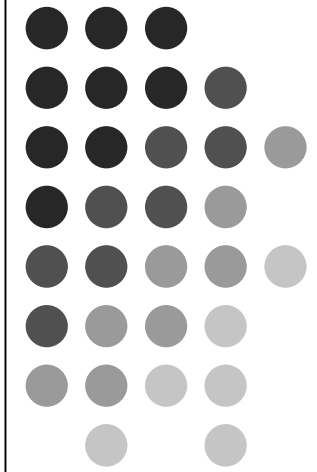
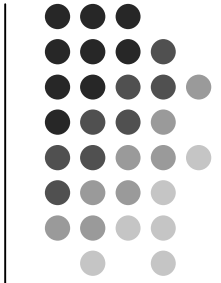
Future of Internet Applications
A Security Perspective



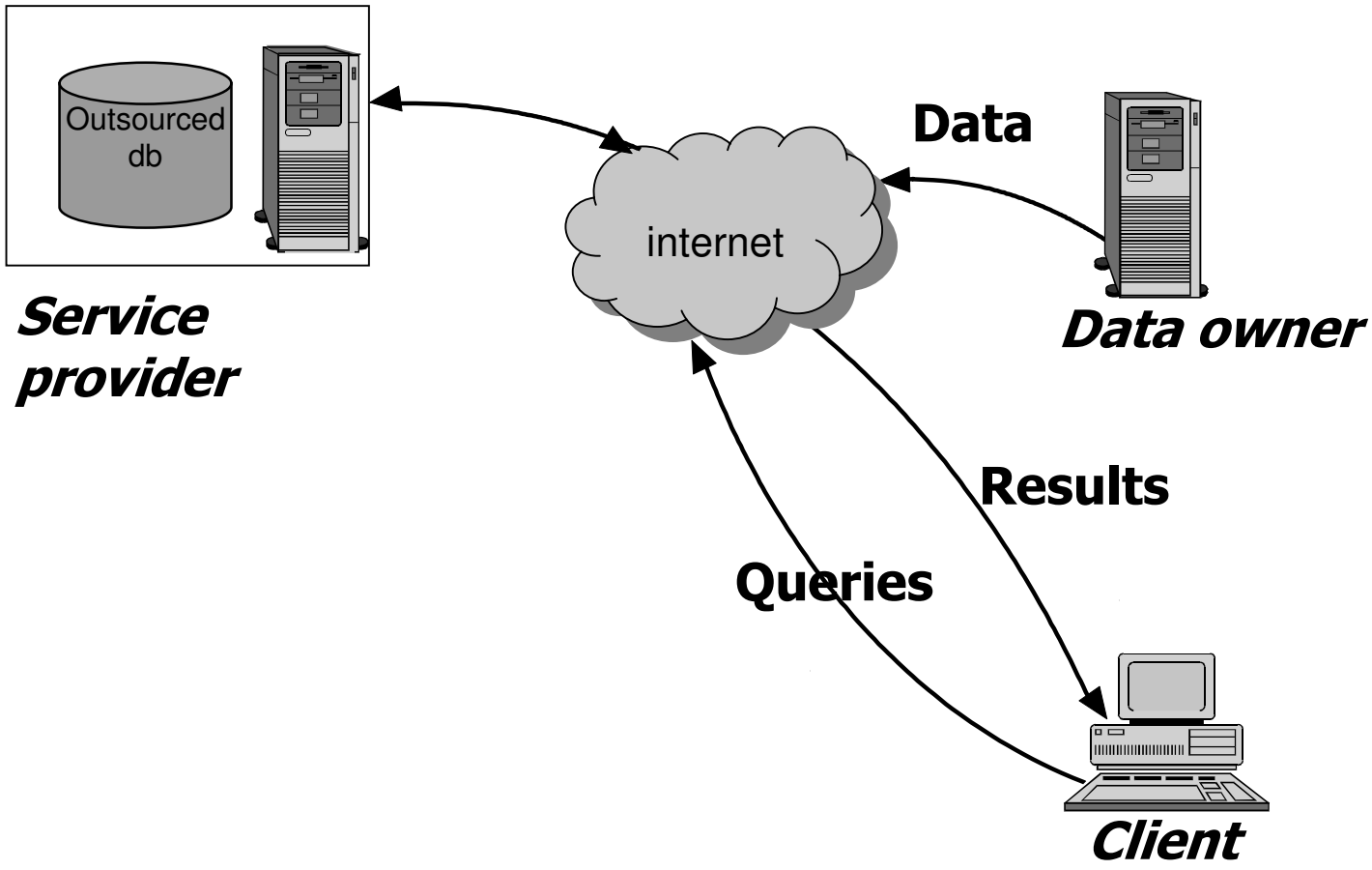
Elena Ferrari
University of Insubria at Como
elena.ferrari@uninsubria.it
http://scienze-como.uninsubria.it/ferrari

Emerging trend: data outsourcing

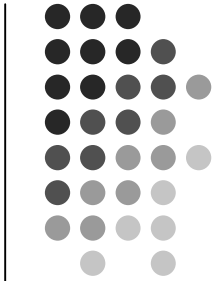


- Database as a service, why?
  - Most organizations need efficient data management
  - DBMSs are extremely complex to deploy, setup, maintain
  - require skilled DBAs (at very high cost!)

Database as a service

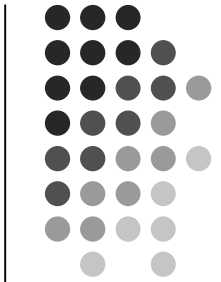


Database as a service



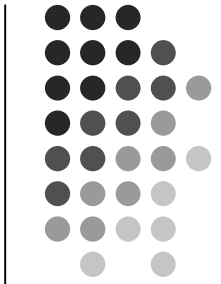
- Driven by faster, cheaper, and more accessible networks
- reduced cost to client:
  - pay for what you use and not for: hardware,software infrastructure or personnel to deploy, maintain, upgrade…
- reduced overall cost:
  - cost amortization across users
- better service
- scalability

Research Issues



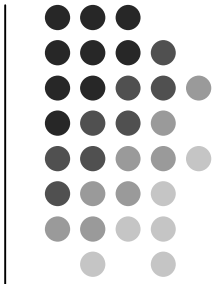
- **Economic/business model:**
  - How to charge for service, what kind of service guarantees can be offered, costing of guarantees, liability of service provider
- **Scalability in the web environment:**
  - Overhead costs due to network latency (data proxies?)
- **Security:**
  - Main requirements: confidentiality (privacy), integrity, authenticity, ownership protection

Security Properties



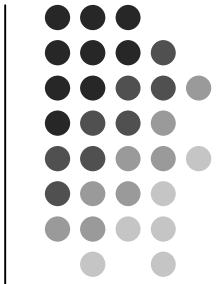
- To be satisfied even in the presence of an unstrusted service provider that:
  - Can modify/delete the data
  - Can access sensitive information
  - Can send the data to non authorized subjects
  - Can send a subject not all the information he/she is authorized to access
- To be satisfied by incurring minimal computation and bandwidth overhead

Possible solutions



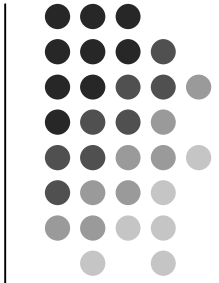
- **Encrypted databases:**
  - Encryption driven by the specified ac policies
  - Techniques for querying encrypted data
  - Key management
  - Data/policies updates
- **Non conventional digital signature techniques:**
  - Merkle Hash Trees, RSA extensions

Some references



- B. Carminati, E. Ferrari, E. Bertino. *Assuring Security Properties in Third Party Architecture.* Proc. of the International Conference on Data Engineering (ICDE'05).
- B. Carminati, E. Ferrari. Trusted Privacy Manager: A System for Privacy Enforcement on Outsourced Data. Proc. of the International Workshop on Privacy Data Management, Tokyo, Japan, April 2005.
- E. Bertino, B. Carminati, E. Ferrari, B. Thuraisingham, A. Gupta. *Selective and Authentic Third-party Distribution of XML Document*. IEEE Transactions on Knowledge and Data Engineering, 16(10): 1263-1278 (2004).
- Bertino, E. Ferrari. *Secure and Selective Dissemination of XML Documents*. ACM Transactions on Information and System Security (TISSEC) 5(3): 290-331, 2002.
- E. Bertino, B. Carminati, E. Ferrari. *A Flexible Authentication Method for UDDI Registres*. In Proc. of the 2003 International Conference on Web Services (ICWS'03), Las Vegas, June 2003.

Some references



- H.Hacigumus, B.Iyer, C.Li, and S.Mehrotra. *Executing SQL over Encrypted Data in the Database Service Provider Model*. In Proceedings of the SIGMOD Conference, 2002.
- M. Narasimha, E. Mykletun and G. Tsudik. Efficient Data Integrity in Outsourced Databases, NDSS 2004.
- H. Hacigumus, B. Iyer and S. Mehrotra. Providing Database as a Service, ICDE-2002