Develop an unbiased algorithm to assign priority to critical cases.

3. Emergency Medical Response Integration:

- Direct connection with hospitals, ambulance services, and first responders.
- Users can request medical assistance or ambulance services during emergencies.

Problem Statement 8: Direct Farmer-to-Consumer Marketplace

Introduction: Farmers often struggle to get fair prices for their produce due to middlemen who take a large share of the profit. This platform aims to eliminate intermediaries by enabling direct connections between farmers, consumers, and retailers. Through a user-friendly mobile application, farmers can list their produce, negotiate prices, manage orders, and receive payments seamlessly. The platform should ensure transparency, real-time communication, and accessibility to a larger customer base, helping farmers increase their income while ensuring fresh produce reaches buyers at reasonable prices.

Solution Expected: Our platform is a mobile and web-based application that enables farmers to directly connect with consumers and retailers. By integrating location-based buyer matching, direct messaging, and an intuitive order management system, the platform ensures efficiency and fairness in agricultural trade.

Unique Selling Points and Features:

Round 1: Core Features

1. Farmer Profile & Product Listings

- Farmers can create profiles and list available produce, including details such as price per unit, available quantity, and expected harvest date.
- Image uploads and descriptions help attract buyers.
- An easy-to-use interface allows farmers to update stock availability in real-time.

2. Location-Based Buyer Matching

- The system suggests nearby buyers or retailers based on the farmer's location.
- Buyers searching for specific produce see a list of farmers offering it within their preferred radius.
- Reduces transportation costs and ensures fresher products reach consumers.

3. Direct Messaging for Negotiation

- In-app messaging system enables buyers and farmers to discuss pricing, quantity, and delivery preferences.
- Supports text and voice messages for inclusivity.
- Pre-set message options simplify negotiations.

4. Order Placement & Confirmation

- Buyers can browse, place orders, and specify quantities.

- Farmers receive notifications and can accept or reject orders.
- Order tracking system updates users on status changes (pending, confirmed, dispatched, delivered).

Round 2: Advanced Features

AI-Driven Dynamic Pricing & Demand Forecasting

- Display detailed reports to farmers on seasonality, weather patterns, and historical sales data customised to the farmer.
- Dynamically suggests optimal pricing for farmers, maximizing profits while maintaining competitive rates for buyers.
- Provides alerts on peak demand periods, helping farmers plan their harvest and sales strategy efficiently.

Scoring Criteria for Direct Farmer-to-Consumer Marketplace

Criteria	Description
Innovation & Feasibility	Novelty, creativity and practicality of the solution in real-world agricultural trade.
Market Impact & Fair Pricing	Effectiveness in eliminating middlemen, ensuring fair prices for farmers and affordability for consumers.
AI & Technology Implementation	Quality of AI generated reports like dynamic pricing and demand forecasting
Usability & Adoption Readiness	Ease of use for farmers with limited technical knowledge and scalability for widespread adoption.
User Interface	Clean and attractive UI/UX

Problem statement: 9 DecentralGig: Blockchain-Powered Freelance Marketplace

Introduction:

The freelance marketplace has evolved significantly, yet centralized platforms like Fiverr impose high fees, enforce strict policies, and control user data, limiting the freedom and financial benefits of freelancers. Additionally, disputes are often resolved unfairly, and users have limited transparency in payment processing. To address these challenges, we propose a decentralized freelance marketplace, leveraging blockchain technology to ensure transparency, reduce fees, and provide users with true ownership over their work and payments.

Solution Expected:
Our platform is a Web3-based decentralized freelance marketplace where freelancers can list services, and clients can hire them using smart contracts. Payments are securely held in escrow and automatically released upon task completion. Dispute resolution is managed through a Decentralized Autonomous Organization (DAO), ensuring fairness. Additionally, decentralized identities (DIDs) and reputation systems prevent fraud while maintaining user privacy.

Unique Selling Points and Features:
Round 1: Core Features
Smart Contract-Based Payments:

Clients deposit funds into a smart contract escrow.
Payment is released automatically upon task completion.
Supports milestone-based payments.
Decentralized Identity & Reputation System:

User profiles are stored on a blockchain to prevent manipulation.
Reputation is built over time and remains verifiable.
Zero-Knowledge Proofs (ZKPs) enable work verification without revealing personal details.
Dispute Resolution via DAO Arbitration:

Users can stake tokens to become arbitrators.
Arbitrators vote on disputes and earn rewards for fair decisions.
Reduces biased and inefficient dispute handling.

Round 2: Advanced Features
P2P Communication & Privacy Protection:

Secure peer-to-peer messaging for freelancer-client discussions.
Job listings stored on IPFS/Arweave for decentralization.
Cross-Chain Payments & Fiat On-Ramps:

Supports Ethereum, Polygon, Solana, and other chains.
Enables easy fiat-to-crypto conversion for onboarding new users.
Minimal Fees & Governance:

No high commission cuts—only minimal protocol fees.
Community governance through DAO voting to propose and implement changes.

Expectation:

We anticipate that our decentralized freelance marketplace will revolutionize the gig economy by eliminating intermediaries, reducing costs, and increasing transparency. By leveraging blockchain technology, freelancers and clients can transact with greater security, privacy, and fairness. The integration of smart contracts, DID, and DAO arbitration ensures a trustless and self-sustaining ecosystem where users have full control over their work and earnings.

Conclusion:

In conclusion, our decentralized freelance marketplace represents a paradigm shift in how freelancing platforms operate. By leveraging Web3 technology, we empower freelancers and clients with a fair, low-cost, and censorship-resistant platform. This initiative aims to set a new standard for freelancing, ensuring that talent and hard work are rewarded without interference from centralized authorities.

Problem Statement10: Identification of Personally Identifiable Information (PII) in Documents and Data

Introduction: In today's digital age, numerous services require users to upload government-issued documents or provide personal data for verification and processing. These documents, such as Aadhaar card, PAN card, driving license, and credit card details, contain personally identifiable information (PII) that can uniquely identify an individual. The inadvertent or intentional exposure of PII poses significant risks, including identity theft, financial fraud, and privacy breaches. Organizations handling such documents must ensure secure data management practices, including storage, encryption, access control, and compliance with data protection regulations.

Solution Expected: A software application or library package that detects and alerts users when PII from government-issued identification documents is embedded in uploaded documents or provided data. The application will help organizations verify the necessity of retaining such PII, enabling them to redact, mask, or remove it when not required. Additionally, it will notify users of potential privacy risks before submitting sensitive information.

Unique Selling Points and Features:

Round 1: Core Features

1. PII Detection in Uploaded Documents

- Automatically scans uploaded documents for Aadhaar, PAN, driving licenses, and other PII-related data.
- Uses OCR and machine learning models to identify sensitive information.
- Provides a risk assessment score for detected PII content.

2. Real-Time User Alerts

- Notifies users before submitting documents containing PII.
- Displays recommendations on whether to proceed with uploading or redact sensitive details.
- Ensures users make informed decisions regarding data privacy.

3. Data Redaction and Masking

- Allows organizations to remove or blur sensitive data from documents.
- Ensures compliance with privacy laws by limiting exposure of unnecessary PII.
- Supports multiple document formats, including PDF, JPEG, and PNG.

4. Compliance and Audit Logs

- Maintains logs of PII detection events for auditing purposes.
- Helps organizations track compliance with data protection regulations.
- Provides an admin dashboard for reviewing past detections.

(Bonus)

5. User Consent & Policy Enforcement

- Ensures users acknowledge data privacy policies before uploading sensitive documents.
- Helps organizations enforce best practices for PII handling.
- Reduces the risk of unauthorized data exposure.

6. Multi-Language OCR Support

- Detects and processes PII across different languages.
- Expands accessibility for diverse user demographics.
- Supports regional government-issued documents.

7. Secure API Integration

- Allows businesses to integrate PII detection into their platforms.
- Provides a secure API for automated scanning and alerting.
- Enables seamless adoption across various digital services.

Round 2: Advanced Features

1. AI-Driven PII Classification

- Categorizes PII types (e.g., financial, identity, contact information).
- Helps organizations implement customized redaction strategies.
- Improves detection accuracy over time through AI training.

2. Batch Document Processing

- Supports bulk scanning of documents for large enterprises.
- Enhances efficiency for compliance checks and risk mitigation.
- Enables organizations to assess PII risks at scale.

3. PII Removal Recommendations

- Suggests best practices for anonymization based on context.
- Guides users on when and how to redact unnecessary details.
- Enhances data security without compromising service functionality.

Scoring Criteria

Criteria	Description
Innovation	Novelty, creativity and feasibility of the product

Accuracy & AI Performance	Effectiveness of AI models in detecting and classifying PII with minimal false positives/negatives.
Scalability & Efficiency	Ability to process large volumes of documents efficiently (e.g., batch processing). Higher scores for optimized performance with minimal latency.
Usability & Integration	Ease of integration via APIs, user-friendly interface, and seamless redaction tools. Higher scores for smooth enterprise adoption.
Impact & Customization	Effectiveness in providing actionable PII removal recommendations. Higher scores for solutions offering adaptive redaction and contextual risk assessments.

Problem Statement11: Humanitarian Crisis Relief and Support App

Introduction: In an increasingly interconnected world, humanitarian crises—such as natural disasters, conflicts, and pandemics—demand swift action and support. However, challenges like misinformation, lack of transparency in donations, and difficulties in mobilizing resources hinder relief efforts. This mobile application aims to address these issues by providing real-time crisis updates, secure and transparent donation processing, and awareness campaigns to educate and engage users. By ensuring accountability and security, the platform will serve as a reliable source of information and a bridge between donors, NGOs, and affected communities.

Solution Expected: A mobile application that provides real-time crisis updates, enables secure donations, ensures transparency in fund distribution, and raises awareness through educational campaigns. It will incorporate AI-powered crisis prediction, decentralized fund management, and a volunteer network to enhance humanitarian response.

Unique Selling Points and Features:

Round 1: Core Features

1. Real-Time Crisis Information

- Integrates official data sources (UN, WHO, Red Cross, government agencies) for accurate updates.
- Displays interactive crisis maps highlighting affected areas.
- Categorizes crises based on type (natural disaster, humanitarian conflict, pandemic, etc.).
- Enables push notifications for urgent crisis alerts.

2. Donation Management

- Implements secure payment gateways (Stripe, Razorpay, Google Pay, PayPal) for seamless transactions.
- Allows users to donate to specific causes or organizations.
- Provides instant digital receipts and confirmation of donations.

3. Transparency and Accountability

- Displays real-time fund distribution reports through visual dashboards.
- Partners with NGOs to share updates on how donations are utilized.
- Implements blockchain-based tracking for transparent fund allocation.

4. Awareness Campaigns

- Creates engaging multimedia content (blogs, videos, infographics) to educate users on crises.
- Runs interactive social campaigns encouraging donations and volunteer participation.
- Gamifies engagement by awarding badges for frequent donors or campaign sharers.

5. User Authentication and Security

- Implements OTP/email-based authentication for secure logins.
- Uses two-factor authentication (2FA) for financial transactions.
- Encrypts user data and payment details to prevent breaches.

Round 2: Advanced Features

1. AI-Powered Crisis Prediction

- Utilizes machine learning models to predict future crises based on historical data and current trends.
- Alerts NGOs and users in high-risk regions before a crisis escalates.

2. Verified Crisis News & Updates Feed

- Aggregates official crisis updates from trusted sources (Red Cross, WHO, UN, Gov APIs, NGOs) into a single news feed.
- Uses keyword-based filtering to highlight key developments and cut through information overload.
- Users can flag misinformation, and moderators can approve or reject news posts, preventing fake updates from spreading.

3. Multi-Language Support

- Provides language customization for a global audience.
- Uses AI-powered translation to ensure inclusivity in crisis updates and communications.

Judging Criteria

Criteria	Description
Innovation	Novelty, creativity, and feasibility of the implemented features.
Functionality	Accuracy and effectiveness of AI-powered crisis prediction and misinformation detection.
User Experience	Intuitive UI, accessibility, and efficiency in delivering crisis-related updates.
Technical Execution	Stability, responsiveness, and real-time performance of crisis alerts and donation processing.
Impact & Reliability	Effectiveness in providing transparent, verified, and actionable crisis response data.