

# IntegriDB: Verifiable SQL for Outsourced Databases



## Challenge:

When outsourcing a database to a cloud server, the client cannot validate the correctness of the results returned for SQL queries on the database.

## Solution:

- A set accumulator supporting set and algebraic operations is proposed. It is used as a building block to validate multi-range and join queries in SQL.

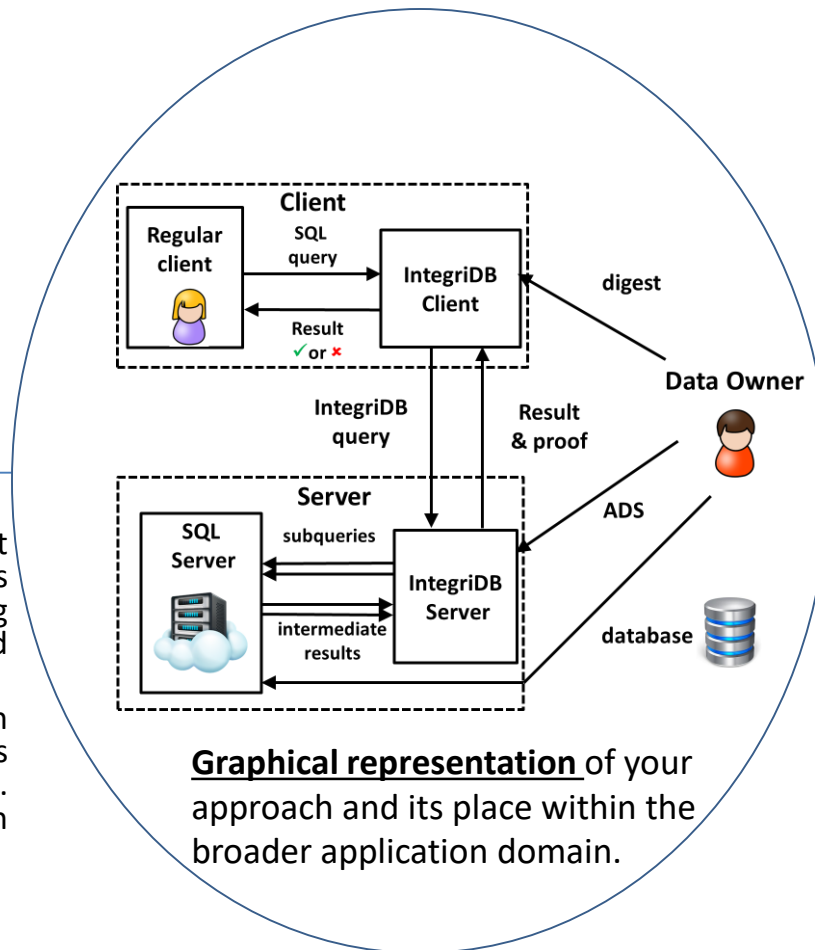
- The accumulator is embedded in to authenticated interval trees that support range queries. Updates of the data structure can be performed efficiently.

NSF award 1514261

University of Maryland

Contact: Charalampos Papamanthou

cpap@umd.edu



## Scientific Impact:

- It is the first implementation of a verifiable database system that supports a rich class of SQL queries.

- It shows the possibility of building efficient verifiable computation systems tailored for important real-world applications.

## Broader Impact:

- The system enables hospitals and government agencies to outsource their computations to cloud servers with a correctness guarantee of correctness of the results.

- Cloud service providers using this technique can attract more users because of the verifiability feature.

- Our approach is 3 orders of magnitude faster than applying existing generic verifiable computation systems.