RSCOE

JSPM'S

RAJARSHI SHAHU COLLEGE OF ENGINEERING

(An Autonomous Institute Affiliated To Savitribai Phule University)

ACBS

Department Of Computer Science and Business Systems

अBHYUDAYA

Soft Solutions

Algorand
Bharat

FIRMWAY
Automating Confirmation & Reconciliation

INFORMATION BROCHURE

Hack-Sphere 2025

5th - 6th February 2025

EdGate®
TECHNOLOGIES

INDEX

Industry Sponsors

FIRMWAY Automating Confirmation & Reconciliation

Algorand Bharat

G Soft Solutions

Industry Partners

Intel® Unnati

EdGate® TECHNOLOGIES

JSPM'S

RAJARSHI SHAHU COLLEGE OF ENGINEERING

(An Autonomous Institute Affiliated to Savitribai Phule University)

Department Of Computer Science and Business Systems

Information Brochure Hack-Sphere 2025

Welcome to **Hack-Sphere 2025**, where ingenuity meets opportunity, and ideas transform into impactful solutions. Whether you're here to push your limits, collaborate with brilliant minds, or solve real-w we're excited to have you as part of this incredible journey. Take a moment to review the guideli smooth and enriching experience for all.

Industry Collaborators

G Soft Solutions   Algorand Bharat   FIRMWAY Automating Confirmation & Reconciliation

Event Overview

- **Event Name**: Hack-Sphere
- **Mode:** Hybrid (Online + Offline)
- **Eligibility:** Open to all Undergraduate (UG) students.
- **Team Size:** 3-4 members per team.
- **Registration fees:** ₹400 / **Team** *

*: Only Final Shortlisted Teams will have to pay the registration fees.

Event Format

1. Round 1: Online Submission

- Participants must submit a PPT outlining their proposed solution.
- The PPT template will be provided by us.

2. Round 2: Offline Hackathon

- Top 20 teams will be shortlisted for a 24-hour hackathon at JSPM's Rajarshi Shahu College of Engineering.
- Teams will develop and demonstrate their solutions in real time.

Prizes and Perks

Prizes:

- Total Prize Pool: **₹75,000 (Domain-specific).**
- Internship Opportunities: Offered by industry partners.

Perks:

- Work on **real-world industry problems** provided by experts.
- Career-boosting **internships and prizes.**
- Mentorship from **SIH finalists and winners.**
- **Networking opportunities** with peers, mentors, and industry leaders.
- **Free Food & Goodies:** Enjoy complimentary meals and exclusive hackathon swags!

Submission Rules

Submission Guidelines:

- Format: PDF (template provided).
- Content: Clearly define the problem, solution, innovation, and feasibility.

Basic Rules:

- Original and non-plagiarized solutions only.
- Adherence to deadlines and guidelines is mandatory.
- Detailed rules will be shared in the official rulebook.

Round 1 Evaluation Criteria

- The PPTs will be evaluated by industry professionals from the organization that provided the problem statement.
- The decisions made by the industry evaluators will be considered final and binding.

Prizes by Domain

Domain 1: Web 3.0

- **Winner** **-** $200 + Internship Opportunities* + Goodies
- **Runner Up -** $100 + Goodies

Domain 2: Security

- **Winner** **-** **₹**15,000 + Internship Opportunities + Goodies
- **Runner Up -** **₹**10,000 + Internship Opportunities + Goodies

Domain 3: AI & ML

- **Winner** **-** **₹**15,000 + Internship Opportunities* + Goodies
- **Runner Up -** **₹**10,000 + Goodies

*: Internships are subjected to industry policies.

Domain 1: Web 3.0

Industry Partner: Algorand

Prize pool: $300 + Internship Opportunity*

Winner - $200 + Internship* + Goodies

Runner Up - $100 + Goodies

Problem Statement ID: 1.1 Decentralized Identity

Overview: As Web3 evolves, managing and securing digital identities in a decentralized manner is crucial. This hackathon invites participants to design and develop a Decentralized Identity solution using blockchain technology to empower users with secure, private, and selfsovereign identity management across decentralized platforms.

Problem Statement: Create a decentralized identity solution that:

- Provides secure storage and management of digital identity credentials.
- Supports seamless authentication across multiple decentralized applications (dApps).
- Ensures data privacy and user control with end-to-end encryption.
- Includes a robust recovery mechanism for lost or compromised credentials.

Expected Outcome: The decentralized identity solution must focus on usability, security,usability, security, and scalability, adhering to Web3 principles of decentralization, self-sovereignty, and data sovereignty.

Problem Statement ID: 1.2 Asset Tokenization Platform

Overview: Tokenization allows for fractional ownership and trading of assets like real estate, art, and commodities. The goal is to develop an innovative platform that simplifies the tokenization process while ensuring compliance and transparency.

Problem Statement:

Design a blockchain-based platform for asset tokenization that includes:

1. Mechanisms to tokenize physical assets into digital tokens.
2. Transparent ownership tracking and trading systems.
3. Smart contracts to automate transactions and ensure trust.
4. Compliance with regulatory standards.

Expected Outcome: Your platform should emphasize user-friendly interfaces, robust security, and scalability for large datasets.

Problem Statement ID: 1.3 Decentralized Donation Platform

Overview: In the realm of social welfare, one of the major issues is the lack of transparency in how donations are utilized. Many potential donors are hesitant to contribute due to concerns about misuse or inefficiency. A blockchain-powered donation platform can solve this problem by offering traceability and accountability for every rupee/dollar donated.

Problem Statement: Develop a blockchain-powered donation platform that enables:

- Secure and traceable donation mechanisms.
- Real-time fund tracking for donors.
- Smart contract-based automation for fund disbursement.

Expected Outcome: A working donation platform prototype that demonstrates transparency and trust, encouraging greater participation in charitable activities.

Problem Statement ID: 1.4 Innovating with Web 3.0

Overview: Participants are invited to bring their own problem statement in the domain of Web 3.0 and leverage AlgoKit, the cutting-edge developer tool from Algorand, to design and enhance innovative solutions**.**

Objective: Empower developers to tackle real-world challenges or pioneer groundbreaking ideas within the Web 3.0 ecosystem using Algorand's robust and scalable blockchain infrastructure.

# **Note:** All the listed problem statements should be developed using AlgoKit**.**
There are going to be webinars and sessions conducted for all shortlisted teams to get familiarize with AlgoKit.

Consider using the Algorand platform to enhance your development experience with advanced tools.

[Check Algorand Resources]

Let the countdown to HackSphere begin! We can't wait to see what you'll build!

Domain 2: Security

Industry Partner: G soft Solutions

Prize pool: ₹25,000 + Internship Opportunities

Winner - ₹15,000 + Internship + Goodies

Runner Up - ₹10,000 + Internship + Goodies

Problem Statement ID: 2.1 Email Spoofing Prevention Checker

Overview: The objective is to build a web-based Email Spoofing Prevention Checker that validates email headers, detects spoofing attempts, and ensures domain authentication compliance with SPF, DKIM, and DMARC protocols. The tool will provide actionable insights to users and administrators, helping to identify vulnerabilities, enhance email security, and reduce the risk of spoofed emails.

Problem Statement: Create a web-based tool that:

Validates email headers to detect spoofing.

Check if an email domain uses proper authentication (SPF, DKIM, DMARC).

Provides actionable feedback to users and domain administrators.

Expected Outcome: A tool that helps prevent email spoofing and improves email security.

Problem Statement ID: 2.2 Biometric Password Vault

Overview: Managing passwords securely is a growing concern for users who need to protect sensitive information. Weak or reused passwords remain a significant security risk. A biometric password vault offers a convenient and secure solution by integrating biometric authentication for accessing stored passwords.

Problem Statement: Design a secure password vault that:

1. Stores passwords using strong encryption algorithms.
2. Allows access only through biometric verification (e.g., fingerprint, facial recognition).
3. Supports multi-platform password retrieval for ease of use.
4. Provides features to generate and manage strong, unique passwords for multiple accounts.

Expected Outcome:

A functional, biometrically-secured password vault that generates, stores, and retrieves passwords with minimal user friction, reducing security risks associated with weak or reused credentials.

Problem Statement ID: 2.3 Real-Time Cyber Threat Detection and Alert System

Overview: With the increasing frequency and sophistication of cyberattacks, organizations struggle to identify and mitigate threats before significant damage occurs. Developing a real-time alert system can help monitor networks, detect anomalies, and respond proactively to potential breaches.

Problem Statement: Design a security solution that:

1. Continuously monitors network traffic for suspicious activities or anomalies.
2. Issues real-time alerts to administrators upon detecting potential threats.
3. Categorizes alerts based on severity and provides actionable recommendations.
4. Supports integration with existing security infrastructure (e.g., SIEM systems).

Expected Outcome:

A functional prototype of a real-time cyber threat detection and alert system capable of enhancing organizational defenses against evolving cyber threats.

Let the countdown to HackSphere begin! We can’t wait to see what you’ll build!

Thank you!

Domain 3: AI&ML

Industry Partner: Firmway

Prize pool: ₹25,000 + Internship Opportunities

Winner - ₹15,000 + Internship* + Goodies

Runner Up - ₹10,000 + Goodies

Problem statement ID: 3.1 Smart Statement Reader

Overview: The objective is to build an AI/ML-powered Smart Statement Reader solution that directly processes PDFs extracted from ERP/accounting systems, automatically detecting and classifying file formats, and accurately extracting tabular financial entries into structured formats like Excel or CSV. By reducing manual intervention, this solution aims to enhance efficiency and accuracy of data being extracted as an exact match of the source file.

Problem Statement: Develop a Smart Statement Reader solution that:

1. Accepts raw PDF files containing accounting data directly from accounting systems.
2. Leverages AI/ML models to:
   - Detect and classify the structure/format of uploaded PDF files (e.g., column layouts, headers, and naming conventions).
   - Extract financial ledger entries into structured formats (Excel/CSV) with high accuracy.
   - Handle variations in document layouts and inconsistencies in data formatting.
   - Self-learn(train the model) based on user feedback to improve data extraction accuracy over time.
3. Groups and classifies uploaded PDFs based on detected formats for streamlined processing.
4. Provides a confidence score for extracted data accuracy, highlighting low-confidence entries for user review.

Expected Outcome: A functional prototype of the Smart Statement Reader solution with:

- High accuracy in detecting, classifying, and extracting financial data from diverse PDF formats.
- A self-learning model that improves performance with user feedback.
- Seamless export of processed data into structured formats (Excel/CSV).

Technology Requirements:

- Use OCR technologies for PDF data extraction.
- Apply machine learning frameworks (e.g., TensorFlow, PyTorch) for format detection and classification.
- Implement feedback mechanisms to train the model iteratively based on user input.
- Develop a user-friendly interface for uploading files, reviewing results, and providing feedback.

Evaluation Criteria:

- Accuracy of data extraction and classification across diverse PDF formats.
- Usability and intuitiveness of the solution.
- Scalability to handle large volumes of files and varied formats.
- Effectiveness of the self-learning feedback loop in improving model performance.

Challenges or Constraints:

- Managing the diversity in PDF formats and data layouts.
- Ensuring the system is robust against noisy or incomplete data.
- Balancing high accuracy with real-time processing speed (within a few seconds output should be shown).

Problem statement ID: 3.2 Intelligent Partial Invoice Matching

Overview: Matching invoice numbers between two datasets is often a challenging task due to inconsistencies such as partial matches, formatting differences, or human errors. This problem results in inefficiencies and delays in the reconciliation process. The objective is to develop an AI/ML-powered solution that automates the matching of partial invoice numbers, provides recommendations for uncertain matches, and self-learns from user corrections to improve over time.

Problem Statement: Develop a solution for intelligent partial invoice matching that:

1. Automatically matches invoice numbers between two datasets, even when:
   - Only partial matches are available (e.g., truncated or missing prefixes/suffixes).
   - Minor discrepancies exist due to formatting or human errors (e.g., extra spaces, special characters).
2. Recommends potential matches with a confidence score(e.g. Between 1-100 range) for entries where certainty is low.
3. Allows users to manually match entries via a user-friendly interface and captures these corrections to:
   - Improve future matching accuracy through a self-learning AI/ML model.
   - Continuously train the model for better performance over time.

Expected Outcome: A functional prototype of the partial invoice matching solution with:

- High accuracy in identifying matches and recommending potential matches.
- A self-learning model that improves through user interactions and manual corrections.
- A user-friendly interface for manual review and confirmation of matches.
- A final report (excel-sheet) of which entry is matched or recommended against which other entry

Technology Requirements:

- AI/ML frameworks (e.g., TensorFlow, PyTorch) for pattern recognition and confidence scoring.
- Natural Language Processing (NLP) for handling partial matches and discrepancies in text.
- Development of an intuitive UI for manual corrections and user feedback.

Evaluation Criteria:

- Accuracy and reliability of automated matching.
- Effectiveness of recommendations for uncertain matches.
- Scalability to handle large datasets with varying formats.
- Usability and intuitiveness of the manual matching interface.
- Improvement in matching accuracy over time through self-learning.

Challenges or Constraints:

- Handling edge cases where multiple potential matches exist.
- Balancing performance (speed) with accuracy for large datasets.

Let the countdown to HackSphere begin! We can’t wait to see what you’ll build!

Thank you!

Scan For More Info

Co-ordinators:

Mayur Shinde	+91 7385784661
Yash Tekade	+91 8624825680
Swaroop Saikar	+91 7796227788
Varad Pawar	+91 8767068260