A Flexible and Secure Shared Object Storage Service for the Cloud

Brian Laub and Douglas M. Blough
CERCS, Georgia Institute of Technology

Motivation and Objectives
• Storing sensitive data in the cloud remains challenging – high redundancy exposes data to threats from cloud admin, multi-tenancy.
• Build a service that provides flexible options for storing and operating on sensitive data in the cloud.
• Use data encoding and virtualization to secure information on shared infrastructure; give users control over levels of security for data.

Flexible support for dynamic data encoding
• Support multiple data encoding schemes through plugin API; encoders transform objects into fragments, stored independently in the cloud.
• Storage zone hierarchies provide data isolation across admin domains and physical cloud resources.
• Placement strategy intelligently maps fragments to zones with constraints.
• Encoding plugins provide flexible tradeoffs for security, efficiency, high availability.

Protected Memory – Keep sensitive data secure on virtualized infrastructures
• Virtualized servers use Protected Memory Area (PMA) – pages allocated by hypervisor to guest that root domain cannot access through standard management toolchain.
• Protection from threats originating within the cloud administrative domain – malicious software or “honest but curious” admins.

Data placement constraints secure data-at-rest
• Zone placement strategy optimizes allocation of encoded fragments to storage zones to ensure isolation and data security.
• Geographic distribution and hardware-separation between zones protects data from failures in cloud infrastructure (replication, erasure codes).
• Threshold encoding strategies used to minimize information leakage (secret sharing).
• Future efforts will investigate constraint-based programming for optimal fragment placement.

Managing object encoding as a service
• Cloud service encodes/decodes objects; metadata mapping fragments to zones is encrypted and persisted in the cloud.
• Clients manage master encryption keys in a Trusted External Key Store; encoding service granted access only when needed.
• Encoding service uses PMA on virtualized servers in the cloud to protect data during fragmentation and recovery.

Use case: sharing encryption keys in the cloud
• Allow clients to share and operate on encrypted data stored in the cloud.
• (k,n) threshold secret sharing scheme to encode encryption key; shares are stored across zones.
• Clients share access to fragments and metadata via ACLs.
• Keys recovered from shares within PMA and sent to clients via HTTPS.
• Clients keep keys secured within PMA on virtualized servers.

Current Implementation and Future Work
• Modified OpenStack Swift object store to implement service-managed encoding in proxy server.
• Developed and deployed on GT “Jedi” IaaS research cloud infrastructure.
• Encoders for replication, secret sharing and forward erasure codes (decoding in progress).
• Fragments assigned to nodes using Swift’s consistent hashing algorithm.
• Future work involves:
  • Evaluation of encoding plugins.
  • Development and evaluation of efficient zone placement algorithms.
  • Evaluation of efficiency and security on large-scale cloud deployment with real applications.

Managed object encoding as a service
• Cloud service encodes/decodes objects; metadata mapping fragments to zones is encrypted and persisted in the cloud.
• Clients manage master encryption keys in a Trusted External Key Store; encoding service granted access only when needed.
• Encoding service uses PMA on virtualized servers in the cloud to protect data during fragmentation and recovery.

Use case: sharing encryption keys in the cloud
• Allow clients to share and operate on encrypted data stored in the cloud.
• (k,n) threshold secret sharing scheme to encode encryption key; shares are stored across zones.
• Clients share access to fragments and metadata via ACLs.
• Keys recovered from shares within PMA and sent to clients via HTTPS.
• Clients keep keys secured within PMA on virtualized servers.

blaub6@gatech.edu / doug.blough@ece.gatech.edu