## **\* About the project**

## *Be sure to write what inspired you, what you learned, how you built your project, and the challenges you faced. Format your story in* [*Markdown*](https://www.markdownguide.org/cheat-sheet/)*.*

## *Ans below:-*

## **About the Project**

This project focuses on building a prototype resembling a Fraud Protection agent that can help ordinary citizens, especially those who are less aware and emerging digital users against scam calls and texts. Such people may include senior citizens, teenagers with recent digital bank accounts, people from rural parts becoming the emerging digital banking customer segment, people who are not very conversant with English or not so tech savvy etc. though recent reports suggest that well informed individuals in senior private and public sector roles have also fallen for such frauds. This prototype Fraud Protection agent, named ArthaRaksha, is intended to be at the user’s service 24x7 in his / her native language through its mobile app version. The prototype is built using Vertex AI's Agent Builder and is powered by Google Cloud Platform and Google latest Large Language and Multi-modal languages such as Gemini 1.0 and Gemini 1.5 pro. The prototype can transcribe and translate native language speech and text, summarize the event, identify the possibility of fraud, analyze a potential fraud, categorize as per RBI (Reserve Bank of India) fraud classification guidelines and help generate incident report of the potential fraud as per the inputs needed by cybercrime departments with pre-filled parameters (powered by Google’s Gen-AI LLM and MLM models underneath) and finally submit the incident with just one ‘click’ through automated API integration to the agencies and also to banks (if applicable).

## **Inspiration**

The first inspiration was from the recent

The inspiration for this project came from personal experiences:

1. In one case, one of the prototype developer’s aunt received a fraud call concerning my cousin with the ultimate intent to siphon off money. The caller claimed that the developer’s cousin was in trouble and demanded immediate payment for supposed legal fees. Although the developer's aunt did not fall for the scam, the experience left a lasting impact on the family, highlighting the urgent need for effective fraud detection mechanisms.
2. In another incident, the other prototype developer’s mother received a fraudulent call from a bank that attempted to steal personal information under the garb of KYC renewal for an existing joint account. This joint account has the family’s lifelong savings linked to it.

When we researched further, we found a recent report by the Indian Cybercrime Coordination Centre in Mar'2024 outlining that digital financial frauds impact on direct individual banking users amounted to a staggering ₹40,000 crore over the last two years, that's approx. 4.8 Billion US Dollars. At the same, time, the number of such fraud calls have grown by more than 110% in the last 2 years in India. Cybercrime, especially financial fraud, poses a burgeoning and rapidly expanding threat in India, impacting millions of individuals and unsuspecting digital banking users.

This alarming situation underscored the increasing prevalence of phone scams and motivated us to develop a solution to help detect and mitigate such fraudulent activities. Generative AI powered ArthaRaksha App prototype built upon the Google Cloud VertexAI Agent Builder platform is an attempt to demonstrate the possibility to complement the relentless efforts of Indian govt, RBI, and banking players in dealing with the herculean, rapidly mutating fraud patterns of scammers. With a collective efforts of all legitimate financial players in India, ArthaRaksha can be powered by a fraud detection and processing platform owned by RBI and contributed to by all interested and legitimate banking players (similar to working models such as those powered by NPCI (UPI), NSDL (for ecommerce marketplace), Digilocker, or upcoming inter operable payment system of RBI). This way, such an underlying model can be continuously trained on newest fraud data and patterns across languages and be up to date not only with latest fraud detection patterns but also new fraud awareness protection, response, and control mechanisms developed by both RBI / Govt agencies and banking and other financial players.

Customized versions of the App can be built and deployed by legitimate financial institutions such as banks whereas the underlying platform, data, and model may be contributed to by all financial players, RBI, and Government financial and cybercrime detection agencies. The app intends to bridge the gap between the genuine, dedicated, and independent initiatives by law enforcement agencies, RBI, banks etc. and their adoption as part of a banking user’s daily life. Adoption is best when the interaction with sophisticated backends are hidden to make it a layman’s app in his hand-held device.

Financial fraud methods are similar to viruses and follow viral evolution patterns - they mutate fast and if the protection system is not fast enough to respond, damage is done at a mammoth scale by the time controls are put in place. The ability envisioned through the solution is to embed a much needed “real-time”, trusted analysis capabilities for fraud call and text content providing users with an immediate warning (in some cases, even before a fraud call is terminated) and to reduce the reaction times of the protection, control, and reporting systems in place.

## **What I Learned**

Throughout the project, I gained invaluable insights and skills:

1. **Understanding of Fraud Tactics and Response systems in place**: Most common tactics used by fraudsters, understanding their methods, channels and psychological ploys to deceive victims.
2. **Understanding of Fraud protection initiatives**: This includes RBI campaigns, crime registration rules, policies, banks initiatives to curb fraud cases, and processes to raise fraud incidents.
3. **Google CLoud’s Vertex AI**: We became proficient in using Vertex AI's agent builder integrating with other Google cloud services such as cloud function, cloud run, Gemini 1.5 pro model available in VertexAI Model Garden, . Learnings also include building, using, and integrating VertexAI data stores (vector Databases), Ready to use Google cloud APi services such as Speech to text and translation services, and more.
4. **Prompt Engineering and grounding:** the reality that Prompt engineering for complex scenarios need structured logical approach to problem solving and work best with robust full functional examples and a fine tuned model is best suited to avoid hallucinations and model distractions. The underlying quality and richness of the data used for grounding is a key make or break factor for such use cases that need to deal with highly unstructured and unexpected data patterns.
5. **Gen-AI based developer empowerment:** Gen-AI capabilities are still evolving but even at their current state of maturity, the technology can fast-track complex Data and AI development projects significantly, they can empower technologies with business acumen and Business analysts with tech acumen thereby blurring the lines of traditional core competence and areas of expertise. Gen-AI supported by ecosystem of data, application, and integration capabilities, can rapidly increase the proportion of AI investment and projects that lead to real, positive Business ROI (and real NPV realizations) but more importantly it can have a real, positive social impact on using technology for the genuine welfare of people.
6. **Promises, Limitations and opportunities:** We learned that Vertex AI Agent builder can become a game changer in the Through the development experience, we came across many limitations, or alternatively opportunitie

## **Building the Project**

### **Step 1: Research and Data Collection**

The first step involved extensive research into the characteristics of fraud calls. We collected data from various sources, including publicly available datasets of scam call recordings and transcripts. Below are example datasets that were used:

* RBI published publicly available documents were used to benchmark category of frauds
  + < put link of RBI doc here>
* A BigQuery scam call dataset was used that was publicly available:
  + <put link of scams calls / sms text that you found>
* Few audio calls simulating real fraud call were made - they are available in github as example calls and used in the prototype flow. Bank / ecommerce clients' names that were used to make the call look real scam calls made by scammers. These are not real scam calls and has no relation with the bank name or ecommerce company name taken in the scam calls.
  + <put github link of the audio calls here.

### **Step 2: Designing the Architecture**

I designed the system architecture using Vertex AI's agent builder. The architecture included:

* **Data Ingestion**: Data is stored on GCS Bucket.
* Pls add here
* **Deployment**: Deploying the trained Agent Builder on Slack.

### 

### **Step 3: Implementation and Testing**

After deploying the Agent Builder, we integrated it with Slack which alerts users when a call is suspected to be fraudulent. We conducted extensive testing to ensure the system's reliability and accuracy, making adjustments as necessary based on feedback and performance metrics.

## **Challenges Faced**

1. **Data Quality**: One of the significant challenges was ensuring the quality and relevance of the training data. Fraud call characteristics can vary widely, making it difficult to create a comprehensive dataset.
2. **Model Accuracy**: Achieving high accuracy in real-time detection was challenging due to the subtle nuances in legitimate versus fraudulent calls.
3. **FYX**: Pls add
4. **XYZ**: Pls add

## **Conclusion**

This project was both a personal and professional journey. Inspired by a real-life incident, I was motivated to leverage advanced Vertex AI technologies to address a growing concern. Through this project, I not only honed my technical skills but also contributed to a cause that could potentially protect others from falling victim to fraud. The challenges faced along the way were valuable learning experiences, shaping my understanding of Vertex AI applications and their impact on society.