REQUEST FOR PROPOSAL (RFP)

Intelligence platform for flagging fraudulent fintech apps

Project: Development of a working prototype for an intelligence tool for flagging fraudulent fintech apps ("the Project") for a financial authority (the "Agency").

Description: A solution for financial authorities to flag fraudulent smartphone apps through the collection, storage, and analysis of app store reviews. Initially intended as an internal supervision tool, the tool must ultimately serve insights to the public through APIs and other interfaces that allow for development of additional services.

Contracting Entity: Financial Innovation for Impact

Countries and Agencies: Reserve Bank of India Innovation Hub (RBIH)

Grant Value: USD TBD

Publication Date: 17 July 2024

Submission of Proposal Deadline: 31 July 2024 23:59 GMT Time (UTC +0)

Project Implementation Dates: August – December 2024

Procurement Process Managed by: Financial Innovation for Impact

Submission: Submit all documents as detailed in Section III (3 a. Submission requirements) below

Queries: email suptech-launchpad@jbs.cam.ac.uk with any queries.

Language: All submissions must be written in English.

I. Project Description

The focus of the project is to create a prototype of an intelligence tool for flagging fraudulent fintech apps. This prototype solution intends to solve the problem that represents the increase in the number of fake fintech applications and scams in the country under supervision of the Agency.

Online scammers follow non-transparent methods, collect exorbitant interest rates, cause harassment through harsh recovery measures, and unauthorised use of personal data. This has affected the general trust in the financial system, and especially on the fintech space and solutions. Moreover, due to involvement of malicious entities based in other countries, such apps have serious impact on national security, general economy, and citizen's safety.

Therefore, the prototype solution that will be developed is an intelligent system to flag to supervisors any instances of potential fraud in fintech apps, based on metadata from (i) purported lending apps from app-stores; (ii) other concerned apps and (iii) other relevant sources within the system, to identify patterns and flag malign actors pre-emptively.

The creation of a robust system to detect frauds is essential for the protection of its users, continued growth, and reliability of the system. Ultimately the system should provide for the future ability to serve as a basis for applications that serve the generally public (e.g., a website or smartphone-based service that can act as a preventive anti-fraud measure while installing any fintech app in the phone of the customer).

The selected solution provider is expected to propose a solution that describes how the technology and code can be transferred to the financial authority upon completion of the prototype project, per the expressed intention of the Agency to transition to in-house maintenance and development.

By default it should be assumed that the entirety of the solution will be transferred to the Agency's in-house team at the end of the prototyping stage. However, throughout the course of the project, the Lab will facilitate conversations between the solution provider and Agency (via the regular Project Team meetings) to more granularly assess which components will be transitioned to in-house development and at what point in the product lifecycle this transition is expected to occur. The solution provider will be expected to maintain and share up-to-date documentation with the Agency and the Lab reflecting the results of such conversations throughout the project.

1. BASIC REQUIREMENTS

Through this tool, the Agency will be able to:

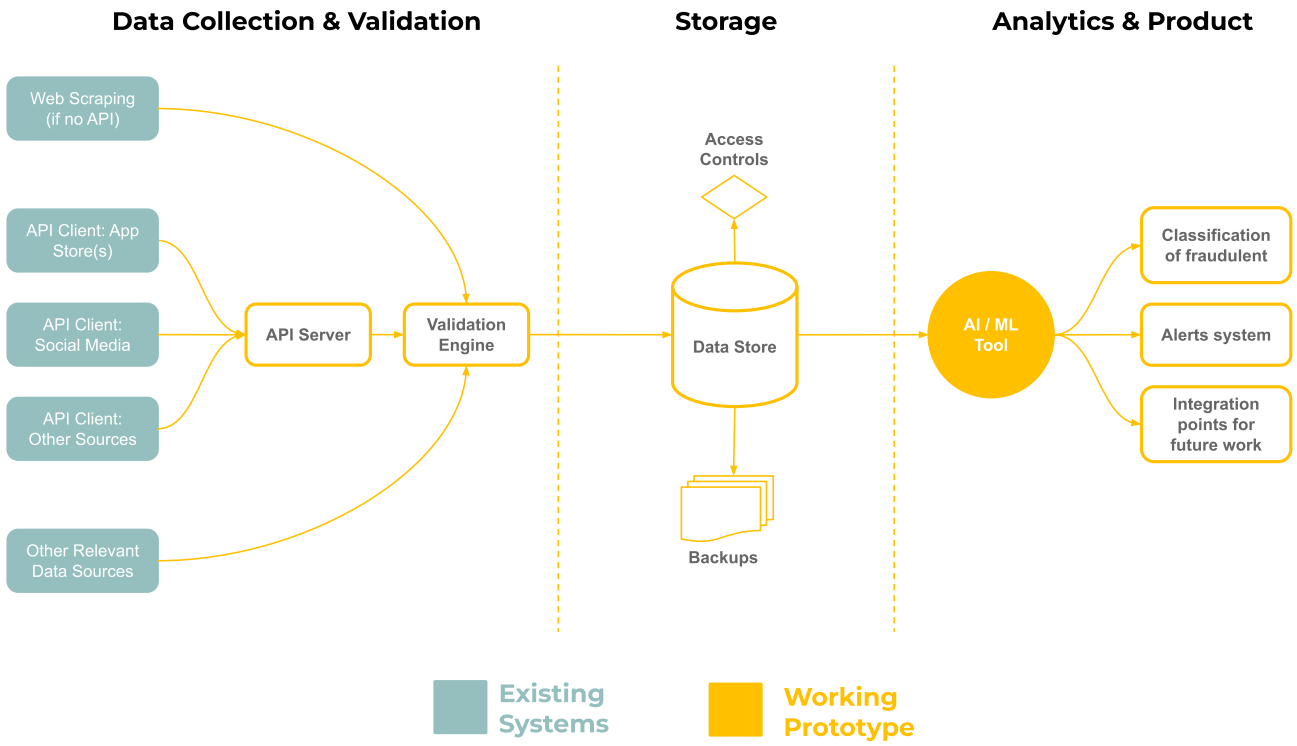
- Collect and analyse metadata to identify the bad actors in the digital lending space (fintech apps, in general), take action, and warn the customers as is appropriate, which

should result in reduction in successful fraudulent activities and enhance the robustness of the fintech ecosystem.

- Pre-emptively screen out malicious apps, to the extent possible.
- Advance sustainable development of financial sector by ensuring people's trust in digital finance.
- Allow for the integration of additional future services, such as tools for end customers to identify fraudulent apps and receive alerts before installing such dubious apps.

2. HIGH-LEVEL ARCHITECTURE

A more granular breakdown of the process follows, including developing APIs to access various databases, refinement of data schemas based on Data Structures, training of the AI/ML based decision engine, testing of the application as per the following data flow diagram:



3. KEY TECHNICAL REQUIREMENTS

The prototype for detecting fraudulent fintech apps will have the following key elements:

COMPONENT	ID	FEATURE	DESCRIPTION	PRIORITY
Data Collection	1.1	API Clients	If an app store has open APIs, a solution would capture metadata directly. In the absence of such endpoints, the solution should provide for a purpose-built web scraper.	HIGH
	1.2	API Server	Dedicated server to manage the API data and data from other sources.	HIGH
	1.3	Instrumentation	Validation engine to inspect and process the data.	HIGH
Centralized Storage	2.1	Formatting	Create a data dictionary and store the data	HIGH
	2.2	Access Controls	The storage mechanism must provide for varying levels of access controls with default access expiration dates	MED
	2.3	Automatic Backup	The storage system should automatically allow for cold storage backups in case of disaster recovery	MED
Decision Engine	3.1	AI/ML based analytics	A tool that analyses data from various sources (metadata on the app available in the app-store, data in the app, data from supervisory entities, unstructured data from social media etc.) to predict whether the app concerned is a good or a bad actor. Example: Network Analysis, Anomaly detection algorithm, etc.	HIGH
Data Product	4.1	Reporting	Reporting interface and dashboard to review applications classified as fraudulent, along with high-level statistical summaries	

In Scope:

- Development of the intelligence tool for detecting fraud among fintech apps using metadata, including data collection and validation mechanisms, storage mechanisms, ML-based analytics, and interfaces for additional future products to integrate with.
- Potential additional valuable features proposed by the solution provider
- For this suptech solution, proprietary solutions are permitted so long as they propose a mechanism for the turnover to RBIH/RBI per the requirements of this RFP.
- For proprietary/licensed fintech smartphone apps, proprietary solutions are permitted so long as there is a reviews site from which to apply the trained model to infer probability of fraudulence

Out of Scope:

- If selected app store does not have Open API, the API client for app store would be out of scope.
- Development of any product for end consumers or the public.

4. APPLICABLE LAWS & REGULATIONS

The engagement may require the Agency to share certain data with the Lab and one or more vendors or innovators working as part of the Lab team. While the solution primarily requires publicly available data, any non-public data can be shared conditionally on the same confirming with the provisions of extant laws and regulations. Following, non-exhaustive, laws and regulations may apply in the collection, processing, and sharing of financial and personal information, including:

- Information Technology Act, 2000 ('the IT Act'), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the SPDI Rules')
- the Information Technology (The Indian Computer Emergency Response Team and the Manner of Performing Functions and Duties) Rules, 2013 ('CERT-In Rules')
- Direction No. 20(3)/2022-CERT-In ('the Directions')
- Consumer Protection Act, 2019 ('CPA') and Consumer Protection (E-Commerce) Rules, 2020
- Rules imposed by the Telecom Regulatory Authority of India ('TRAI')
- Rules imposed by the Securities and Exchange Board of India ('SEBI')
- Rules imposed by the Pension Fund Regulatory and Development Authority
- Unified Licence Agreements issued pursuant to the National Telecom Policy, 2012 by the Department of Telecommunications ('DOT')
- The Digital Personal Data Protection Act passed by parliament in 2023

II. Project Structure

1. PHASES

The Project has four phases, elaborated below:

1. Kickoff and interface design, including technical integration specifications
2. Development of a working prototype
3. Integration and development of additional data analytics and/or visualization
4. Testing and signoff of the working prototype

Throughout all project stages, vendors are expected to meet weekly with key stakeholders of the Agency as well as the Lab's Launchpad team, to ensure close coordination and agility.

1) Kickoff and interface design, including technical integration specifications

During the first phase, the selected vendor (in coordination with the Lab's Launchpad team) will gather requirements from the Agency and produce an initial Design Document that includes integration and user interface specifications. This living document should include specifications for the client-facing portion of the prototype, communicated in a manner such that clients of the prototype can understand how to integrate with systems and processes, submit data, and

use the system without necessarily understanding the entire architecture behind the software. This includes specifications for the data integration (analytics and visualization) phase of the project. This Document is to be shared as needed with any other key stakeholders (e.g., vendors of relevant software used by the Agency, any financial institutions needing to integrate) to allow them to develop integrations and/or adapt existing software during the development phase. The design document should also include criteria for user acceptance testing for use during the testing phase.

2) Development of a working prototype

The Detector system will first receive a small subset (a representative sample, defined and shared by RBI) of historical data needed to train and test the model in a controlled environment.. Initial data being submitted via the Detector will be sample data to start, with real data only being introduced to the system once proper security protocols and data sharing agreements are in place. Starting with a prototype and a small data set will allow the vendor to quickly identify and address any unforeseen issues early in the Project development cycle. For example, this data may include:

- Meta data from app stores
- Historical data on registered financial institutions from the website of the Agency's published data that could be useful to train the model, or other data needed during prototyping to help establish inputs and tags for machine learning.
- Data from sample apps previously collected, pertaining to both good actors and bad actors.
- Data from Social Media apps

Once agreements are in place, the Detector's model can be trained, tested, and validated on more sensitive real data, complaints data drawn from the Agency's complaints system.

The working prototype will also facilitate candid discussions among Project stakeholders regarding issues such as model interpretability, potential externalities, and the like.

3) Integration and development of additional data analytics and/or visualization

Once the working prototype has been developed, tested, and accepted, the vendor will provide any analytics and visualization tools defined during the design stage.

Additionally, the selected vendor should (i) assess the needs of the Agency to understand which dashboards, reports, and statistics are most useful and/or difficult to produce under the current web-based market monitoring system; and then (ii) propose and develop a prototype mechanism for extracting and visualizing this information from data consumed, processed, and

produced by the working prototype. This could involve creating custom queries, scheduling the generation of reports, and outputting them in various formats.

The final UI of the prototype must be done before the final tests of Phase 4.

4) Testing and signoff of the working prototype

Once the proof of concept has been completed to the satisfaction of the involved parties, integration and testing with real institutional data can begin. The working prototype will be tested with the Agency, based on any user acceptance criteria defined during the design stage, to allow the vendor to ensure that the prototype is functional with real data before it is scaled into full production. This approach also minimizes the risk of interruption due to unforeseen technology failure and serves to inform estimates of the cost to scale the prototype to a production-grade service.

A cyclical final test of the prototype and improvements by the developers must be done until the product is adherent to the functional specification document as reflected through the completion of the user acceptance testing criteria. Once UAT is complete, the prototype package will be expected to be delivered, including training materials, project documentation, and other items to be specified in the Project Agreement with the selected vendor.

2. TIMELINE

The project should commence as soon as practically possible after the Project agreement (contract) comes to effect. This Project will ultimately deliver a prototype that will be tested by the Agencies no later than December 2024.

III. Vendor Selection

1. PROJECT AWARD

The successful applicant will:

- Be awarded a grant from the Bill & Melinda Gates Foundation and International Finance Corporation to develop and test the required solution. This is a fixed-sum contract to cover all the applicant's expenses related to the development and testing work, including staff time, hardware, software, travel, and all other project-related expenses.
- Be listed in the Lab's online Vendor Database, a dynamic, web-based platform to explore and connect with solution providers who have been active in the global suptech market.

- Be invited to the Lab's SupTech Week - the largest gathering of the suptech community globally, where you will have the opportunity to demo the prototype to potential clients and connect with funders.
- Be recognised in a case study the Lab will write following the successful completion of this project, distributed through the Lab's direct newsletter to a list of over 20,000 global contacts in the suptech space, and on LinkedIn.
- Engage with the suptech community through the Lab's hackathons and tech sprints and receive tailored coaching from the Lab on coordinating suptech projects with Financial Authorities.

2. KEY FEATURES OF THIS INITIATIVE

- Blind review process: A panel of expert reviewers will score anonymised proposals without knowing the name of the vendor submitting them
- Competitor scorecard: Applications will be assessed by the panel using a set of scoring metrics and weighing the relative importance of each attribute.
- Rapid turnaround time: We will select the winning vendor and award 50% of the grant within15 working days from submission of a valid invoice. The remaining 50% of the award will be granted in one installment upon completion of the deliverables according to projected timelines.

3. RULES AND GUIDELINES

a. Submission Requirements

Selected vendors must demonstrate that their proposed solution meets the needs of the Project, both in terms of technical topic responsiveness, execution, and innovative approach.

Please complete all sections using font Century Gothic, size 11, line spacing multiple at 1.15.

Submit your RFP here

In the 'Proposal' section, please submit your proposal following the prescribed structure below:

1. **Part 1 - Brief company background:**
    - Technical expertise to effectively implement the project
    - List of representative projects
    - Managerial capabilities and relevant experience to effectively implement the project
    - Adequate resources to devote to the successful implementation

This section should be no longer than 4 pages

Part 2 - Technical proposal:

- **Detailed technical specification and architecture.** This should address components of the key technical requirements in Section I. This section should be no longer than 8 pages. A technical architecture diagram should be included.
- **Execution plan and resourcing.** Indicative development / implementation schedule based on the timeline parameters set out above and the project structure set out in Section II. This section should be no longer than 4 pages
- **Additional element for consideration.** A free-form response to elaborate on the innovative aspects of the solution you propose and why your agency should be awarded this competition. This section should be no longer than 1 page
- **Indicative development / implementation schedule**. Based on the timeline set out above.

Information needed for due diligence

Any questions and requests for clarification should be sent via email to suptech-launchpad@jbs.cam.ac.uk with a subject of "RBI Prototype"

b. Tips for applicants

1. Your proposal must demonstrate an innovative approach that meets all stated goals and complies with all restrictions and guidelines.
2. Personal and organizational information should be provided separately from the proposal. Proposals will be sent to reviewers without personal or organizational information. Do not include any identifying information directly in your proposal.
3. In addition to subject matter experts, your proposal will be reviewed by a panel with broad expertise and a track record in identifying innovations – these reviewers may not be deep domain experts in your field. You must describe your ideas in unambiguous language without the use of jargon unique to your field.
4. The work proposed in your application must include a clear set of key activities required to develop and test the prototype solution. Proposals with vague descriptions or vague methodologies will not be funded.

c. Disclaimer

The Lab reserves the right to edit, invalidate, terminate, and/or reissue this RFP at any time and for any reason. The Lab also reserves the right to select a vendor through an alternate method and/or adopt an alternate timeline for vendor selection that differs from the method and/or timeline described in this document, the websites of the Lab and Launchpad, and any other communications related with the process. Furthermore, the Lab expressly disclaims responsibility for any costs incurred by any vendor in responding to this RFP, regardless of whether the RFP is edited, invalidated, terminated, and/or reissued at any time and for any reason.