Processing Encrypted Data in the Cloud

Donald Kossmann
Systems Group
Department of Computer Science
ETH Zurich
Cloud Era

10011 01001 01100 11011 ...
Alternative 1: Data in the Cloud

- **Data are not encrypted**
  - Great to process the data in the cloud 😊
  - Little protection against attackers 😞
Honest & Curious Attackers

- Are interested in your data
- Are not interested in disrupting your service
- Often internal and powerful
  - may have root privileges to machines
- Several examples recently with huge impact
Alternative 2: Silos

• Data are encrypted
  – A great deal of protection against attackers. 😊
  – Processing data outside of cloud results in high cost. 😞
  – No way to integrate data from multiple owners. 😞
Cipherbase: Secure Co-processor

• Idea: Farm out computation on encrypted data to co-processor
• Most database work on commodity hardware (cheap & fast)
  – Logging, Locking / Synchronization, Buffer Management, Scheduling etc.
  – Expressions on encrypted or (partially) homomorphically encrypted data
• Secure co-processor evaluates expressions on encrypted data
  – Arithmetic, Comparisons and Intrinsics (MIN, MAX etc.)
  – Trusted Code Base easy to verify
Cipherbase: Use Case 1

- Data encrypted in the cloud. Good protection. 😊
- Data processed in the cloud: cheap & fast. 😊
• Donald, Joachim authorize Dirk for his query.
• Dirk only sees (aggregated) results. Dirk does not see base data.
• Donald, Joachim only see their own data.
• Scales to data from millions of users.
Why trust trusted Hardware?

• Three options
  – Dedicated co-processors: e.g., IBM 4970
  – Extensions to commodity processors: Intel SGX
  – Custom hardware: FPGAs

• We chose FPGAs
  – no operating system (less software to trust)
  – open source the layout
  – available and cheap
TPC-C Results

![Normalized Throughput Graph]

- **Plaintext**: Opt (1.0) NoOpt
- **Customer**: Opt (0.9) NoOpt (0.7)
- **Strong/Weak**: Opt (0.8) NoOpt (0.6)
- **Strong/Strong**: Opt (0.4) NoOpt (0.2)
Summary

• Goal: Generality, Performance, Security

• Only way to achieve goal today is with HW

• HW is becoming available

• Careful HW/SW co-design for good performance