O

NOT TRUSTED

Owns/maintains

Database 1

Raw data

(encrypted)

Owns/maintains

Cloud service 2

Cloud service 1

Database 2

relational

TRUSTED

3

decision forwarder

2

7

6

5

4

1,8

Local software

Take query and gets key

Then pulls data from table(s)

Within DB1 each table is encrypted using ABE, table names are also encrypted

DB2 stores all the user keys for the ABE system encrypted as well as the keys to access the keys

Process for data retrieval:

1: user provides a query to the local software

2:local software sends query and key to middle man, and key request to cloud service 2

2A:Middle man waits for conformation form CS2

3:CS2 retrieves users decrypt key

4: and sends to MM

5:MM forwards query to CS1

5A:MM waits for query return

6:CS1 retrieves encrypted data and sends to MM

7:MM decrypts with CS2 key and re-encrypts with user key(or something like Diffie Hellman exchange)

8::MM returns to software and then to user

Point to point communication can use AES or similar encryption communication

MM – decision forwarder

A system that only forwards messages from specific addresses and only to one destination

CS2 key +Diffie Hellman+ user key = CS1 decrypt key

Focus of the project is the decision forwarder to help realize encryption based access control

SELECT - extracts data from a database.

UPDATE - updates data in a database.

DELETE - deletes data from a database.

INSERT INTO - inserts new data into a database.

CREATE DATABASE - creates a new database.

ALTER DATABASE - modifies a database.

CREATE TABLE - creates a new table.

Steps for select:

User writes query and sends to decision forwarder

decision forwarders request relevant tables from DB2

decision forwarder uses response from DB2 and request that info from DB1 + unused requests

return results to user

Steps for update:

User writes query and sends to decision forwarder

decision forwarders request relevant tables from DB2

decision forwarder uses response from DB2 and user query and send new encrypted data to DB1

Steps for delete:

User writes query and sends to decision forwarder

decision forwarder requests relevant tables from DB2

decision forwarder uses response from DB2 and user query to have DB1 mark data as empty