Is it Secret, is it Safe?

Security Services in Peer-to-Peer Database Systems

Tony Young

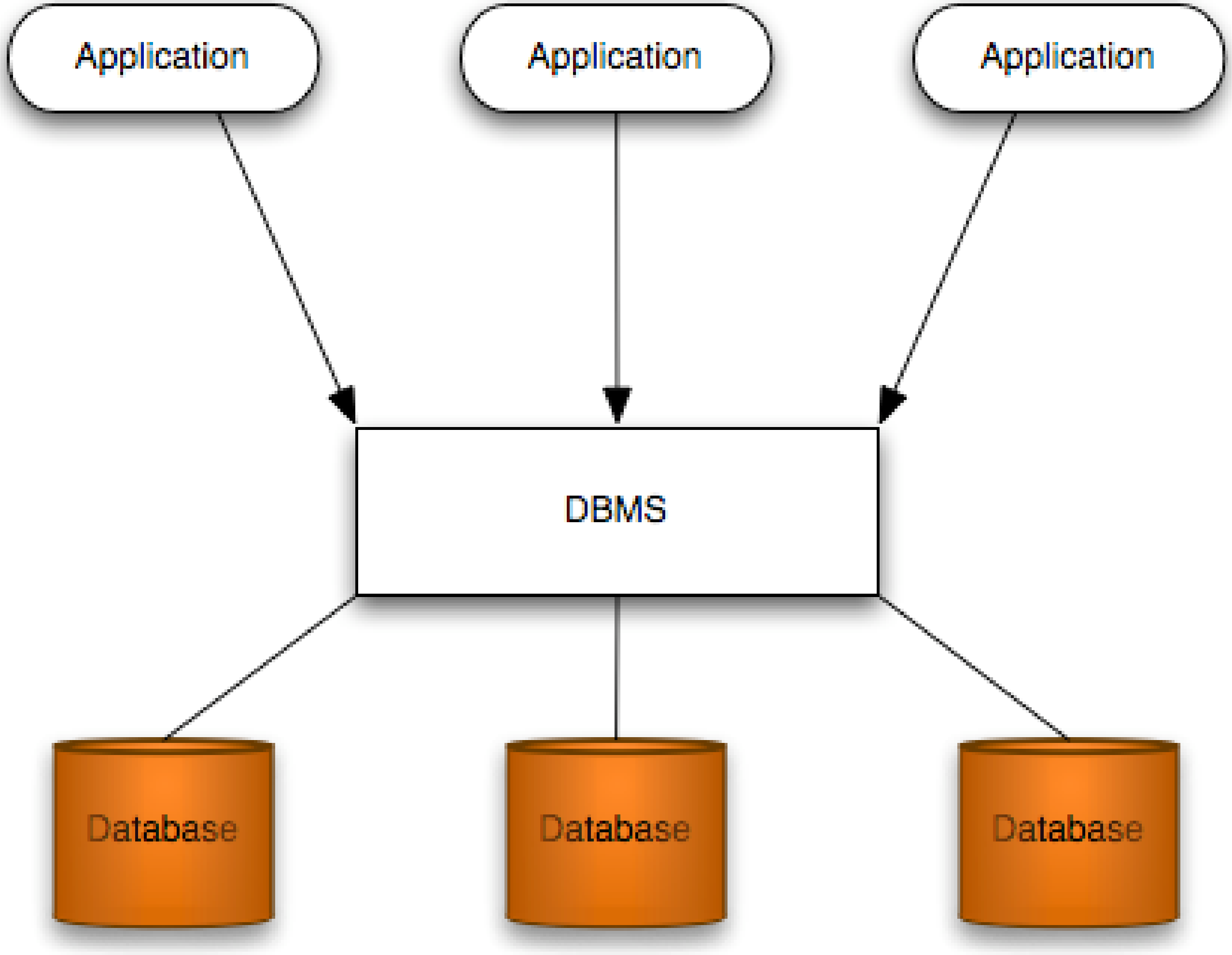
M.Math Candidate

October 28th, 2004

Traditional Database Systems

- Database systems have been in use for many years
  - Large companies store employee, product, invoicing information
  - Schools store student records
  - Hospitals store patient records
  - Families store budget and income tax information
  - … Etc.
- Databases have the power to organize our information and provide quick and easy access to it

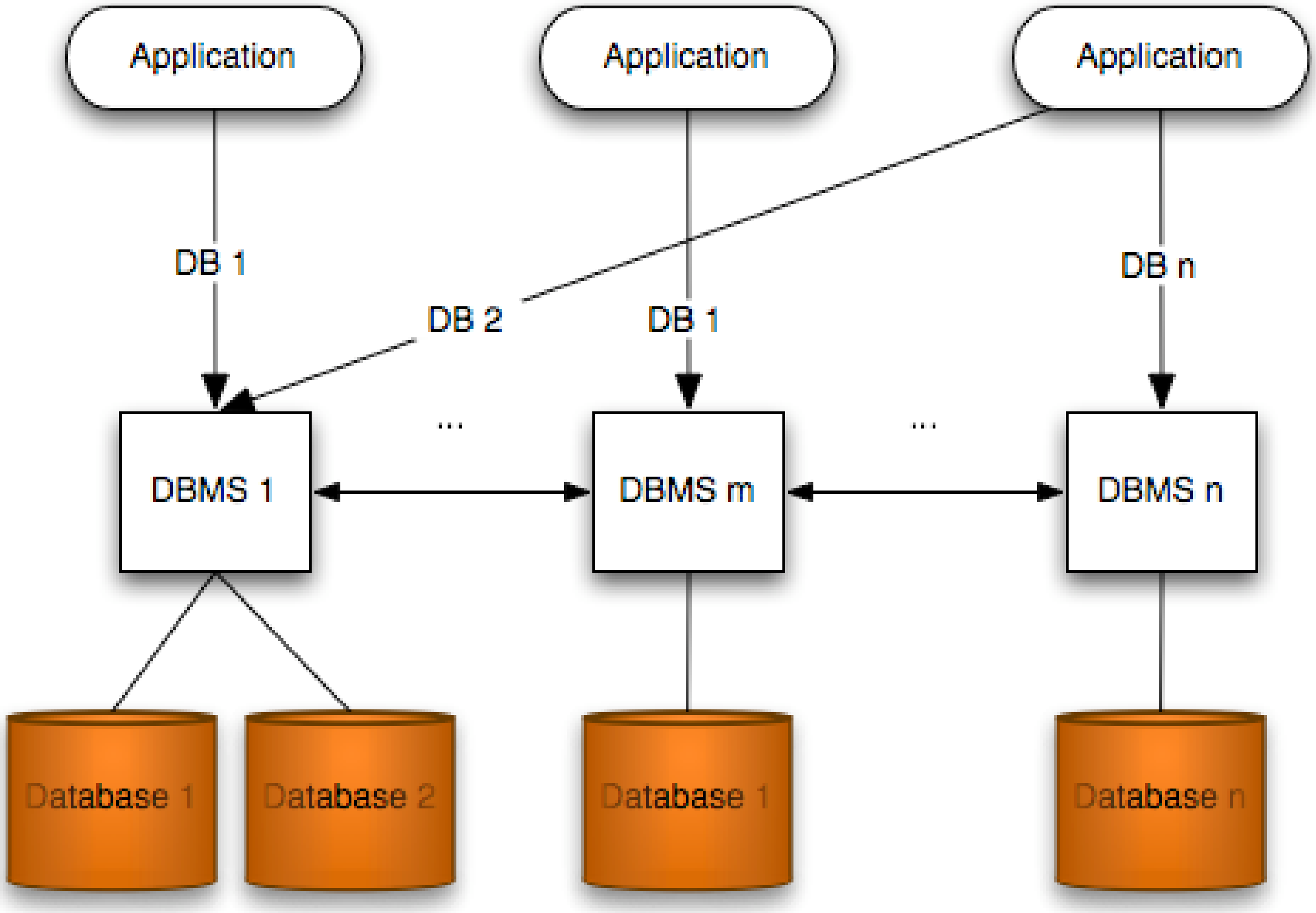
Traditional Database Systems



Distributed Database Systems

- Distributed database systems have been in use for many years
- Allow for
  - Local autonomy
  - Improved query performance
  - Greater data reliability through replication
  - Greater data availability through replication
  - High expandability
  - Easy data sharing
- Distributed database systems give organizations flexibility to tune their storage and access protocols
  - Replication = speed

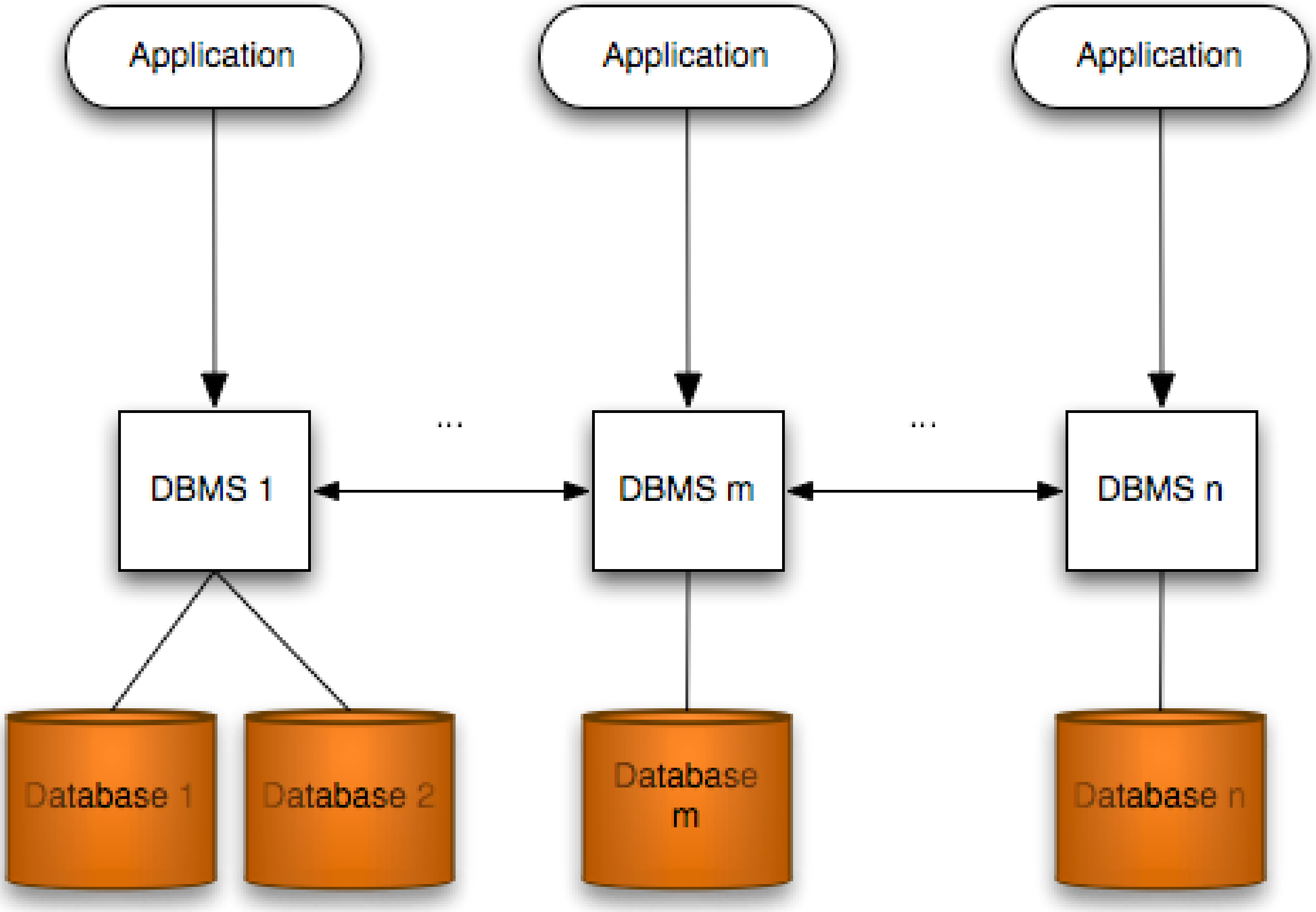
Distributed Database Systems



Peer Database Systems

- Peer-to-peer (peer) architecture has recently been applied to database systems
  - Allows a node to act as a client for performing queries and a server to answer them
- Peer databases pose many implementation challenges

Peer Database Systems



Implementation Challenges

- Nodes may join and leave a cluster at any time and are not known to the cluster ahead of time
- In distributed database systems, nodes are added out of necessity and are known to the cluster ahead of time

Implementation Challenges

- The schema for a peer database is not global/homogeneous (i.e. several schemas might be used to represent the same data)
- The schema for a distributed database is global/homogeneous (i.e. data stored at one site is in the same format as data stored at another)

Implementation Challenges

- The data in a peer database system might not be complete (i.e. a group of peers might not have the complete set of information required to answer a query)
- A distributed database system contains a complete set of information in each cluster

Implementation Challenges

- Peer database systems must route queries to many nodes in order to receive a complete answer to their query
- Distributed database systems must route queries to a small set of nodes (sometimes only one) in order to answer a query

Application Areas

- Peer databases can be applied to
  - Development environment configuration management
  - Genomics
  - Healthcare
  - Contact information management
  - … Etc.

Issues of Importance

- There are many important issues in development of peer database systems
- Two are:
  - Data encryption
  - User authentication

Data Encryption

- In order to protect data from unauthorized viewing, it must be encrypted in transit and in storage
- Encryption ensures that sensitive or private data is kept private

User Authentication

- Working alongside data encryption to keep private information private is user authentication
- Only privileged users should have access to privileged data
  - Especially in healthcare!

Proposal

- I propose to determine the sate of security services in peer database systems such as DBGlobe and Edutella
- I propose to determine how authentication and encryption protocols can be applied to such systems

Proposal

- Milestones
  - Things I will achieve
    - Complete a thorough literature survey of peer database systems
    - Complete a thorough literature survey of authentication and encryption protocols
    - Complete a critical analysis of some selected peer database systems
    - Complete a critical analysis of some selected authentication and encryption protocols

Proposal

- Milestones
  - Things I plan to achieve
    - Complete a discussion of how selected authentication and encryption protocols might be applied, and how well they might perform with, selected peer database systems
    - Propose an experiment to implement some authentication and encryption protocols on top of some peer database systems as well as metrics to measure how well the systems perform under attack

Proposal

- Milestones
  - Things I might achieve
    - Complete a test implementation of some authentication and encryption services in a peer database system and determine if the security they provide is adequate to safeguard critical documents

Thank You

- Questions?