Protection of Sensitive Data in Clouds
Using Active Privacy Bundles and Agent-Based Secure Multiparty Computation

Akram Y. Sarhan (Advisor: Prof. Leszek T. Lilien)
Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008

Introduction

- Challenges for protecting data in clouds (cf. TechInsights Report, 2013)
  - "Security" below includes privacy
    - Infrastructure readiness/network
    - Visibility into services across cloud
    - Contracts/liability concerns
    - Cultural/political issues
    - Performance/availability
  - Cost
  - Security
  - Privacy/Legal issues
- APB creation – cont.
  - Send APB to a cloud backup server
  - Store APB copy on the backup server
  - Send APB to cloud mediator
  - Send APB to a cloud backup server
- Problems with using TTPs
  - Bottleneck, insecure, single point of failure
- Solution components and their roles
- Two types of solutions for cloud-based privacy and security

Motivation and Objectives

- Providing adequate privacy and security for data in clouds
- Self-protecting data
- Fine-grained access control
- Fault tolerance
- Protect cloud data against attackers
  - Dishonest cloud providers
  - Unauthorized sub-contractors
  - Dishonest tenants (i.e., other cloud users)
- Protecting data with decentralized TTP (without centralized TTP)
  - Using multi-agent systems (MAS) for implementing decentralized TTPs
  - Using MAS for performance improvements
    - Thanks to parallel processing of data

Methods

- Solution components and their roles
- Active privacy bundle
- Secure multiparty computation
- Multi-agent systems
- Attribute-based encryption
- Secret sharing
- Verifiable secret sharing
- Polynomial interpolation

Major results

- Designed and partially developed the APB-SMC scheme
  - Integrated SMC into APB implementation
  - SMC uses RSA threshold cryptography and BGW protocol
  - APB-SMC replaces the centralized TTP with a distributed trust mediator
  - SMC used in constructing and enabling APB
  - Enhanced APB evaporation
  - Enhanced APB apoptosis
  - Integrated ABE and CP-ABE into APB-SMC
    - Provide higher security and fault tolerance
    - Support access right delegation and revocation

Results: The Proposed Solution

- APB creation and enabling algorithms in APB-SMC
  1) APB creation
    - Identify sensitive data
    - Create access policy attributes
    - Create access structure
    - Generate public and master keys
    - Encrypt sensitive data
    - Encrypt metadata
    - Hash and sign the APB
    - Encrypt APB
    - Plan APB itinerary
  2) APB enabling
    - APB host trust verification
    - APB permission
    - APB integrity verification
    - APB policy enforcement
    - APB decryption

Using APB-SMC to protect sensitive data in clouds

Conclusions

- Current work status
  - Completed design of the APB-SMC scheme
  - Working on modeling, formal model analysis, simulation experiments
- Future work
  - Demonstrate that APB-SMC provides privacy, security, fault tolerance, and efficiency
  - Integrate a multi-agent system (MAS) framework into APB-SMC
  - Validate and optimize MAS-based APB-SMC

Data Owner

Mediator

SP

Backup Server

CS

SPA

SP2

SP3

SAAS

Bob

Alex

PK

DA