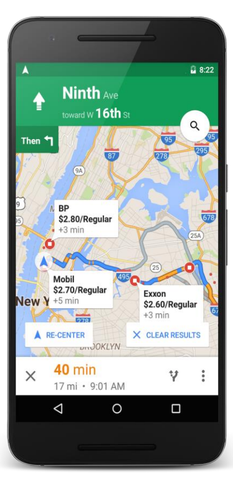
Oblivious k-Nearest Neighbors for Secure Map Applications

Jamie Lee, United States Naval Academy

Faculty Advisers: Adam Aviv, George Washington University, Travis Mayberry, United States Naval Academy, Daniel Roche, United States Naval Academy



Introduction

Cloud storage enables cheap, efficient, and reliable data access and storage. **Map applications** are types of cloud storage servers that allow users to query for nearby facilities and locations such as restaurants, gas stations, or post offices.

Relevance to SaTC

Our goal of enhancing map application security is aligned with the purpose of the SaTC PI Meeting of supporting research in the protection of cyber systems, improvements in network resiliency, and promotion of safe usability. This project will describe one unique approach to preserving user privacy and developing trustworthy technology that can be used by users around the world.

Problem Statement

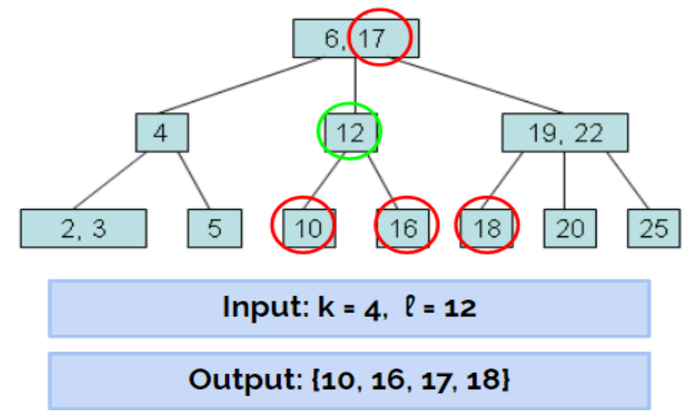
Cloud storage users are susceptible to data leakage through their access patterns. Even if the client trusts the server to store and retrieve data without modification, the server can attempt to obtain data about the user through factors relating to their access patterns. In map applications, the server can observe the user's location as they are making search queries, which is a significant security risk.

Solution

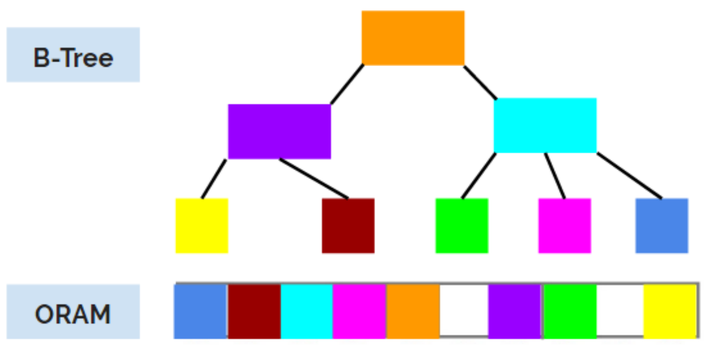
We propose a novel remotely-stored data structure, the **ORAM-backed Hilbert B-Tree**, with the following features:

- modification of the **B-Tree data structure** to enable oblivious **k-Nearest Neighbor** queries
- implementation of orthogonal **Hilbert space-filling curves** to store 2D coordinate data
- storage of the B-Tree's nodes in an **oblivious RAM (ORAM)** to obfuscate the user's access patterns

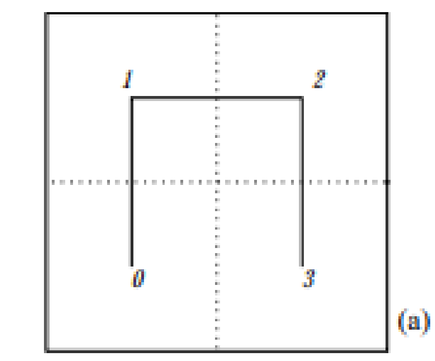
Once fully implemented, it will be integrated into the network to operate as a cloud server and tested with Google Cloud Services to evaluate accuracy, performance, and monetary cost.

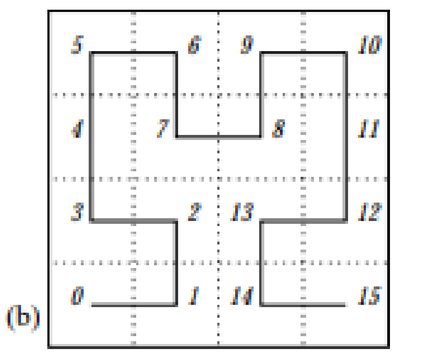


k-Nearest Neighbor Range Query



ORAM Algorithm



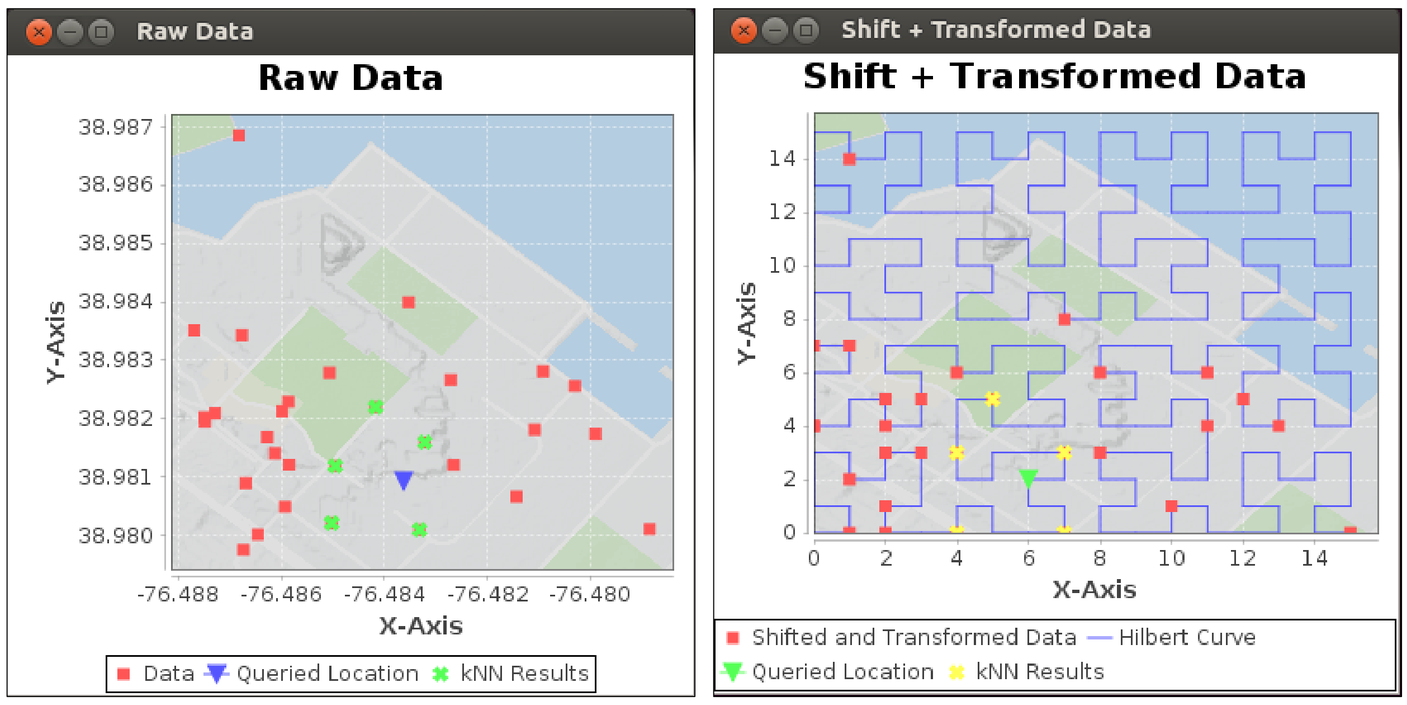


Hilbert Space-Filling Curve

Contributions

Through this research project, we are:

- Developing a new oblivious data structure to support 2D queries using $O(log^2 n)$ **bandwidth**
- Implementing the data structure with **orthogonal Hilbert Curves and B-trees stored in an ORAM** to support oblivious 2D search queries
- Enabling **oblivious k-NN search queries** for 2D map applications in cloud services



k-NN query in dataset of USNA landmarks in Annapolis, MD. Left displays results plotted on raw data, right displays results plotted on points fitted to Hilbert Curve of order 4.

Practical Impact

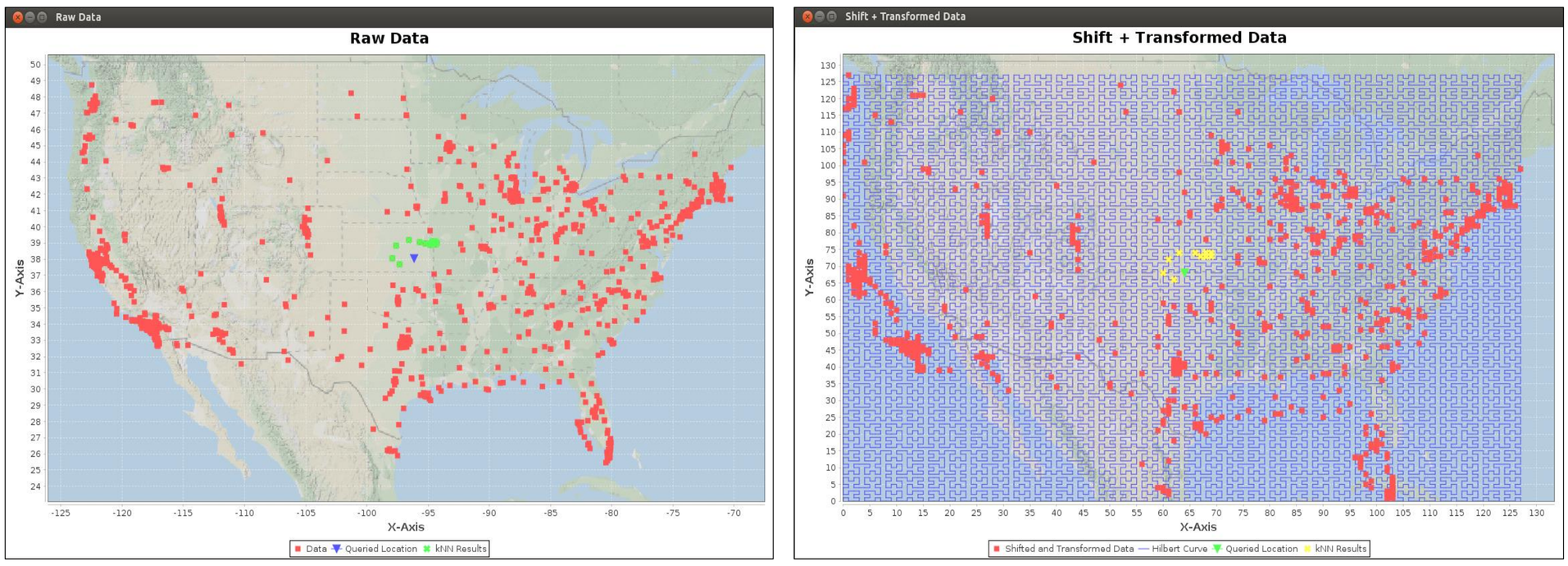
This research will provide a **significant improvement in map application security without compromising performance**. This could also improve security of military operations that utilize GPS and tracking systems such as the Android Tactical Assault Kit (ATAK), an Android smartphone geospatial infrastructure and military situational awareness app built using NASA WorldWind.

Education & Outreach

This research was presented at the 2019 **Jean Bartik Symposium**, an event that invites US service members to celebrate women and underrepresented groups in computing disciplines.

SaTC Grant

Supported by Award #1618269 "**TWC: Small: RUI: Achieving Practical Privacy for the Cloud**," along with Seung Geol Choi of the United States Naval Academy.



k-NN query in dataset of 1000 largest cities of the Continental US. Left displays results plotted on raw data, right displays results plotted on points fitted to Hilbert Curve of order 7.