A machine learning application for reducing the security risks in hybrid cloud networks

Usman Kuramshin, 20121

Outline:

Introduction

Objectives

Methodology

Results and conclusion

References

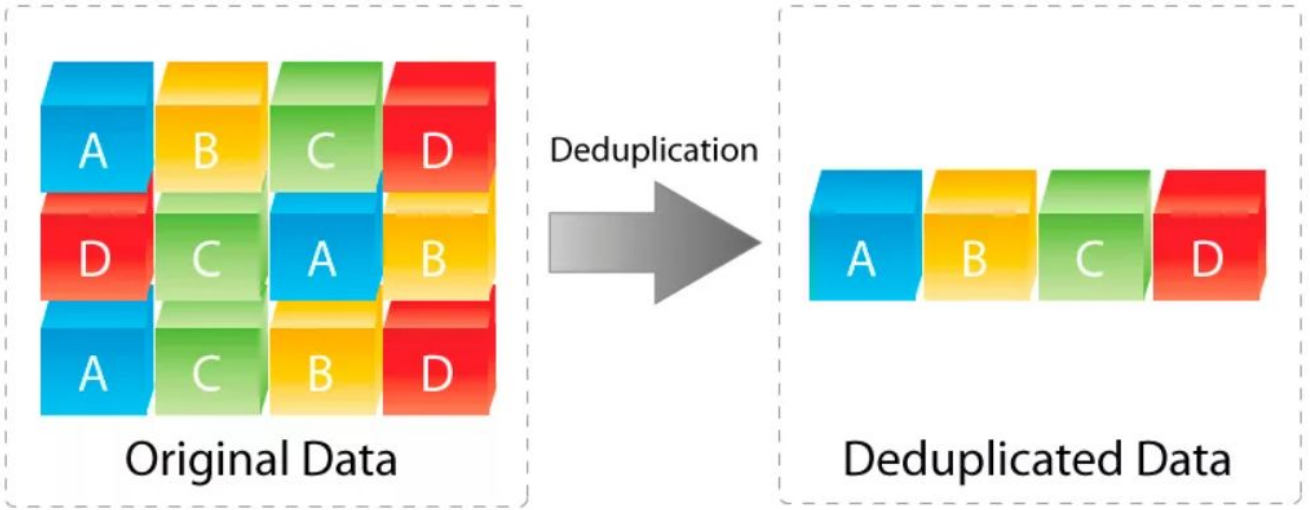
Introduction

Cloud computing facilitates enormous support of the public, business and emerging applications.

Introduction

In cloud network environment, the data security is playing crucial roles.

Deduplication process

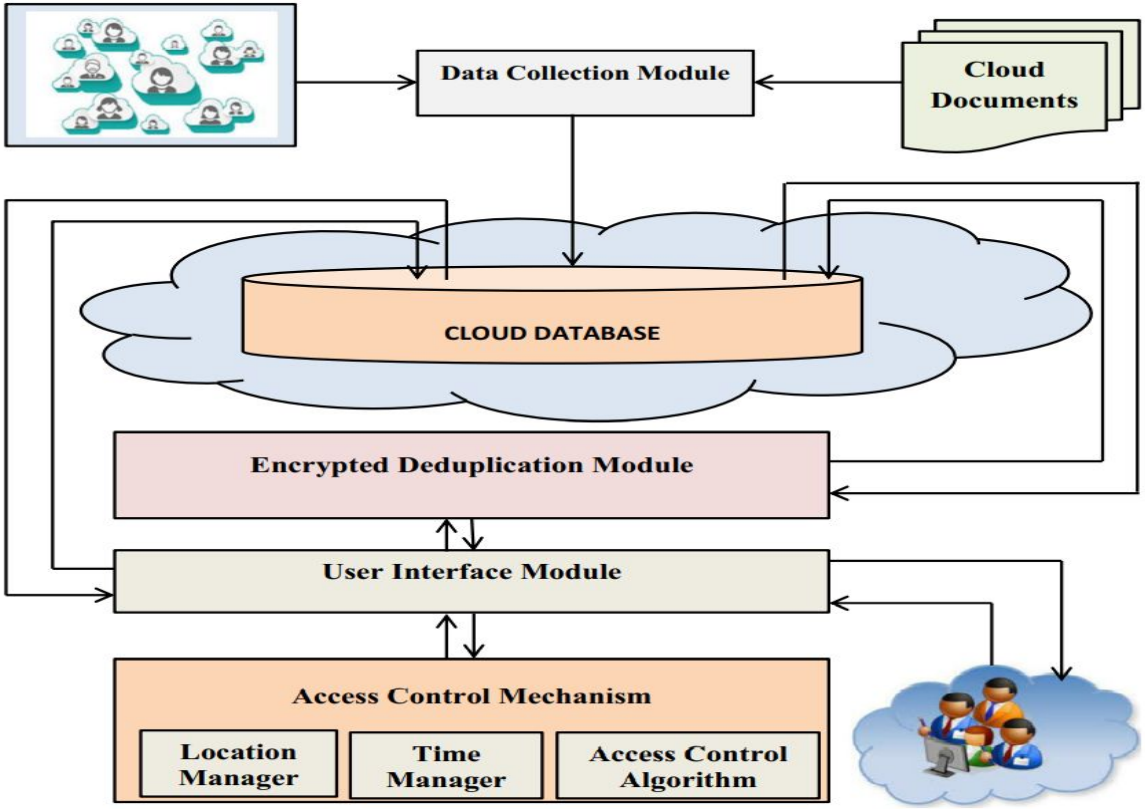


Objectives

- Introduce a new access control mechanism which is working dynamic in nature that is based on time and place.

- Create a new deduplication process for storing the data securely and also for avoiding the data duplication during the retrieval process

System architecture



Proposed work

DDPA

DSRBACA

DDPA:

Deduplication Processing Algorithm

Input: User Data / Documents
Output: Encrypted data

Phase 1: Similarity Analysis

Step 1: Read the first document from the database.
Step 2: Read the first line from the first document
Step 3: Check the similarity for the first line with other lines of the document.
Step 4: Calculate the similarity score using Cosine similarity formula.
Step 5: If the similarity score is above 60 then remove the particular line from the document.
Step 6: Remove the documents which are having more similar contents.
Step 7: Store the remaining documents in Hashtable in a secured manner using SHA-512

DDPA:

Phase 2: Encryption

Step 1: Read the content of a document from the database using the hash-indexed value
Step 2: Apply RSA algorithm for encrypting the content.
Step 3: Add the secret key over the content
Step 4: Store it as encrypted content into the database using hash along with the key.
Step 5: End

Dynamic spatial role based access control algorithm

DSRBACA:

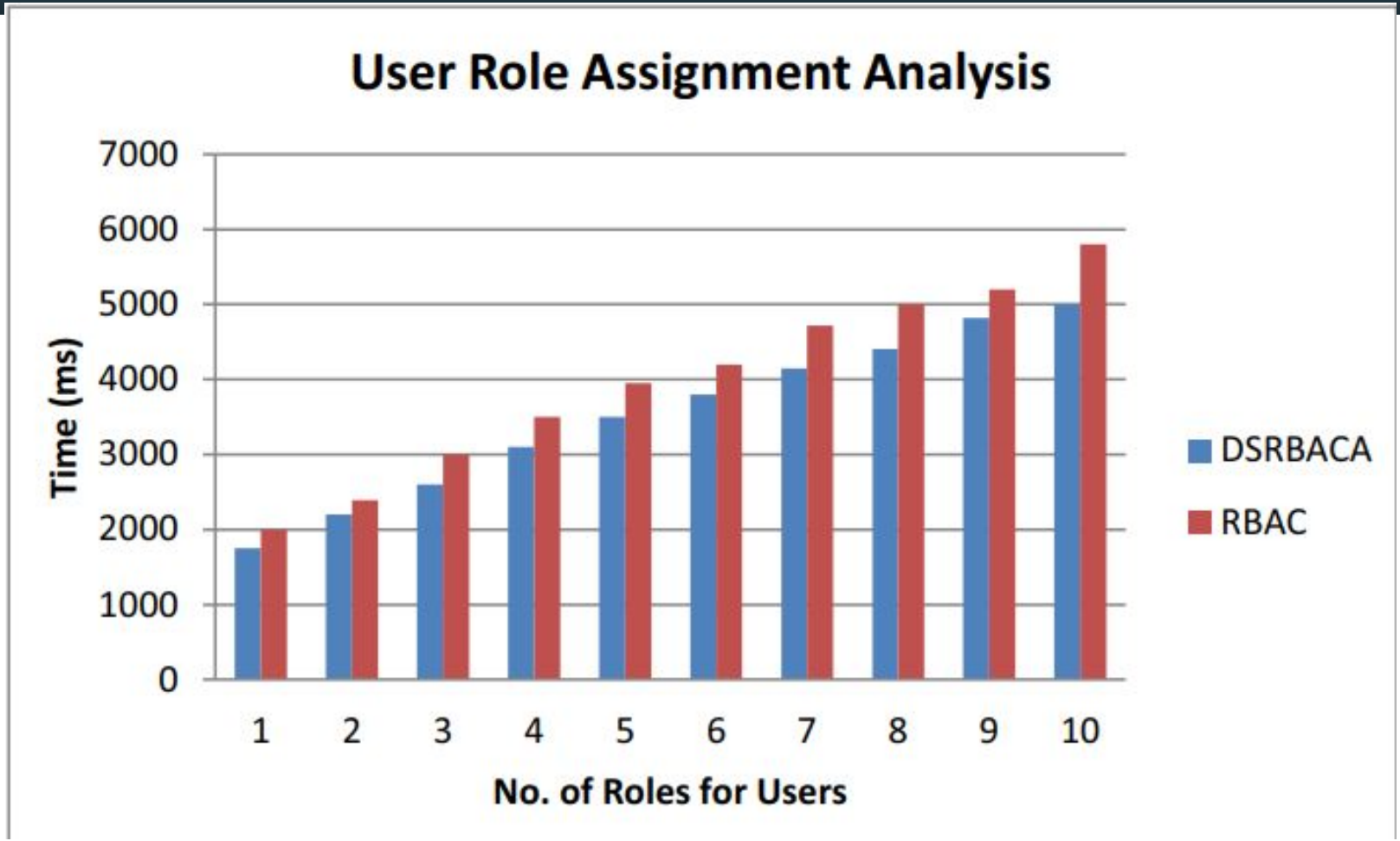
Input : Encrypted Data

Output: Original Data accessed by Cloud users

Step 1: Read the user queries from cloud users
Step 2: Initialize the user queries in queue
Step 3: Read the cloud users queries from the queue for accessing the data
Step 4: While (Queue != Empty)
Begin
Step 5: Read the next users request from the queue
Step 6: Check the cloud user query by using the user level and the database access privileges
Step 7: If the user level is greater than 5 then
Step 8: Check the user rights using time and space to assign the suitable role
Step 9: The user level is updated based on the time and space
Step 10: If the cloud user is a valid user and the rights are stored already for the cloud users in the past query by checking the time and spatial constraints
Step 11: If the cloud user is valid then
Identify the position where the address of the data stored in the hash table
Read the content and key from the respective position
Apply RSA for decrypting the stored encrypted data
Display the original data
Else
Display the SORRY message to the cloud user.
Step 12: Repeat the steps 4 to 11 until the queue become empty.
Step 13: End

Table 1 User Requests Denied Analysis

Exp. No	No. of User Request Tried	No. of requests denied by	
		RBAC	DDPA + DSRBACA
1	100	5	6
2	200	9	10
3	300	13	15
4	400	17	19
5	500	22	20


User Role Assignment Analysis
7000
6000
5000
4000
3000
2000
1000
0
Time (ms)
1
2
3
4
5
6
7
8
9
10
No. of Roles for Users
DSRBACA
RBAC

Results and conclusion

A new machine learning application has been developed for providing security to the hybrid cloud networks while storing the data and retrieving or accessing the data from cloud databases.

References

1. Alabdulatif A, Kumarage H, Khalil I, Yi X (2017) Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption. J Comput Syst Sci 90:28–45

2. Elumalaivasan P, Kulothungan K, Ganapathy S, Kannan A (2016) Trust based Ciphertext policy attribute based encryption techniques for decentralized disruption tolerant networks. Aust J Basic Appl Sci 10(2):18–26

3. Gordon A (2016) The hybrid cloud security professional. IEEE Cloud Comput 3(1):82–86

4. Helmi AM, Farhan MS, Nasr MM (2018) A framework for integrating geospatial information systems and hybrid cloud computing. Comput Electr Eng 67:145–158

5. Hudic A, Smith P, Weippl ER (2017) Security assurance assessment methodology for hybrid clouds. Comput Sec 70:723–743

Thank you for your attention!