WHISPER: Weather Hiding via Intent Semantics and Private Edge Retrieval

Yannis Lagrosa, Sam Houston State University, HBCU/MI; Raul Rivero, UNC Chapel Hill, AFRL/RF Internship; Tyree Sloan, Norfolk State University, HBCU/MI; Nicholas Yagnik, Princeton University, *VICEROY MAVEN*

Abstract

Weather data is ubiquitous, freely accessible, and innocuous, yet repeated queries to meteorological APIs can reveal sensitive information about an observer's location, operational timing, and intent.

Our program, **WHISPER** (**W**eather **H**iding via **I**ntent **S**emantics and **P**rivate **E**dge **R**etrieval) is a privacy-preserving agentic system that obscures the true nature of weather data requests through query fragmentation, decoy injection, and adversarial provider routing.

Introduction

This poster concerns itself with establishing two LLM-driven Publicly Available Information (**PAI**) methodologies for obtaining information on the network edge.

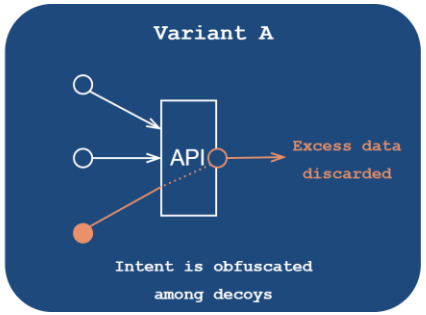
Variant A surrounds the target request with decoys, obfuscating the original data.

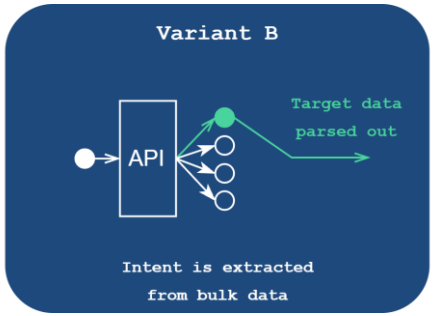
Variant B instead requests a bounding box for the area, randomizing the location of the target within that box to further obscure the original target location.

These variants yield their own advantages, so we evaluate and benchmark them against each other to determine an optimal balance between intent obfuscation and edge resource constraints. We then dynamically choose the model based on real-time network statistics and threat levels.

Variant A — Hide In The Crowd

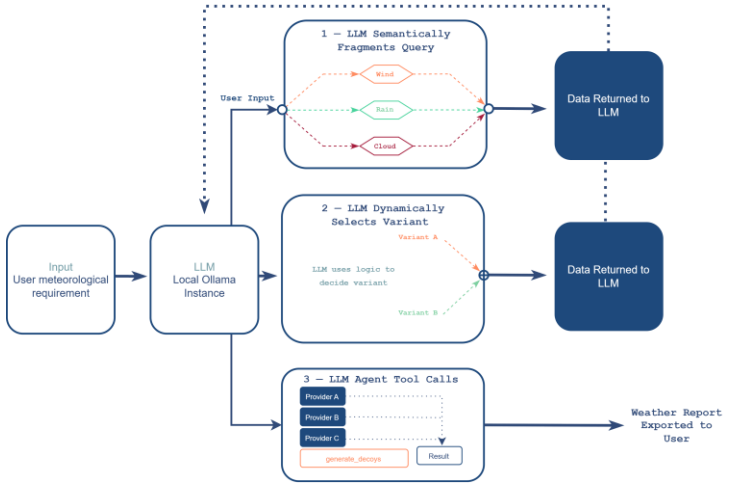
Variant A utilizes decoys to hide the intended target in a crowd of fakes. We leverage the reasoning capabilities of the LLM, ensuring that the decoy coordinates are geopolitically relevant to the original set of coordinates. Before reaching the LLM, API calls that do not relate to the target location are sanitized and removed.





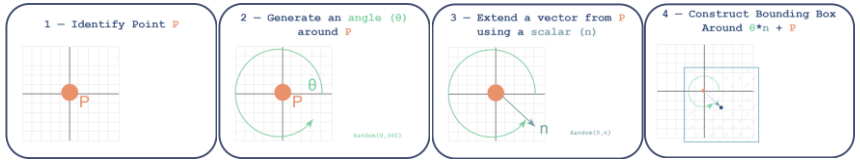
Variant B — Request In Bulk

Variant B casts a wide bounding box around the target coordinate, filtering out only relevant results from the perspective of the client. We *randomize* the location of the target coordinate inside of the bounding box to ensure that adversaries cannot gather data on the target using the box's parameters.



WHISPER first acquires the user's meteorological request, sending the data to the LLM which utilizes semantic analysis to decipher the goal and fragment it into atomic queries.

For **Variant B**, The target coordinate should be randomly distributed inside of the bounding box.



Discussion

Current Private Information Retrieval (PIR) or cryptographic methods to privately exchange data between a client and server are predicated on the assumption that the server is cooperative. This design ensures that no single provider receives sufficient contextual signal to reconstruct the original query or infer the requester's operational context.

WHISPER supports the mission of the Airforce, allowing high-stakes operational teams such as: UAV/Drone operators, reconnaissance teams, resupply teams, and field teams to acquire weather data without the risk of surveillance.

Conclusion

- For **Variant A**, the probability that an adversary is able to successfully isolate the target query is:

$$P_{isolate} = (1/k)^n$$

- Fragmented, decoy-padded queries reduce per-provider information gain.

The WHISPER model ensures that user intent is obfuscated, utilizing purely open-source meteorological data and an LLM running on the edge to generate light-weight weather reports without sacrificing privacy. WHISPER shows that by decomposing queries across multiple API providers, weather data can be privately accessed without the cooperation of the server.

Approved for Public Release on 09 July 2026; Distribution Unlimited: Case Number: AFRL-2026-3153

Advisor: Dr. Soamar Homsi (AFRL/RIGA) | soamar.homsi@us.af.mil