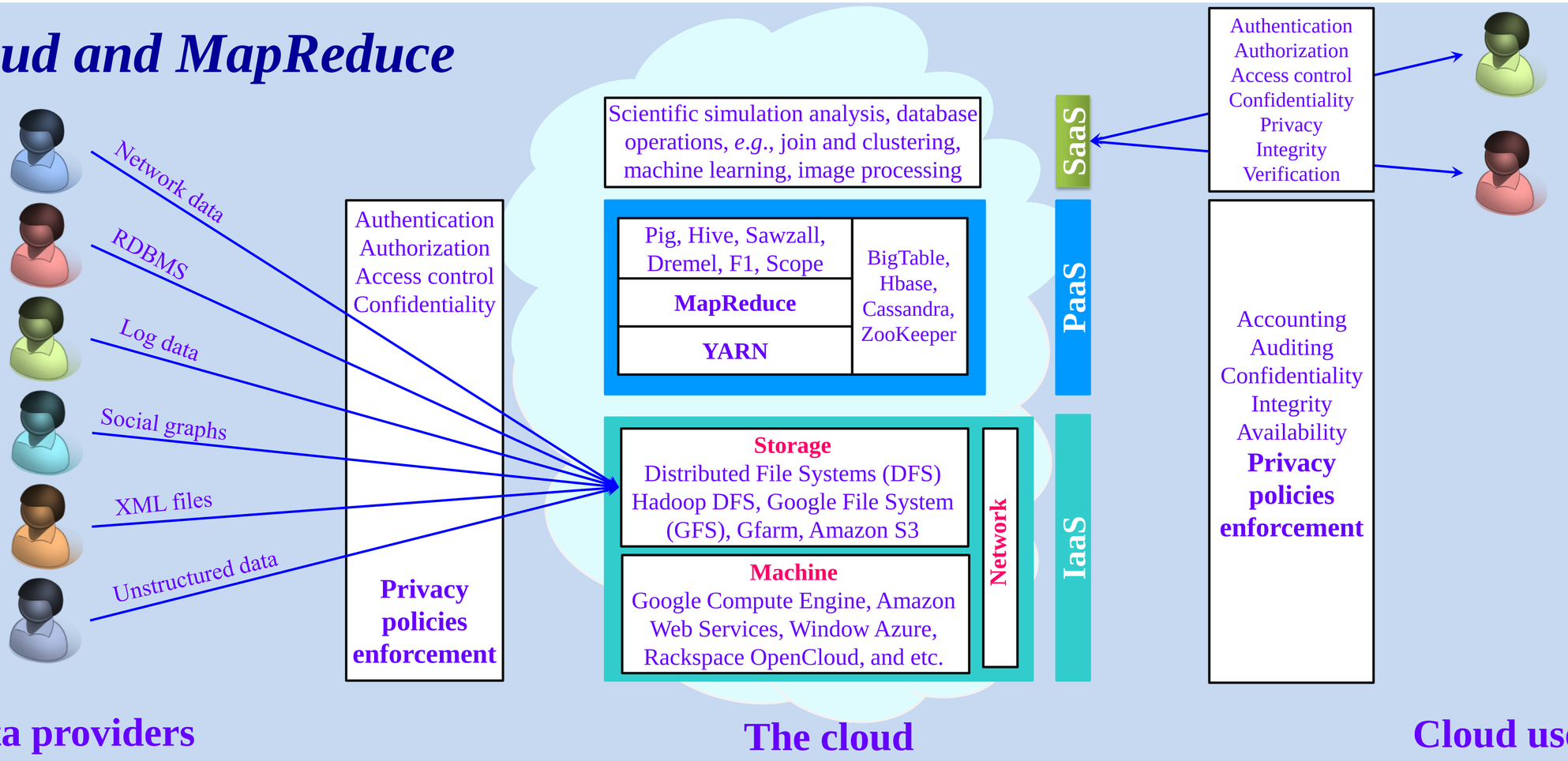
Privacy-Preserving Computations on MapReduce

Shlomi Dolev[1], Shantanu Sharma[1], and Yin Li[2]

[1] Ben-Gurion University of the Negev, Israel. [2] Xinyang Normal University, China.

Goal: Information-theoretically secure data and computation outsourcing

1 The cloud and MapReduce



2 A relation: Employee

Id	F. Name	L. Name	Dept.
E101	Adam	Smith	Sale
E102	John	Boro	Design
E103	Eve	Smith	Sale
E104	John	Williams	Sale

3 The Problem

How to perform **information-theoretically secure data and computation outsourcing**, so that a malicious cloud provider cannot know the database and a query.

4 The Solution

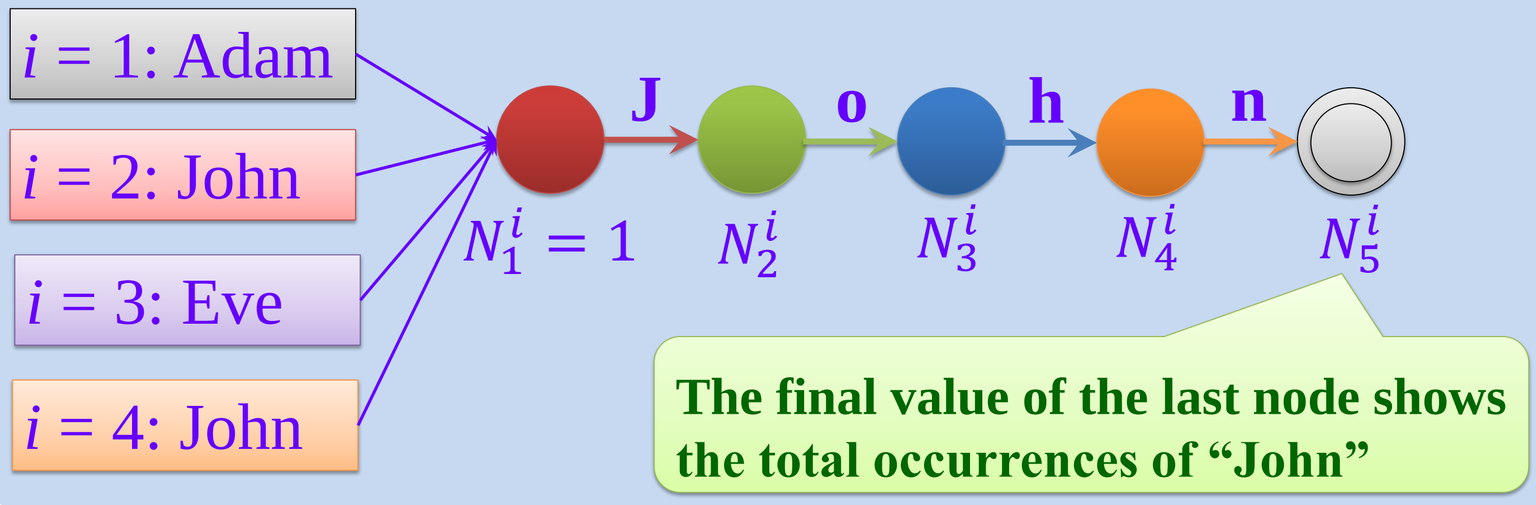
Shamir Secret-Sharing + Accumulating Automata

Four MapReduce-based operations

1. **Count**
2. **Search and Fetch**
3. **Equijoin**
4. **Range selection**

5 Count Operation

How many people have their first names as "John"



6 Search and fetch

Fetch the tuple where the first name is "Adam"

Id	F. Name	L. Name	Dept.
E101	**Adam**	Smith	Sale
E102	**John**	Boro	Design
E103	**Eve**	Smith	Sale
E104	**John**	Williams	Sale

Adam

Execute accumulating-automata over each first name and then multiply the resultant to the whole tuple. At the end, add all the values of each attribute.

For multi-tuple fetch, equijoin, and range selection, check the reference.

7 Reference

- S. Dolev, S. Sharma, and Y. Li. *Private and Secure Secret Shared MapReduce*. Based on the patent *Accumulating Automata and Cascaded Equations Automata*.