Trustworthy Data From Untrusted Servers
Rohit Jain, Sunil Prabhakar
{jain29, sunil}@cs.purdue.edu
Purdue University

Motivation
- Data is often stored at untrusted servers
  - Data in the cloud
  - Insecure server
- Can we establish the trustworthiness of data from these servers? I.e.
  - Authenticity of retrievals
  - Integrity of data (updates)
  - Provenance of data
  - Indemnity for the server (cloud)

Protocol for Static Data
- Data is static
  - Only Alice can modify data

Model
- Untrusted Server
- Trusted Server

Challenge: Dynamic Data
- Clients can modify data. No centralized vetting of updates
  - A trusted server is used to keep track of proofs

Experiments
- Easy to implement on top of an existing DBMS (e.g. PostgreSQL)
- Protocols provide authenticity, integrity and indemnity for relational databases
- Significantly reduces level of trust required
- Verification is decoupled from transaction execution
- Easy to implement
- Reasonable overhead