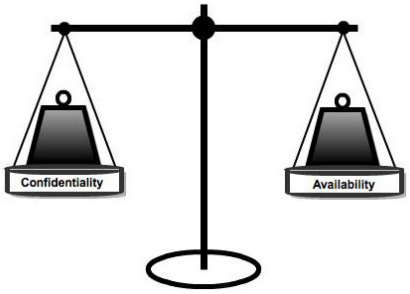
Cloud Security and Insider Attacks

By Frank Warnock, Supervisor: Prof. Hamzeh Roumani

Computer Science and Engineering, York University

The Problem

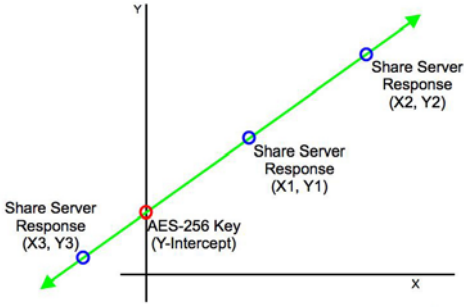
The threat of attacks from within a host's security perimeter is one of the many concerns introduced by cloud storage.



Increasing security measures in the pursuit of confidentiality often leads to a decrease in availability. Reducing the number of parties with access to the encryption key, for example, greatly increases the chances that the key becoming unobtainable.

The Solution*

By implementing a secret sharing scheme, the threat posed by a malicious party inside the security perimeter is greatly reduced without impacting the availability of the data to the end user.



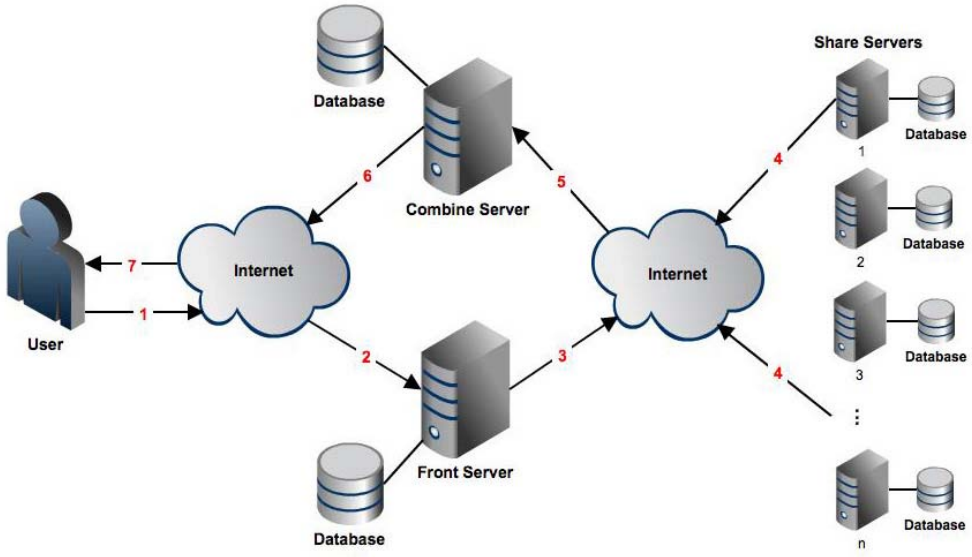
The key is interpreted as the y-intercept of a straight line, whose points are distributed among multiple parties. The benefits of this approach include:

- Defense against a single rogue employee: knowing any one point does not reduce the entropy of the key, whereas knowing two reduces it to zero.
- Availability through redundancy: even if n – 2 nodes are unresponsive, the key can still be recovered.

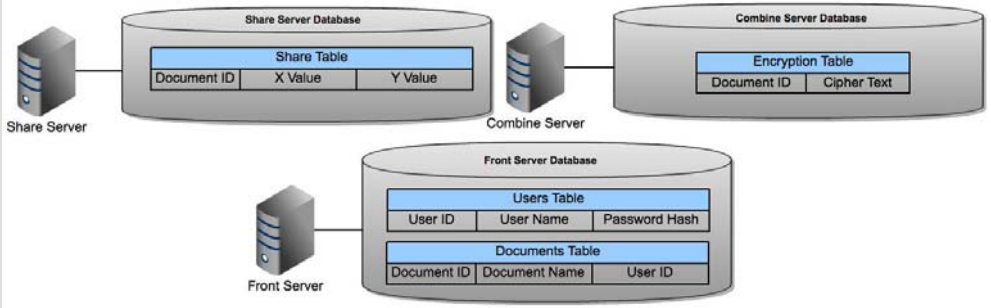
*Based on the works of Adi Shamir and George Blakley (1979).

My Implementation

The system is comprised of three main components: the Front Server, the Share Servers and the Combine Server. By utilizing the components in the system as outlined in the operating sequence below, confidentiality can be maintained without impacting availability.

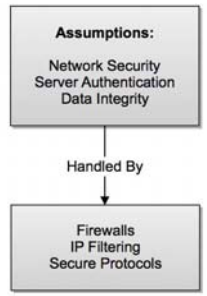


1. User requests a document stored within the cloud
2. Front Server captures the request, extracting the document ID from the payload
3. Front Server dispatches a request to the available Share Servers containing the requested document ID and a nonce
4. Available Share Servers send a request to the Combine Server with data points for the requested document, the document ID and the nonce
5. Combine Server captures the first two requests it receives for a given document ID/nonce combination
6. Combine Server calculates the key and decrypts the requested document
7. User is redirected to the Combine Server which verifies the document ID and nonce provided, returning the plain text data to the user



Threat Model

The main threat present from an insider attack is access to the encryption key by a malicious party within the security perimeter.

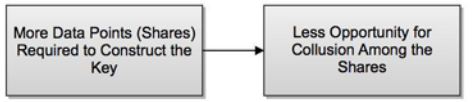


The above concerns are to be handled by existing safeguards. Hence, they fall outside the scope of this implementation.

Future Work

Utilizing a Polynomial or Plane:

The system described operates on the principle that two points are required to determine the y-intercept of a line. A system that requires that more than two points are needed to construct the key (i.e. a polynomial or plane) may be developed.



Accounting for Collaboration Between Users:

Augmenting the Front Server database with a table linking user IDs to document IDs may be implemented. This approach would allow for the grouping of users based on each distinct document promoting collaboration between users.

Byzantine Fault Tolerance:

Detection measures may be implemented allowing for the detection of so called Byzantine failures. This would be beneficial in situations where the Share Servers are returning improper data points as a result of one or more compromised nodes.