**Utilizzo locale del AI BAFIT e controllo sulla diffusione dati.**

**PROBLEMA INIZIALE:**

Quando si avviava il modello Gradio eseguiva il codice in un web con IP locale e uno con IP pubblico accessibile a chiunque.



Il rischi che si hanno in questo modo risultano essere 2:

1) Qualsiasi persona interna o esterna all’azienda può avere accesso e utilizzare BAFIT e ciò potrebbe danneggiare il modello a tramite feedback errati.

2) I file utilizzati per allenare la AI potrebbbero essere caricati in cloud quando si passa per hugging face.

**PROBLEMA INIZIALE:**

Impedire che Gradio esegua il codice in modo pubblico.

**Errato**, mettendo share=true si va a creare sia Gradio fa l’hosting sia locale che pubblico



**Corretto**, con questo cambiamento si impedisce a gradio di fare un hosting pubblico.



**Risultato:**



Dopo dei semplici controlli nel codice si puo comprendere che i dati non vengono caricati nel cloud grazie a queste ragioni:

* Per utilizzare il modello di llama3-8 utiliziamo Ollama il quale scarica ed esegue il modello in modo locale
* Il modella llama3-8 non è capace di collegarsi alla rete ne di eseguire ricerche, è un modello pre-trained il quale però non ha i dati aggiornati in tempo reale.
* Gradio esegue una interfaccia locale e quindi non c’è il rischio che i dati vengano caricati in cloud passando per hugging face.
* All’interno del codice quando viene definito la classe “Chatbot” non avvengono chiamate ad hugging face, a hugging face hub oppure al suo API