CERIAS

The Center for Education and Research in Information Assurance and Security

Secure and Private Outsourcing to Untrusted Cloud Servers

Presenter: Shumiao Wang
shumiao@purdue.edu

Advisor: Mikhail Atallah
mja@cerias.purdue.edu

Dept. of Computer Science, Purdue University

Problem Addressed

-Organizations are reluctant to use cloud servers for confidential data and computations

-Impediment to larger-scale usage of cloud storage and server-aided computation

Our Goal

-Design protocols for using cloud servers without revealing to them the confidential data and computations

-No sacrifice in **quality of results**. (“As if fully shared”)

-Using existing **inexpensive** cloud infrastructure (not the Premium services)

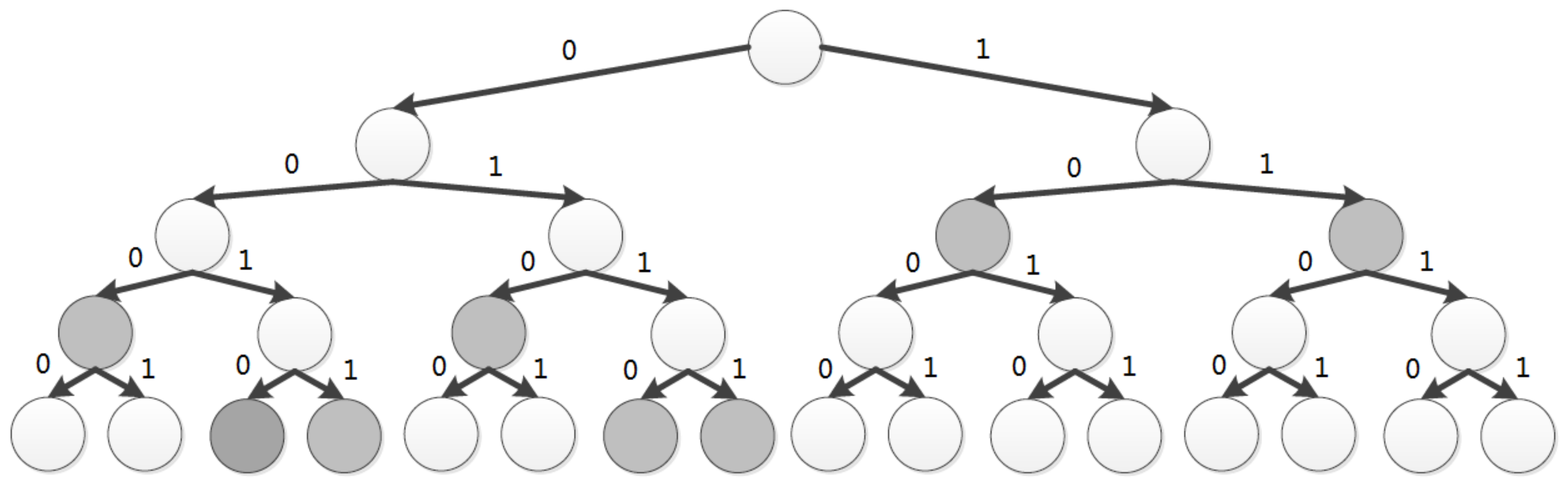
-Achieve the advantages (cost, convenience, etc.) of the Cloud without its drawbacks

Storage Outsourcing

-The client has limited storage
-Enable efficient search and retrieval from the database without leaking the client‘s data

Example: Outsourcing the **Nearest Neighbor** queries

What does the server store?
-Encrypted indexing prefixes associated with their nearest neighbors



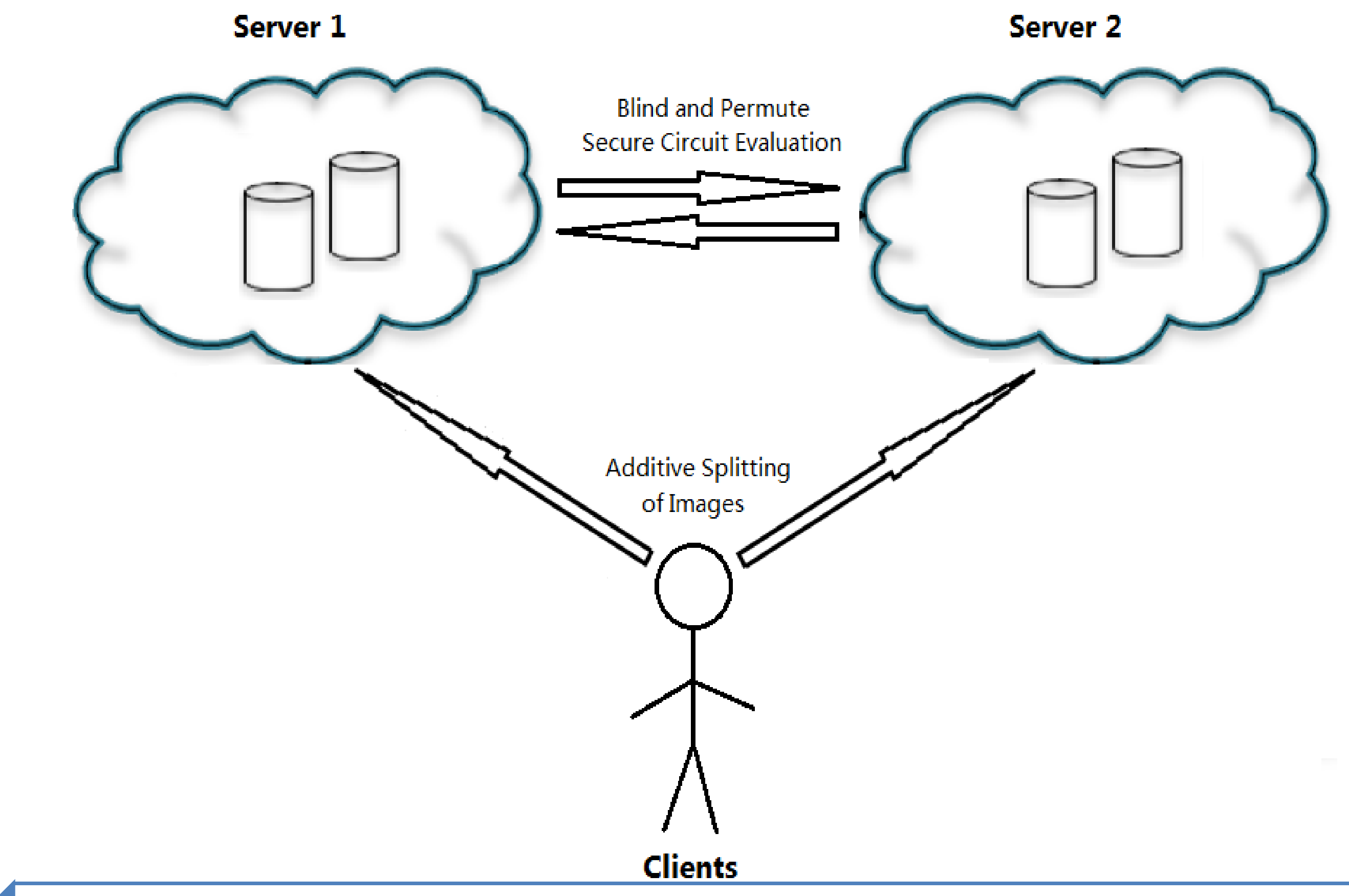
Example of Indexing Prefixes for a dataset S={2,6,7,11}

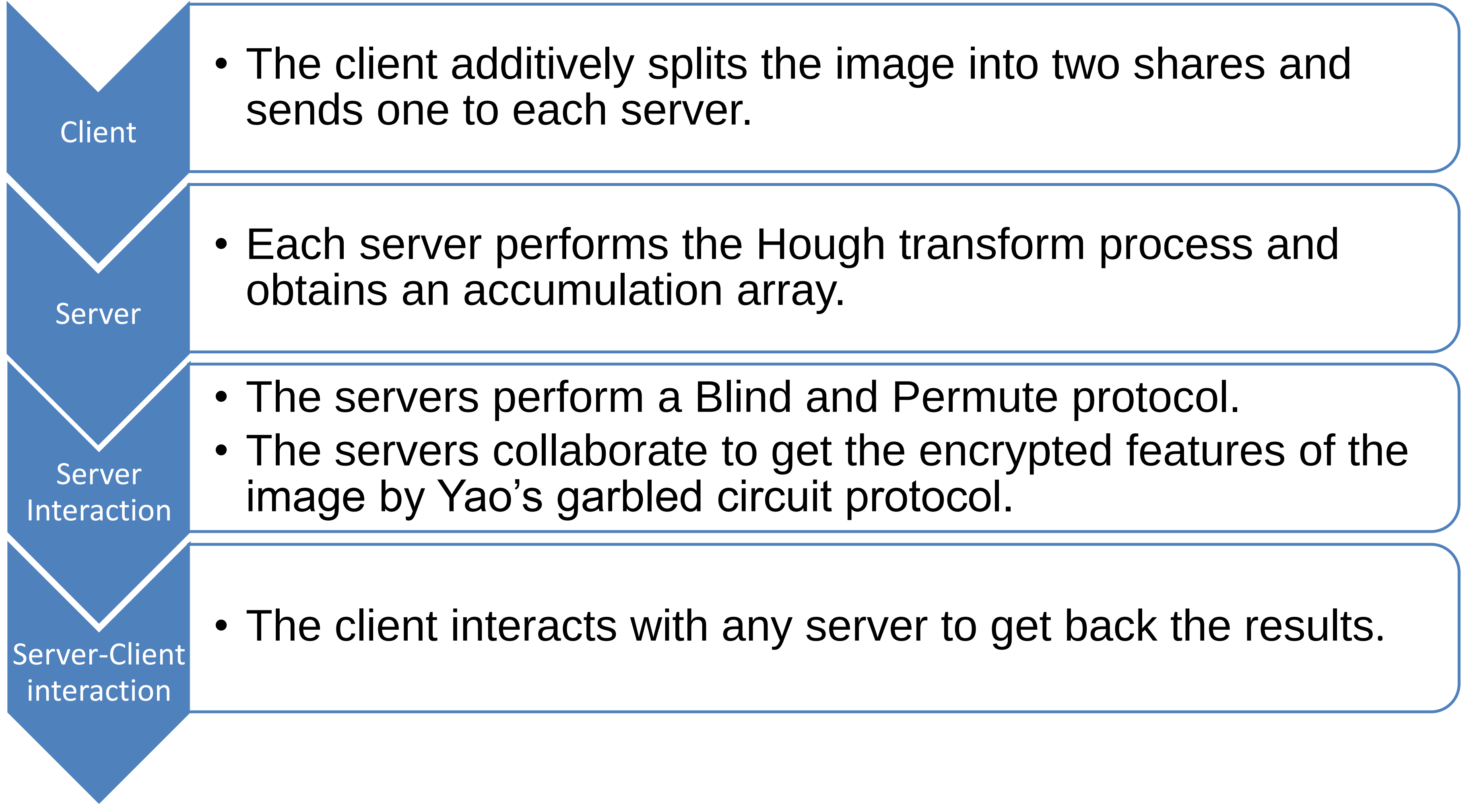
How to query?
-The client constructs all the prefixes of the query value, which contains exact one matching item at the server side, sends them to the server and gets back the matching item and its nearest neighbor.

Computational Outsourcing

-The client has weak computational power
-The server performs specific computation on the client’s inputs without seeing them

Example: Outsourcing the **shape based feature extraction** of images





Client
- The client additively splits the image into two shares and sends one to each server.

Server
- Each server performs the Hough transform process and obtains an accumulation array.

Server Interaction
- The servers perform a Blind and Permute protocol.
- The servers collaborate to get the encrypted features of the image by Yao’s garbled circuit protocol.

Server-Client interaction
- The client interacts with any server to get back the results.

CERIAS

PURDUE UNIVERSITY