Enhancing Digital Financial Safety with athenaGUARD: A User-Centric Approach

**Introduction:**

In the ever-evolving landscape of digital finance, ensuring the safety and security of users is paramount. This document outlines the objectives, target audience, and user requirements for the development of "athenaGUARD," a user-centric large language model (LLM) solution. With a focus on guiding and assisting citizens in their digital financial journey, athenaGUARD aims to guard against scamsters by providing to-the-point anti-scam information and addressing scam-related concerns.

**Objectives and Target Audience**

The primary objective of athenaGUARD is to empower citizens who has been affected by financial scams, especially those new to digital financial apps, by offering real-time, need-specific solutions to counter scams. The utilization of the Llama2 model enhances its capabilities in extracting scam-specific information, and the fine-tuned localized policy knowledge base ensures relevance to the user's context.

**Target Audience:**

AthenaGUARD is designed for citizens intending to access digital financial apps but harbor concerns about scams. We have categorized our audience into three personas:

* Awareness Seekers (First-time digital financial app users): Providing informative resources such as best practices, guidelines, and do's and don'ts to educate users about potential scams.
* Affected Users (Those affected by scams & looking for quick help): Offering guided interaction through bank helplines, forms, and consumer helpers to assist users promptly.
* Security Providers (Banks, Government Agencies Security Team): Delivering policy and compliance standards, including anti-scam steps, regulations, and up-to-date knowledge on digital financial security.

**Solution Differentiators**

AthenaGUARD distinguishes itself through various solution differentiators:

* User-tailored Functionalities: Offering a range of features such as FAQ, Q&A, and scam query resolution to cater to diverse user needs.
* Optimized Resource Utilization: Ensuring efficient use of resources, with model optimization based on availability and real-time adaptability.
* Up to Date Policies and Compliance Knowledge: Providing users with the latest information on policies, compliance standards, and regulatory changes.
* Smart Defaults for Parameters: Introducing intelligent defaults to enhance user experience and streamline interactions.
* User Query Soft Prompting: Facilitating user engagement by employing soft prompting for natural queries.

**Advanced Features and Capabilities**

* Precise & Factual Information Retrieval: Utilizing the Llama2 model for accurate and consistent information retrieval.
* Capture Patterns in Policy Writing: Identifying patterns in policy guidelines to enhance the precision, diversity, and sensitivity of the information provided.
* Context-Aware Insights: Ensuring coherent and responsive outputs by maintaining awareness of the context in which queries are presented.
* User-Centric Approach: Incorporating a user-friendly natural query auto-enhancement feature and self-adaptation based on human feedback to enhance user satisfaction.

**Conclusion and Future Developments**

In conclusion, athenaGUARD stands as a pioneering solution in the realm of digital financial safety, catering to the diverse needs of users and addressing the growing concerns about scams. The continuous improvement of athenaGUARD through self-adaptation and user feedback ensures its relevance and effectiveness over time. Future developments will focus on expanding functionalities, integrating emerging technologies, and strengthening partnerships with security providers to fortify the digital financial landscape.

This document serves as a guide for the LLM, elucidating the purpose, objectives, and unique features of athenaGUARD, fostering a deeper understanding of its role in enhancing digital financial security for users.

Bottom of Form