LOGO

CHƯƠNG 4

ỨNG DỤNG MẬT MÃ TRONG AN TOÀN CSDL

TS. Trần Thị Lượng
* Khoa An toàn thông tin *

NỘI DUNG

1. Đảm bảo an toàn CSDL bằng mật mã
2. Mã hóa CSDL trong các DBMS
3. Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

NỘI DUNG

1. Đảm bảo an toàn CSDL bằng mật mã
2. Mã hóa CSDL trong các DBMS
3. Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖ 4.1.1. Giới thiệu

An toàn cơ sở dữ liệu có thể được mô tả bằng các tính chất sau:

- Bí mật: Không thể truy cập được thông tin đối với người dùng không hợp lệ.
- Toàn vẹn: Dữ liệu không bị sửa đổi sai lệch, chỉ có người dùng hợp lệ mới có thể sửa đổi dữ liệu.
- Sẵn sàng: Người dùng hợp lệ có thể truy cập vào dữ liệu đáng tin cậy ở tất cả mọi thời điểm.

❖ 4.1.1. Giới thiệu

Mã hóa dữ liệu có thể cung cấp độ an toàn rất mạnh cho dữ liệu lưu trữ nhưng có nhiều yếu tố cần được xem xét trước khi mã hóa cơ sở dữ liệu, chẳng hạn:

- Dữ liệu nên được mã hóa bởi DBMS hay bởi ứng dụng đã tạo ra chúng?
- Ai có thể giải mã dữ liệu?
- Các tác động đến hiệu suất trên DBMS như thế nào?
- Có phải tất cả dữ liệu đều cần được mã hóa không?

Đảm bảo an toàn CSDL bằng mật mã

❖ 4.1.1. Giới thiệu

- Hai yêu cầu chính liên quan đến mã hóa dữ liệu.
  - ▪ Công nghệ mã hóa an toàn để bảo vệ dữ liệu nhạy cảm.
  - ▪ Chương trình quản lý và tạo khóa đáng tin cậy.
- Mục đích của mã hóa CSDL:
  - ▪ Đảm bảo tính không trong suốt của CSDL bằng cách giữ thông tin được ẩn với bất kì người nào không có thẩm quyền
  - ▪ Bảo vệ được tính bí mật của dữ liệu lưu trữ.

❖ 4.1.2. Lợi ích, nguyên tắc và tác động của mã hóa

- Mã hóa cơ sở dữ liệu mang lại những lợi ích sau:

▪ Bảo đảm tính bí mật cho cá nhân và tổ chức

▪ Phương pháp đơn giản, hiệu quả nhất đáp ứng các yêu cầu của tổ chức.

▪ Bảo đảm an toàn cho dữ liệu có giá trị nhất của tổ chức.

▪ Nâng cao bảo vệ và giảm rủi ro an toàn cho dữ liệu.

▪ Góp phần bảo đảm an toàn cho hoạt động của tổ chức.

▪ Duy trì tính cạnh tranh.

▪ Bảo đảm an toàn cho dữ liệu outsource.

▪ Đáp ứng các yêu cầu và quy định quản trị.

❖ 4.1.2. Lợi ích, nguyên tắc và tác động của mã hóa

- Nguyên tắc mã hóa:

▪ Để mã hóa dữ liệu, các khóa ngẫu nhiên được sử dụng. Các khóa tương ứng được sử dụng để giải mã dữ liệu.

▪ Tính bảo mật của dữ liệu được mã hóa phụ thuộc vào thuật toán mã hóa được sử dụng, khóa, kích thước khóa và việc thực hiện thuật toán mã hóa.

❖ 4.1.2. Lợi ích, nguyên tắc và tác động của mã hóa

- Tác động của mã hóa dữ liệu

▪ Mã hóa dữ liệu thường có thể ảnh hưởng nghiêm trọng đến hiệu suất nếu không có kế hoạch khôn ngoan về chiến lược mã hóa.

▪ Mã hóa và giải mã dữ liệu chắc chắn sẽ gây ra một số suy giảm hiệu suất do bản chất của tính toán mã hóa, tùy thuộc vào lượng dữ liệu được mã hóa, thuật toán mã hóa và kích thước khóa.

❖ 4.1.3. Các chiến lược mã hóa cơ sở dữ liệu

- Dữ liệu sẽ được mã hóa ngay sau khi chúng được lưu trữ
- Lợi thế của chiến lược mã hóa này là nó trong suốt đối với các ứng dụng, do đó không cần thay đổi đối với các ứng dụng.

❖ 4.1.3. Các chiến lược mã hóa cơ sở dữ liệu

4.1.3.1. Mã hóa bên trong DBMS

Có hai dạng sau:

- Mã hóa mức lưu trữ
- Mã hóa mức cơ sở dữ liệu

❖ 4.1.3. Các chiến lược mã hóa cơ sở dữ liệu

4.1.3.1. Mã hóa bên trong DBMS

- Mã hóa mức lưu trữ

  - Thực hiện mã hóa dữ liệu là mã hóa dữ liệu trong hệ thống lưu trữ phụ (mã hóa toàn bộ tệp và thư mục và bảo vệ dữ liệu lưu trữ).
  - Chiến lược mã hóa này không thể liên quan đến đặc quyền của người dùng.

❖ 4.1.3. Các chiến lược mã hóa cơ sở dữ liệu

4.1.3.1. Mã hóa bên trong DBMS

- Mã hóa mức cơ sở dữ liệu

- Mã hóa này có thể liên quan đến lược đồ cơ sở dữ liệu (có thể được mã hóa ở cấp độ bảng, hàng hoặc cột.)
- Mã hóa ở mức cơ sở dữ liệu có thể làm giảm hiệu suất vì nó phức tạp ở việc lập chỉ mục dữ liệu được mã hóa.

❖ Các chiến lược mã hóa cơ sở dữ liệu

4.1.3.2. Mã hóa bên ngoài DBMS

- Nếu cần mã hóa dữ liệu trong quá trình truyền thì một giải pháp phù hợp hơn là mã hóa dữ liệu bên ngoài DBMS ở mức ứng dụng. Do đó, dữ liệu được truyền dưới dạng văn bản mã và được lưu trữ, truy xuất từ DBMS ở dạng mã hóa.

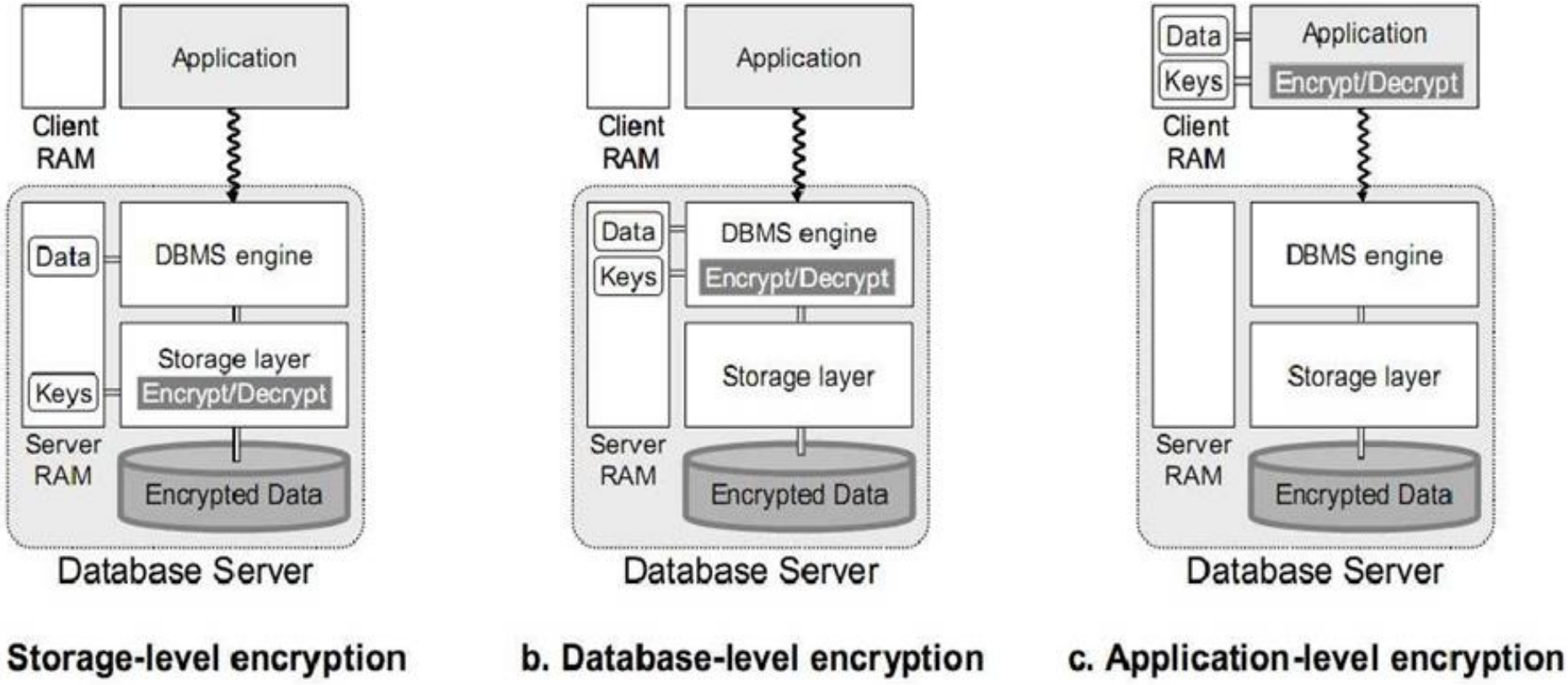
❖ Các chiến lược mã hóa cơ sở dữ liệu

4.1.3.2. Mã hóa bên ngoài DBMS

- Giải pháp này mang đến sự linh hoạt về thuật toán mã hóa có thể làm giảm chi phí hoạt động và tăng tính bảo mật.
- Ngoài ra, giải pháp này có khả năng mở rộng cao liên quan đến số lượng người dùng và cơ sở dữ liệu được mã hóa (nghĩa là người ta có thể thêm nhiều cơ sở dữ liệu mà không cần sửa đổi máy chủ mã hóa).

Đảm bảo an toàn CSDL bằng mật mã

❖ Các chiến lược mã hóa cơ sở dữ liệu



Ba chiến lược mã hoá cơ sở dữ liệu

❖ Quản lý khóa

Cần xem xét các vấn đề sau:

- Nơi các khóa được lưu trữ và ai có quyền truy cập vào chúng.
- Số lượng khóa mã hóa, giới hạn cho người dùng được ủy quyền và tần suất các khóa nên thay đổi

❖ 4.1.5. Ứng dụng mật mã bảo vệ CSDL

4.1.5.1. Bảo vệ tính bí mật

Khi dữ liệu nhạy cảm bị truy cập trái phép thì tính bí mật bị vi phạm

- Truy cập trực tiếp: truy cập vào chính khóa dùng để mã hóa dữ liệu.
- Truy cập gián tiếp: là truy cập vào một ứng dụng hoặc dịch vụ có quyền truy cập vào khóa.
- Việc kiểm soát chặt chẽ truy cập trực tiếp vào khóa có thể kiểm soát, tuy nhiên việc kiểm soát truy cập gián tiếp vào khóa sẽ khó khăn hơn.
- Việc bảo vệ chống lại các quản trị viên có quyền truy cập đầy đủ vào cơ sở dữ liệu hoặc máy chủ ứng dụng là vấn đề quan trọng trong kiểm soát truy cập gián tiếp vào các khóa

❖ Ứng dụng mật mã bảo vệ CSDL

4.1.5.1. Bảo vệ tính toàn vẹn

- Mật mã giúp phát hiện và ngăn chặn sự sửa đổi trái phép dữ liệu.

=> Giải pháp:

- Chỉ cần mã hóa thông tin bằng mật mã khóa đối xứng
- Sử dụng mã xác thực thông báo (MAC).

Đảm bảo an toàn CSDL bằng mật mã

❖ **Các rủi ro khi mã hóa:**

- Rủi ro bị mất khóa
  - ▪ Khi khóa bị mất thì bất kỳ dữ liệu nào được mã hóa bằng khóa đó cũng sẽ bị mất.
  - ▪ Điểm yếu quy trình quản lý khóa có thể gây nguy hiểm cho an toàn tổng thể.
- Rủi ro khi thực thi
  - ▪ Nếu dữ liệu khác được sử dụng trong quá trình mã hóa, có thể sẽ nhận ra các mẫu trong dữ liệu được mã hóa và có thể suy ra dữ liệu thực.

Đảm bảo an toàn CSDL bằng mật mã

❖ **Các rủi ro khi mã hóa:**

- Truy cập khóa gián tiếp:

- Thiết kế hệ thống mật mã để đảm bảo rằng các khóa không bao giờ có sẵn bên ngoài mã lệnh sử dụng chúng.
- Hệ thống mật mã được bảo vệ bởi các điều khiển truy cập mạnh đòi hỏi xác thực và ủy quyền cho mỗi lời gọi giải mã.
- Honeycombing là một kỹ thuật có giá trị chống lại tấn công thỏa hiệp giải mã. Honeycombs có vai trò như hũ mật đối với các ứng dụng và cơ sở dữ liệu giống như trong các hệ thống mạng.

NỘI DUNG

1. Đảm bảo an toàn CSDL bằng mật mã
2. Mã hóa CSDL trong các DBMS
3. Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖ 4.2.1. Một số dạng thuật toán mã hóa CSDL

- **Mã hóa đồng cấu riêng tư**: tính toán được thực hiện trên văn bản mật và thu được kết quả khớp với các tính toán được thực hiện trên văn bản rõ.
- **Mã hóa bảo toàn thứ tự**: xây dựng các chỉ mục trên văn bản mã và để so sánh trực tiếp trên dữ liệu mã.
- **Mã hóa so sánh nhanh**: so sánh nhanh thông qua kỹ thuật giải mã từng phần, mã hóa văn bản rõ theo byte (byte by byte) cho phép so sánh nhanh bắt đầu từ byte đánh dấu và dừng ngay khi tìm thấy sự khác biệt.

Mã hóa CSDL trong các DBMS

LOGO

❖ 4.2.2. Ứng dụng mã hóa trong DBMS

- Một số tính năng mã hóa trong các DBMS hiện đại bao gồm:
  - Mã hóa lưu trữ mật khẩu
  - Mã hóa chọn lọc
  - Mã hóa phân vùng dữ liệu
  - Mã hóa mật khẩu qua mạng
  - Mã hóa dữ liệu qua mạng

❖ 4.2.2. Ứng dụng mã hóa trong DBMS

Các hệ quản trị CSDL thường được phát triển theo hai hướng:

- Hướng thứ nhất: các hệ quản trị CSDL mã nguồn mở: MySQL, PostgresSQL, v.v.

Mã hóa CSDL trong các DBMS

LOGO

Ví dụ: hệ quản trị MySQL đã được phát triển thành hệ quản trị có bảo mật để giải quyết được các bài toán chính:

1) bảo mật dữ liệu lưu trữ;

2) bảo mật dữ liệu trên đường truyền;

3) bảo mật dữ liệu trong quá trình sao lưu;

4) xác thực và phân phối khóa cho người sử dụng;

5) hỗ trợ giao diện có hỗ trợ mật mã.

❖ 4.2.2. Ứng dụng mã hóa trong DBMS

- Hướng thứ hai: các hệ quản trị CSDL thương mại: Oracle, SQL Server, DB2, v.v.

Ví dụ: Hệ quản trị Oracle hỗ trợ các gói công cụ DBMS_ OBFUSCATION_ TOOLKIT ,cho phép sử dụng các thuật toán DES, 3DES (2 khóa hoặc 3 khóa) để thực hiện các thủ tục mã hóa và giải mã. Vì vậy, người phát triển sản phẩm có thể xây dựng các giải pháp bảo mật CSDL cho các ứng dụng cụ thể.

Mã hóa CSDL trong các DBMS

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

Khái niệm: Là một trong những cơ chế an toàn cho phép mã hóa dữ liệu nhạy cảm được lưu trữ trong bảng và không gian bảng. Dữ liệu được mã hóa và giải mã trong suốt đối với người dùng và các ứng dụng có quyền truy cập vào dữ liệu

Ví dụ: Bảo vệ dữ liệu bí mật, chẳng hạn như thẻ tín dụng và số an sinh xã hội.

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

Lợi ích:

- Các quản trị viên có thể chắc chắn rằng dữ liệu nhạy cảm được đảm bảo an toàn trong trường hợp phương tiện lưu trữ hoặc tệp dữ liệu bị đánh cắp.
- Giải quyết các vấn đề tuân thủ quy định liên quan đến an toàn.

❖4.2.3. Mã hóa dữ liệu trong suốt (TDE):

Lợi ích:

- Dữ liệu từ các bảng được giải mã trong suốt cho người dùng và ứng dụng cơ sở dữ liệu.
- Dữ liệu được giải mã trong suốt cho người dùng và ứng dụng cơ sở dữ liệu.
- Các ứng dụng không cần phải sửa đổi để xử lý dữ liệu được mã hóa
- Hoạt động quản lý được tự động hóa

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

Hạn chế

- Ảnh hưởng đến hiệu năng:
  - TDE ảnh hưởng đến hiệu năng chỉ khi dữ liệu được tác động bởi các câu truy vấn trên các cột dữ liệu được mã hóa.
- Ảnh hưởng đến lưu trữ:
  - Việc mã hóa mỗi cột sẽ cần thêm 32 đến 48 byte không gian lưu trữ cho mỗi hàng (tính trung bình).

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong SQL Server:**

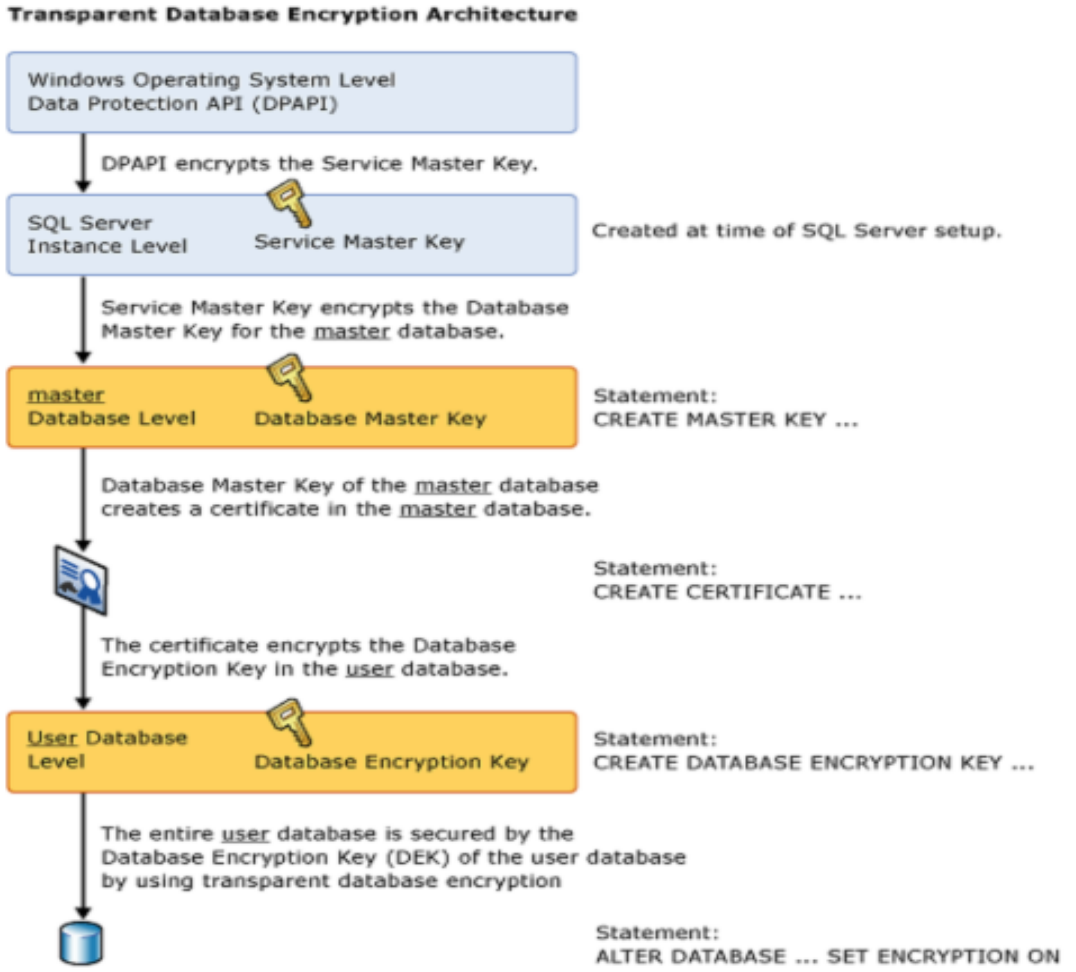
TDE cung cấp khả năng mã hóa toàn bộ cơ sở dữ liệu và quá trình mã hóa hoàn toàn trong suốt cho ứng dụng truy cập cơ sở dữ liệu. TDE mã hóa dữ liệu được lưu trữ trong cả hai tệp cơ sở dữ liệu (.MDF) và tập log (.LDF) bằng cách sử dụng thuật toán mã hóa AES hoặc 3DES.

Mã hóa CSDL trong các DBMS

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong SQL Server:**

  - Kiến trúc của mã hóa TDE trong SQL Server



4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong SQL Server:**

Các bước để mã hóa một CSDL:

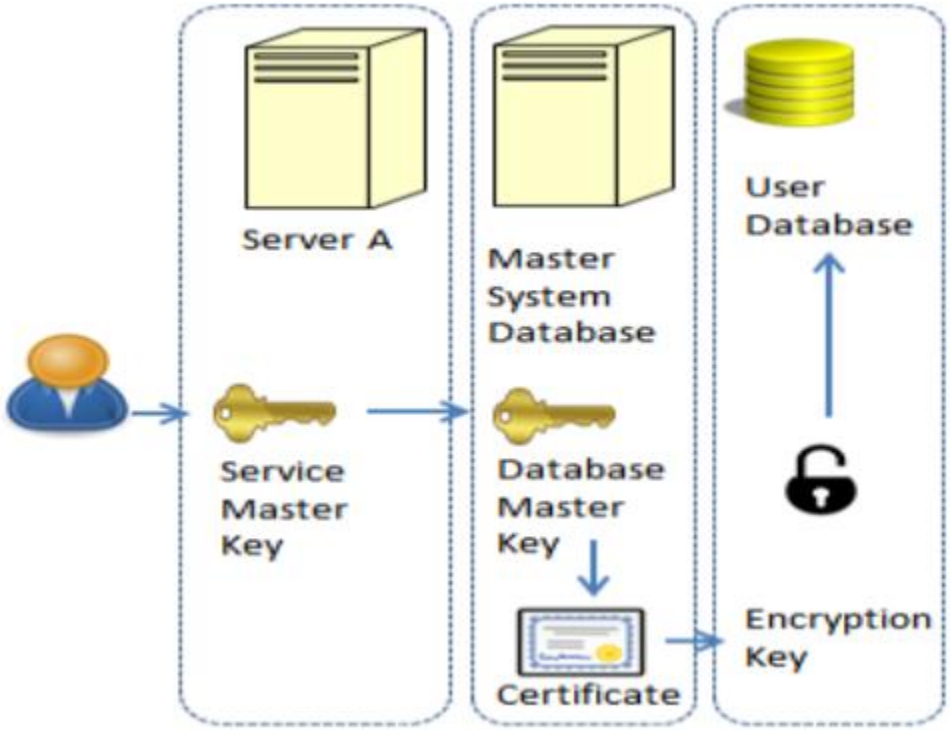
- Tạo một khóa chủ của cơ sở dữ liệu, đó là khóa DMK.
- Tạo một chứng chỉ được bảo vệ bằng khóa DMK.
- Tạo một khóa đặc biệt được sử dụng để bảo vệ cơ sở dữ liệu. Khóa này được gọi là khóa mã cơ sở dữ liệu (DEK) và chúng ta bảo vệ nó bằng cách sử dụng chứng chỉ.
- Thực hiện mã hóa.

Mã hóa CSDL trong các DBMS

❖4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong SQL Server:**

- Hệ thống phân cấp mã hóa TDE



❖4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong SQL Server:**

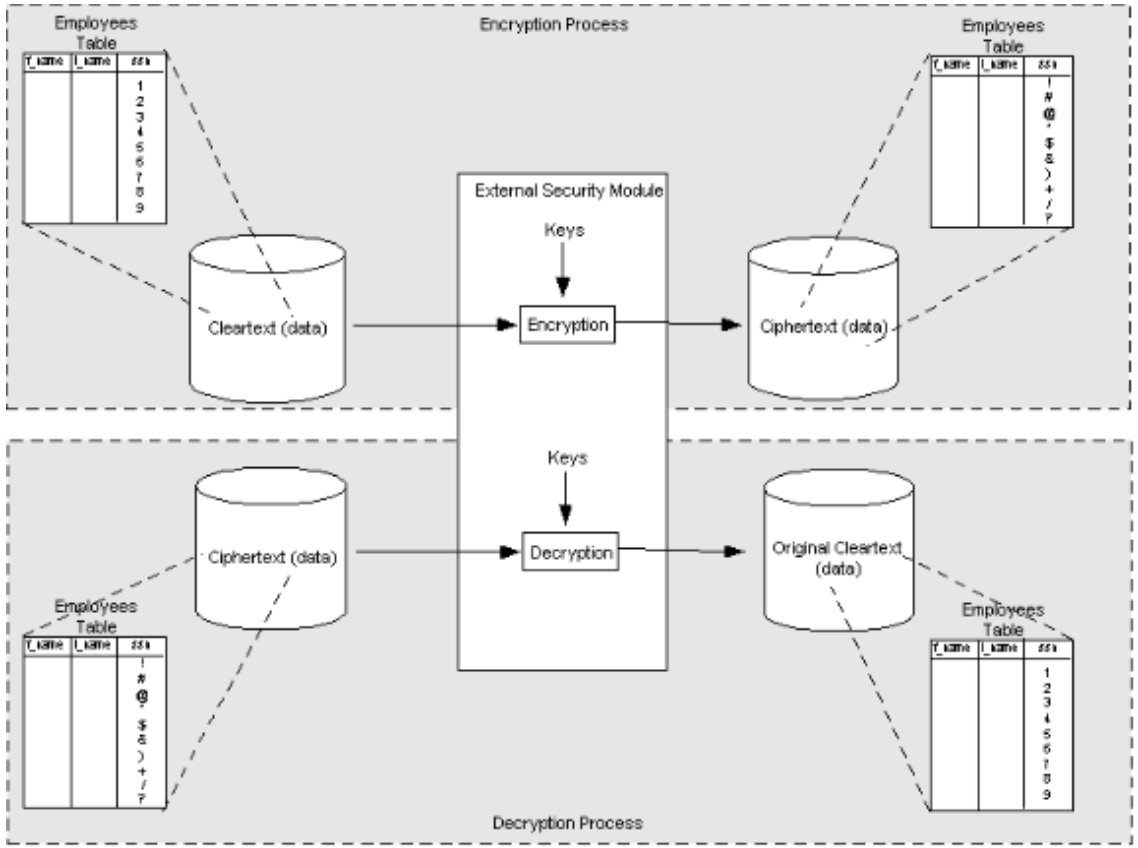
Các bước để mã hóa một cơ sở dữ liệu

Mã hóa CSDL trong các DBMS

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong Oracle:**

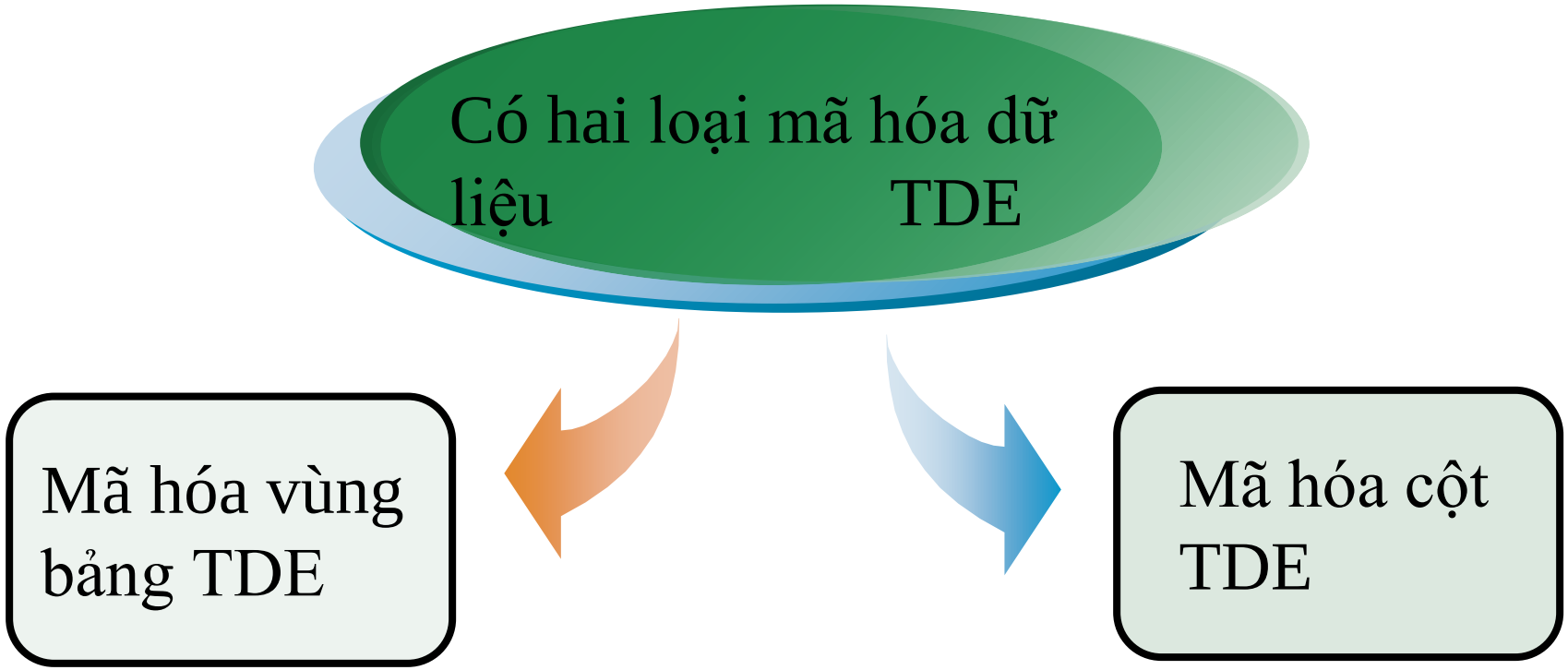
  - Kiến trúc của mã hóa TDE trong Oracle



❖4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong Oracle:**

Phân loại



❖4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong Oracle:**

Mã hóa cột TDE

Khóa chủ mã hóa TDE được lưu trữ trong mô-đun bảo mật bên ngoài

Mỗi khóa bảng TDE được mã hóa riêng với khóa chủ mã hóa TDE

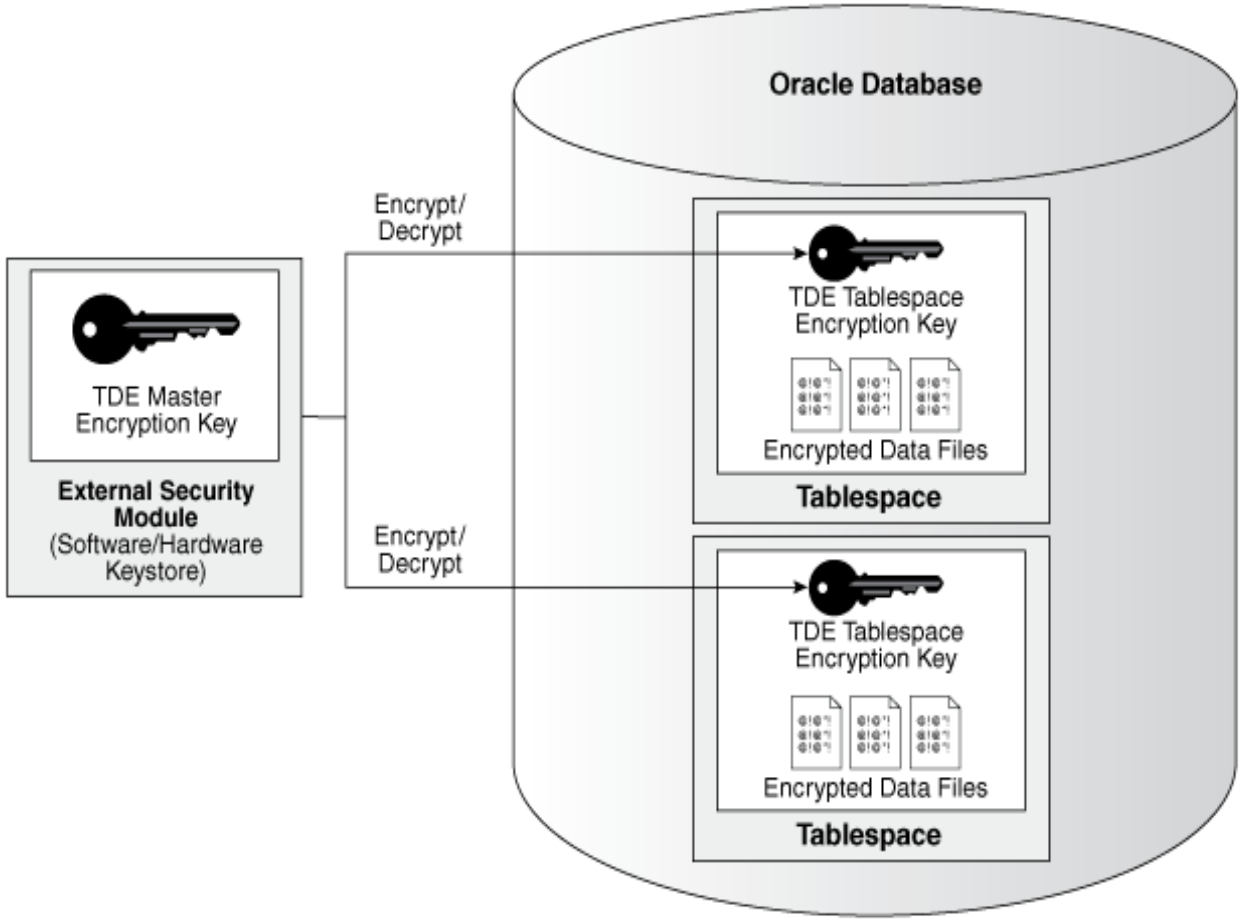
Mã hóa CSDL trong các DBMS

❖4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong Oracle:**

  Mã hóa cột TDE

Tổng quan về mã hóa cột



Mã hóa CSDL trong các DBMS

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong Oracle:**

  Mã hóa vùng bảng TDE

Tất cả các đối tượng được tạo trong vùng bảng được mã hóa sẽ tự động được mã hóa

Tận dụng tối đa mã hóa và bộ nhớ đệm để cung cấp hiệu năng nâng cao

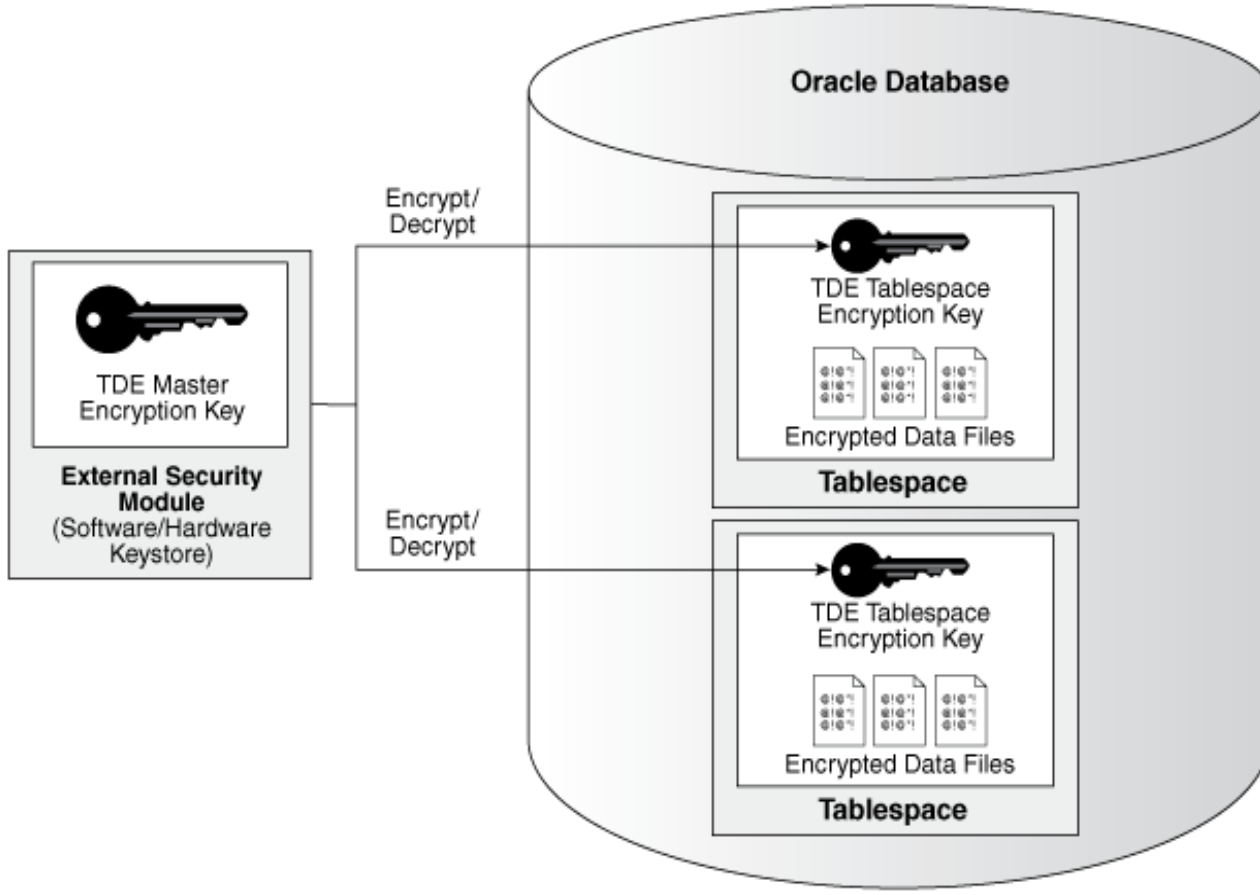
Được lưu trữ ở định dạng được mã hóa trên đĩa

Mã hóa CSDL trong các DBMS

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

- **Mã hóa dữ liệu trong suốt trong Oracle:**
- Mã hóa vùng bảng TDE

Tổng quan về mã hóa vùng bảng



Mã hóa dữ liệu trong suốt

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

Mã hóa dữ liệu trong suốt trong Oracle:

- *Cơ chế quản lý khóa*

TDE dùng "ví" (Wallet) để quản lý khóa. Trong đời thường, ví được dùng để lưu những gì quan trọng như: tiền, CMND, thông tin bí mật, v.v.. Ví trong Oracle cũng vậy, ví là một tập tin nhị phân và thường dùng để lưu khóa chủ, ta gọi khóa này là MK (Master Key).

Tuy nhiên, TDE lại mã hóa dữ liệu trong bảng của CSDL với khóa CK (Column Key).

Mã hóa dữ liệu trong suốt

4.2.3. Mã hóa dữ liệu trong suốt (TDE):

Mã hóa dữ liệu trong suốt trong Oracle:

- *Hoạt động của TDE*

Quá trình mã hóa và những khóa mật mã kết hợp được tạo ra và được quản lý bởi cơ sở dữ liệu.

Sự mã hóa đó có thể xác định một cách trực tiếp trong các cú pháp: create table, alter table và create tablespace.

Mã hóa dữ liệu trong suốt

❖ 4.2.3. Mã hóa dữ liệu trong suốt (TDE):

So sánh mã hóa dữ liệu trong suốt trong SQL Server và Oracle

Oracle

- Không hỗ trợ giải pháp truy vấn trên dữ liệu mã
- TDE của Oracle đơn giản hóa việc quản lý các khóa mã hóa được sử dụng để mã hóa dữ liệu ở các mức độ chi tiết khác nhau.

SQL Server

- Hỗ trợ giải pháp truy vấn trên dữ liệu mã như đối với giải pháp luôn luôn mã hóa AE
- Mã hóa dữ liệu trong suốt thực hiện mã hóa và giải mã các tệp vật lý thay vì dữ liệu trong hệ thống cơ sở dữ liệu.
- Sửa đổi các ứng dụng truy cập cơ sở dữ liệu là không bắt buộc

NỘI DUNG

1. Đảm bảo an toàn CSDL bằng mật mã
2. Mã hóa CSDL trong các DBMS
3. Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

Dữ liệu được mã/giải mã ở đâu

Các khóa mã được lưu trữ ở đâu

Phân quyền truy cập tới các khóa mã như thế nào

- Bảo vệ CSDL

Lựa chọn cơ chế mã hóa nào có thể hài hòa giữa bảo mật dữ liệu và yêu cầu về tốc độ truy vấn?

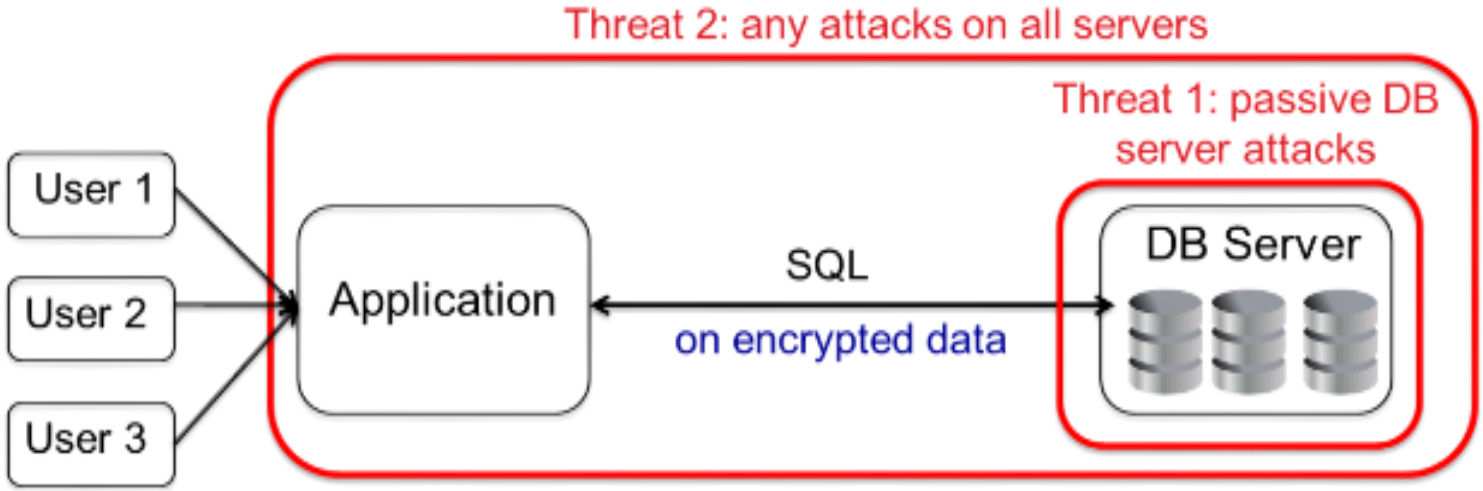
Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.1. Vấn đề truy vấn trên dữ liệu mã:

Nguy cơ tấn công lên CSDL

Nguy cơ 1: Tấn công trực tiếp lên hệ thống máy chủ CSDL.

Nguy cơ 2: Tấn công lên tất cả các máy chủ, đường truyền.v.v



Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.1. Vấn đề truy vấn trên dữ liệu mã:

- ***Các thách thức đặt ra***
  - CSDL phải được lưu ở dạng bản mã và luôn được mã hóa trên hệ thống máy chủ.
  - Thực hiện truy vấn trên dữ liệu mã (thay cho việc truy vấn trên dữ liệu rõ).
  - Cần hỗ trợ đầy đủ các kiểu truy vấn và thực hiện trong suốt đối với người dùng đầu cuối.
  - Đảm bảo hiệu năng truy vấn và truyền thông.
  - Đảm bảo chống lại được các kiểu tấn công có thể trên hệ thống CSDL.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.1. Vấn đề truy vấn trên dữ liệu mã:

- ***Các kiểu kiến trúc truy vấn SQL trên dữ liệu mã***

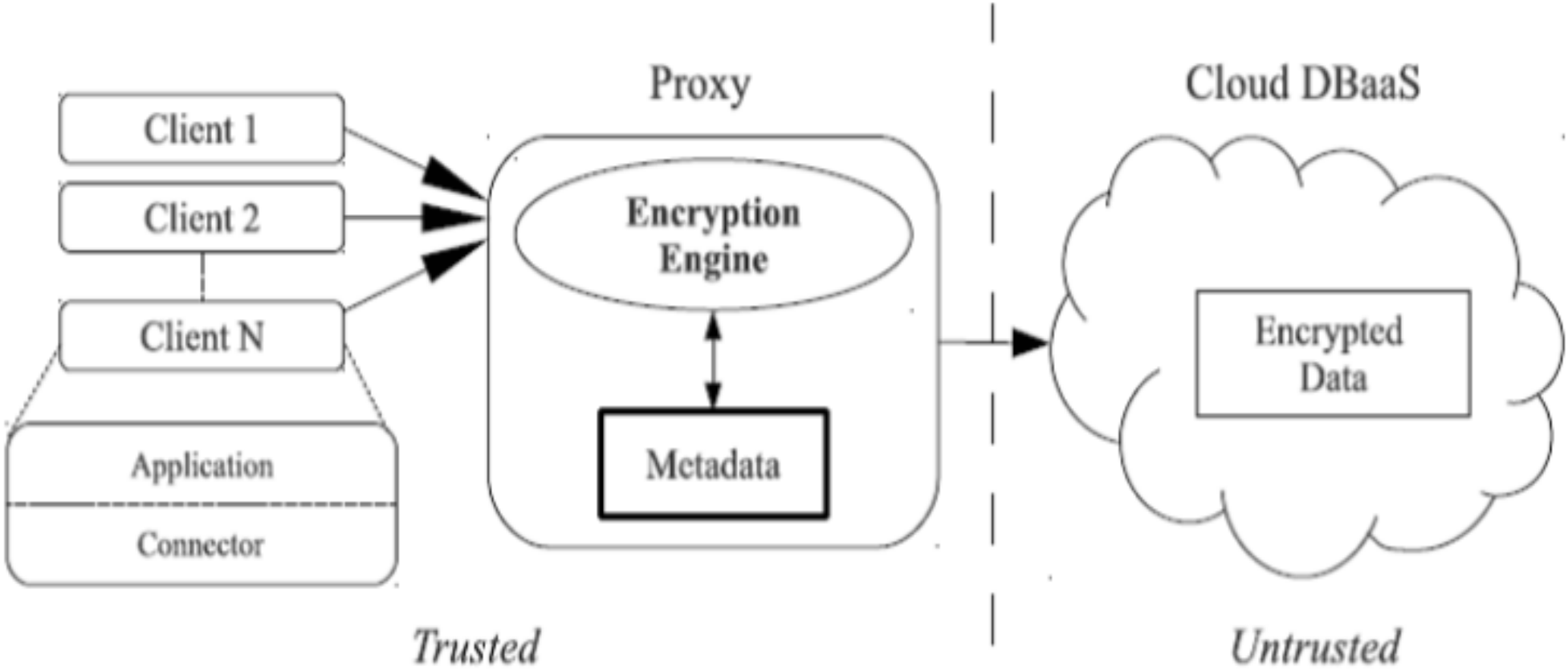
  - Kiến trúc dựa trên máy chủ proxy (proxy-based architectures).

  - Kiến trúc không sử dụng máy chủ proxy (proxy-less architectures): trong đó bao gồm:
    - Kiến trúc lưu trữ metadata tại phía các client
    - Kiến trúc lưu trữ metadata tại máy chủ CSDL đám mây.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖4.3.1. Vấn đề truy vấn trên dữ liệu mã:

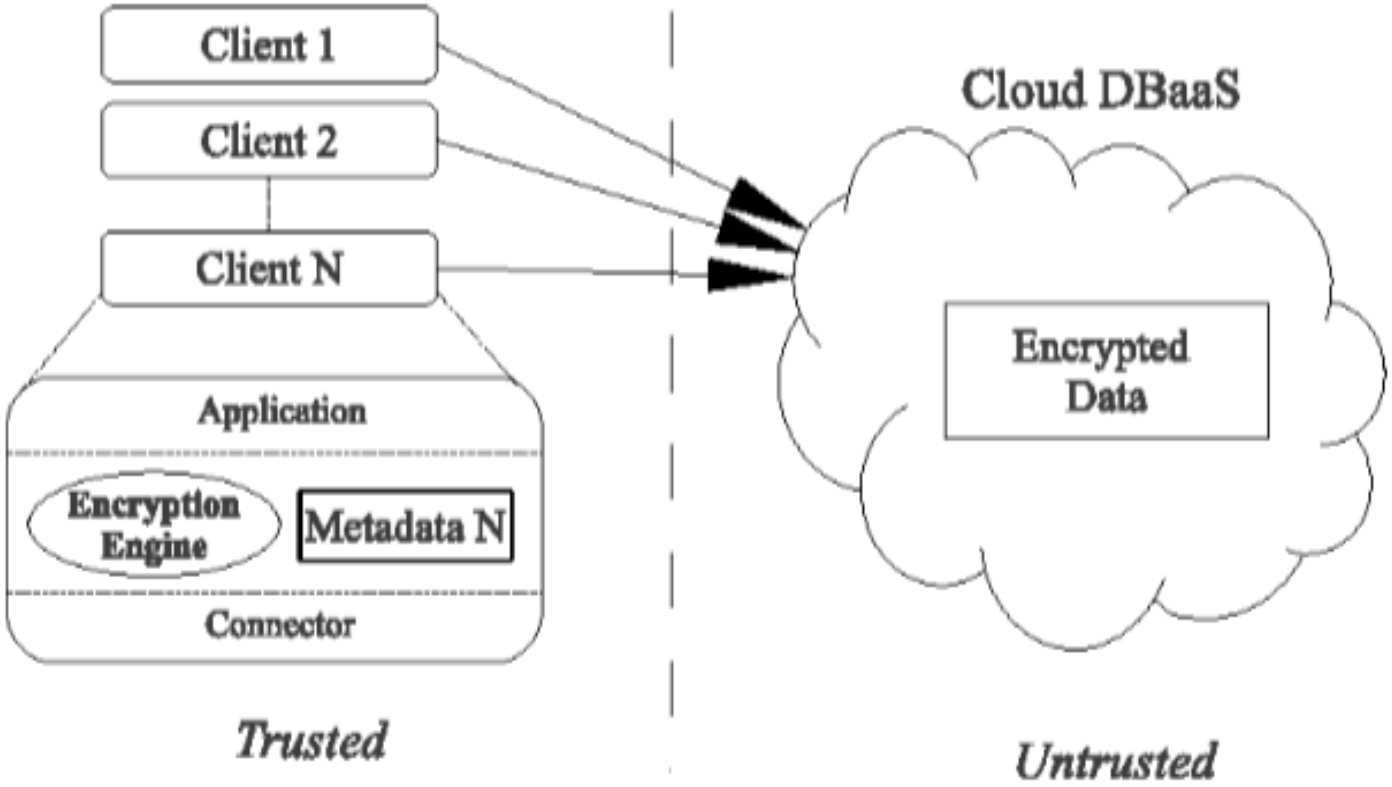
- Kiến trúc dựa trên máy chủ proxy (proxy-based architectures).



Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.1. Vấn đề truy vấn trên dữ liệu mã:

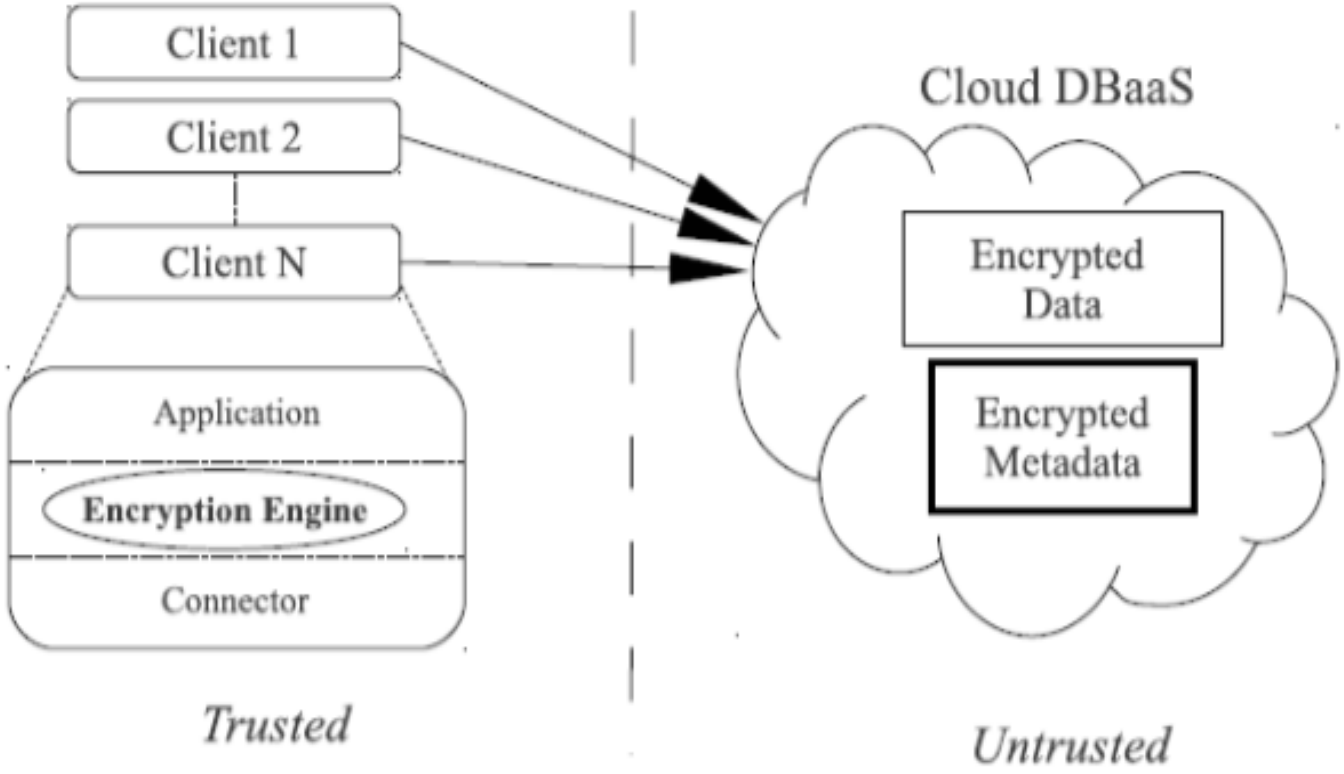
- Kiến trúc không sử dụng máy chủ proxy (proxy-less architectures): lưu trữ metadata tại phía các client



Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.1. Vấn đề truy vấn trên dữ liệu mã:

- Kiến trúc không sử dụng máy chủ proxy (proxy-less architectures): lưu trữ metadata tại máy chủ CSDL đám mây.



Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.2. Một số giải pháp mã nguồn mở:

- **4.3.2.1. Giải pháp dựa trên máy chủ Proxy:**
  - CryptDB
  - Một số giải pháp mã nguồn mở khác: Monomi, ZeroDB

4.3.2. Một số giải pháp mã nguồn mở:

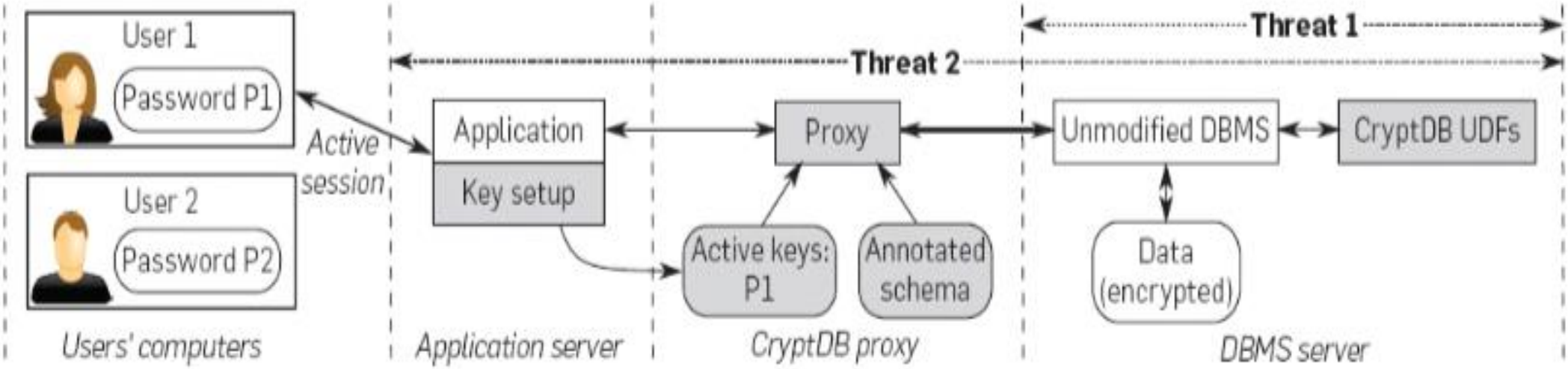
- **CryptDB:**

- CryptDB là một giải pháp mã nguồn mở cho phép xử lý truy vấn trên các cơ sở dữ liệu mã hóa giải quyết vấn đề thực tế, nó sẽ được lồng vào một số lớp mã hóa dữ liệu, mỗi lớp sử dụng một khóa khác nhau, cho phép mã hóa dữ liệu cho một phép toán đơn giản.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖4.3.2. Một số giải pháp mã nguồn mở:

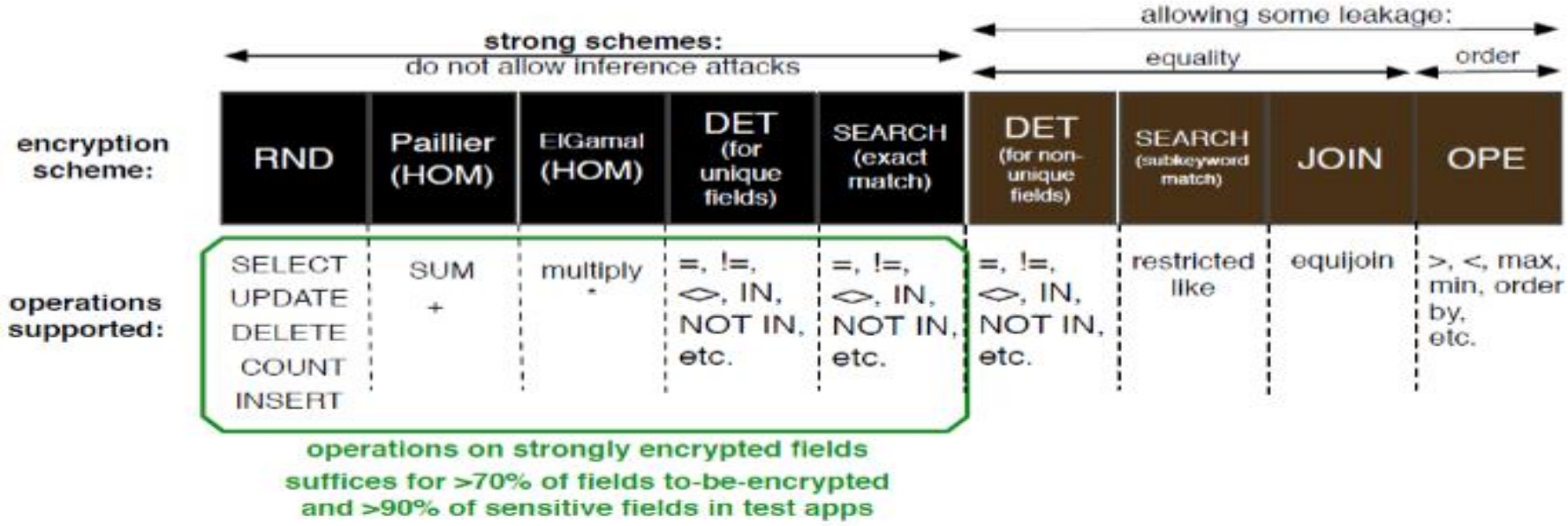
- **CryptDB:**
- *Mô hình bảo mật của CryptDB*



Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖4.3.2. Một số giải pháp mã nguồn mở:

- **CryptDB:**
- *Các thuật toán sử dụng để thực hiện truy vấn trên dữ liệu mã*



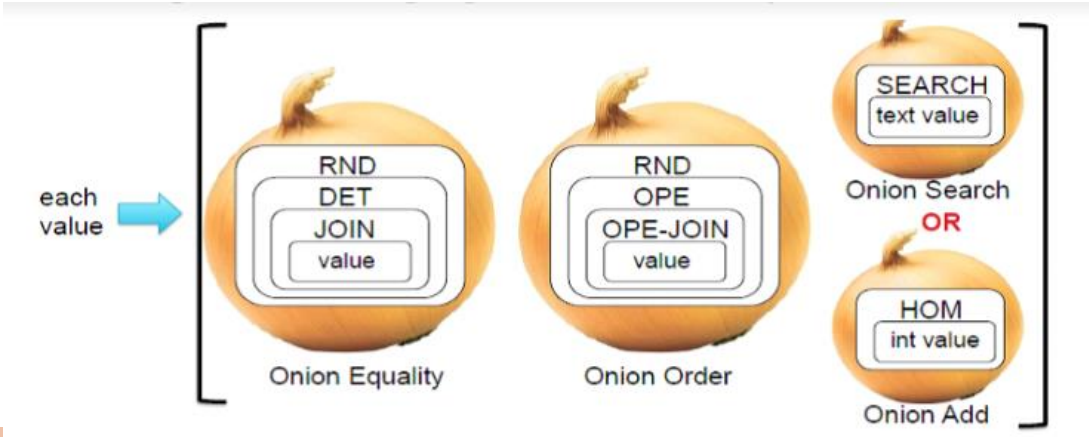
Mã hóa dựa trên truy vấn có thể điều chỉnh (Adjustable Query basedEncryption)

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.2. Một số giải pháp mã nguồn mở:

- **CryptDB:**
- *Các thuật toán sử dụng để thực hiện truy vấn trên dữ liệu mã*
  - Mã hóa nhận thức SQL (SQL-aware Encryption)
  - Mã hóa dựa trên truy vấn có thể điều chỉnh (Adjustable Query-based Encryption)
  - Mã hóa mỗi mục dữ liệu trong một hoặc nhiều lớp của "củ hành" (onions).

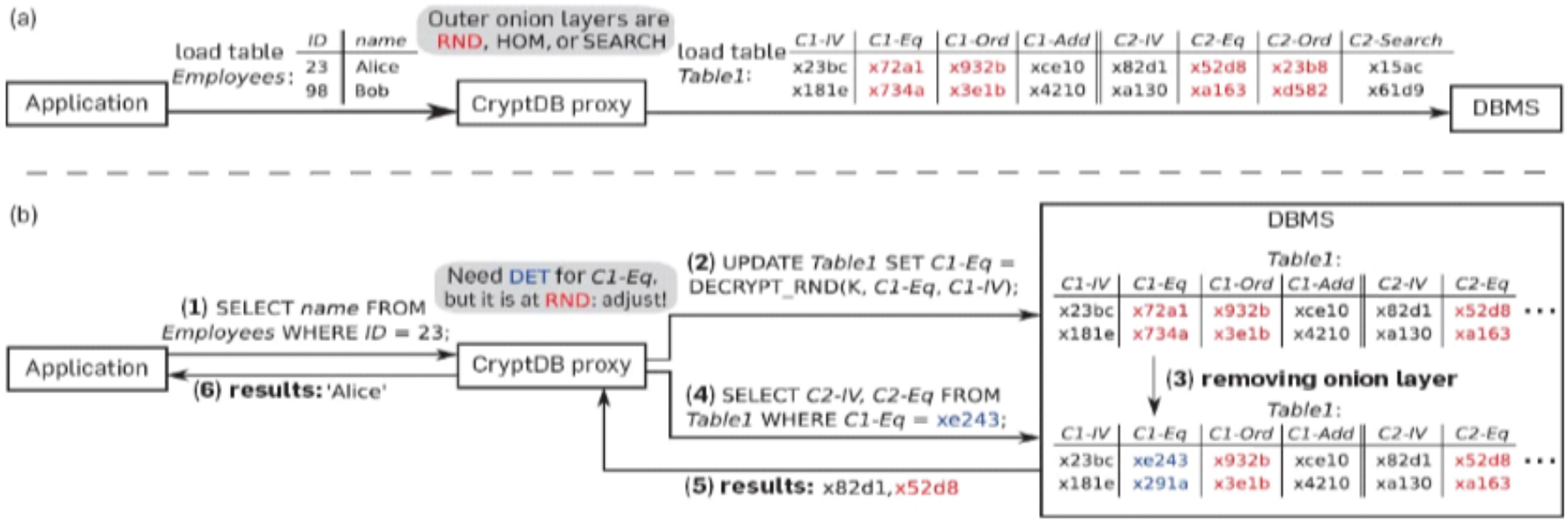
Giải pháp mã hóa kiểu "củ hành"



Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.2. Một số giải pháp mã nguồn mở:

- **CryptDB:**
- *Thực hiện truy vấn trên dữ liệu mã*
  - Máy chủ proxy thực hiện các chuyển đổi câu lệnh hoạt động trên các lớp của "củ hành".



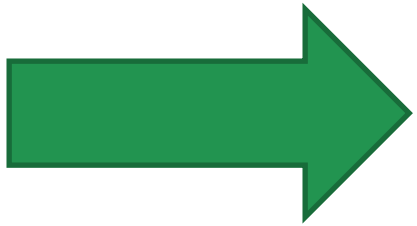
Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖4.3.2. Một số giải pháp mã nguồn mở:

- **CryptDB:**

  Khả năng hỗ trợ truy vấn

  - CryptDB chỉ hỗ trợ 4/22 câu truy vấn TPC-H có thể.
  - CryptDB làm tăng đáng kể không gian lưu trữ và thời gian truy vấn.



là giải pháp đầu tiên mang tính thực tiễn với kỹ thuật truy vấn trên dữ liệu mã.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

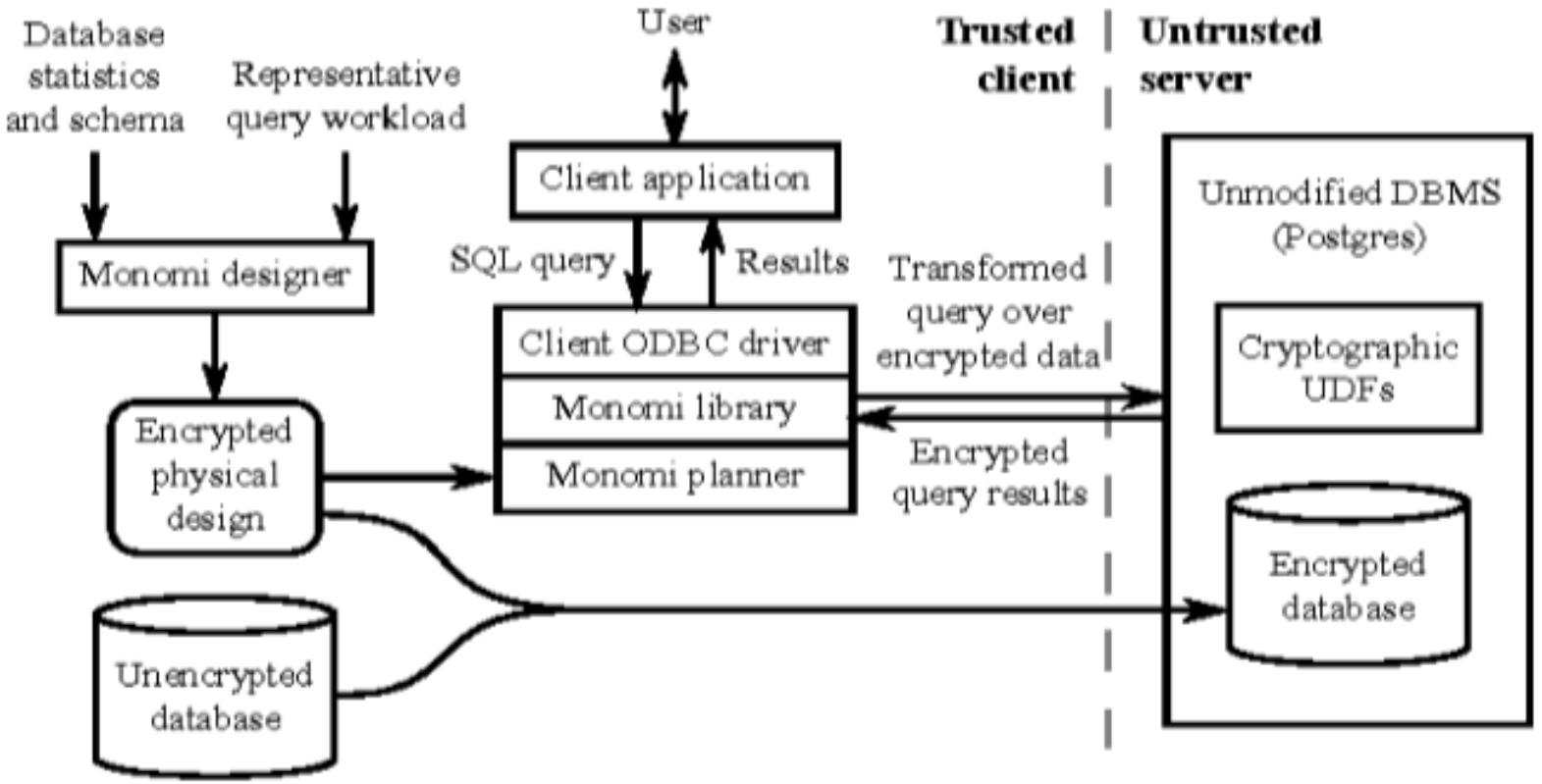
4.3.2. Một số giải pháp mã nguồn mở:

- ***Monomi***
  - Sử dụng giải pháp truy vấn bằng cách chia việc thực hiện truy vấn trên cả phía máy chủ và đầu cuối (client/server query execution), nó có thể thực hiện các truy vấn phức tạp bất kỳ trên dữ liệu mã, cũng như đưa ra một vài công nghệ cho phép cải thiện hiệu năng như tính toán trước theo hàng, mã hóa tiết kiệm không gian, v.v.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.2. Một số giải pháp mã nguồn mở:

- **Monomi**
- *Mô hình bảo mật CSDL của Monomi*



4.3.2. Một số giải pháp mã nguồn mở:

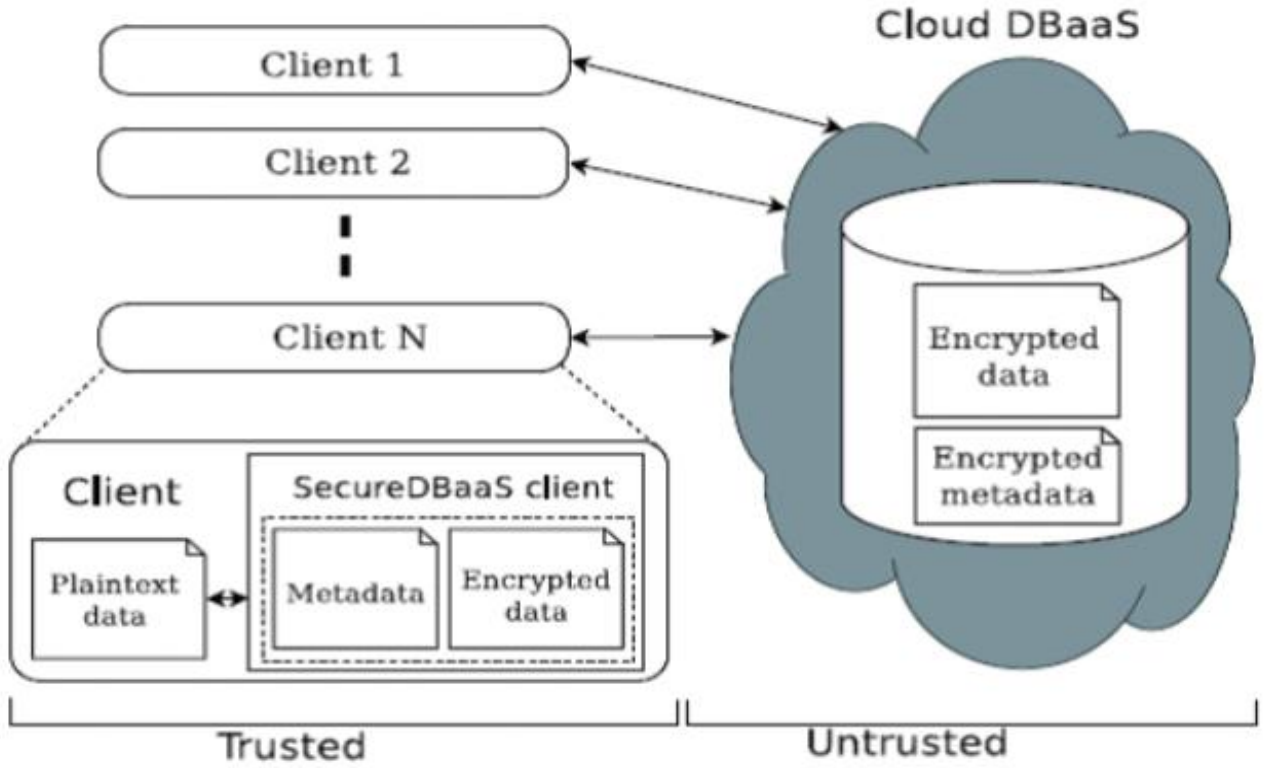
- ***ZeroDB***
  - ZeroDB là một giải pháp truy vấn CSDL khác mã hóa từ đầu cuối đến đầu cuối mà hỗ trợ các đầu cuối thực hiện các truy vấn (search, sort, query, share) trên dữ liệu được mã hóa mà không làm lộ khóa hoặc dữ liệu rõ cho máy chủ. Nó sử dụng kiến trúc client-server, nhưng các truy vấn logic và các khóa mã được đặt ở phía đầu cuối. Giải pháp này hỗ trợ hoạt động trên hệ quản trị CSDL hướng đối tượng (object-oriented database).

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.2. Một số giải pháp mã nguồn mở:

4.3.2.2. Một số giải pháp không dựa trên máy chủ proxy

- *Kiến trúc bảo mật CSDL đám mây 1*



4.3.2. Một số giải pháp mã nguồn mở:

4.3.2.2. Một số giải pháp không dựa trên máy chủ proxy

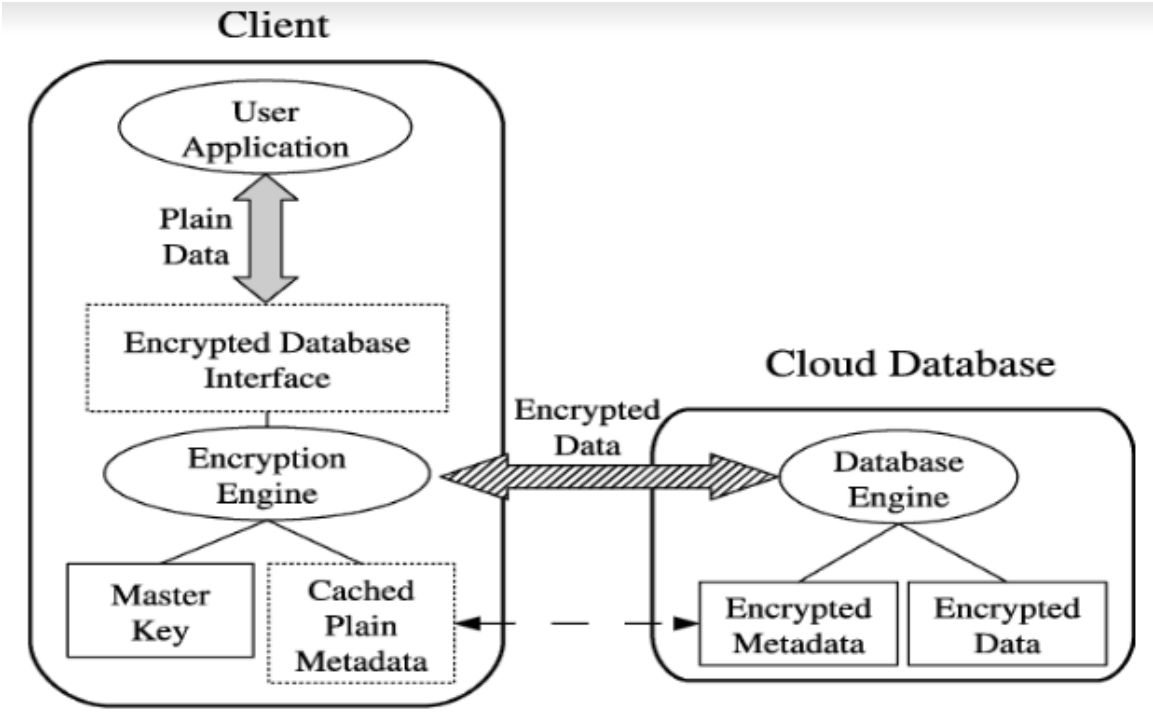
- *Kiến trúc bảo mật CSDL đám mây 1*
  - Các khóa mật sẽ được quản lý và lưu trữ trực tiếp trên các client, trên mỗi client sẽ cài đặt một ứng dụng an toàn (SecureDBaas Client).
  - Từ các client này người sử dụng có thể thực hiện các thao tác truy vấn trên CSDL đã mã hóa (có sự phân quyền trên các client tương ứng).
  - Các client sẽ lưu trữ thông tin rõ (một số thông tin rõ phục vụ truy vấn CSDL) và các thông tin metadata và dữ liệu mã hóa (encrypted data). Trên đám mây sẽ lưu trữ các dữ liệu đã được mã hóa và metadata đã được mã hóa.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.2. Một số giải pháp mã nguồn mở:

4.3.2.2. Một số giải pháp không dựa trên máy chủ proxy

- *Kiến trúc bảo mật CSDL đám mây 2*



4.3.2. Một số giải pháp mã nguồn mở:

4.3.2.2. Một số giải pháp không dựa trên máy chủ proxy

- *Kiến trúc bảo mật CSDL đám mây 2*

- Sử dụng các thuật toán mã hóa nhận thức SQL (SQL-aware encryption algorithms), nó đảm bảo thực hiện các truy vấn SQL trên dữ liệu đã mã hóa.
- Sử dụng các lớp mã hóa củ hành như sau:

+ Random (Rand) – lớp mã hóa ngoài cùng, được sử dụng để lấy dữ liệu;

+ Deterministic (Det) – lớp mã hóa tất định, được sử dụng để thực hiện các truy vấn bằng;

4.3.2. Một số giải pháp mã nguồn mở:

4.3.2.2. Một số giải pháp không dựa trên máy chủ proxy

- *Kiến trúc bảo mật CSDL đám mây 2*

+ Order Preserving Encryption (Ope) – lớp mã hóa thực hiện trên dữ liệu kiểu số để thực hiện các truy vấn (=, <, ≤, >, ≥);

+ Homomorphic Sum (Sum) – lớp mã hóa cho phép thực hiện các tính toán trực tiếp trên dữ liệu mã;

+ Search (Search) – lớp mã hóa cho phép thực hiện các truy vấn tìm kiếm;

+ Plain – dữ liệu ở dạng rõ.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖4.3.3. Một số giải pháp thương mại:

- **Giải pháp của CipherCloud:**

Cung cấp khả năng mã/giải mã dựa trên việc sử dụng cổng mã hóa (gateway) (dữ liệu đi vào và đi ra đều được mã/giải mã dựa trên cổng này).

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖4.3.3. Một số giải pháp thương mại:

- **Giải pháp của CipherCloud:**

Nó cung cấp các phương pháp mã hóa:

1) mã hóa bảo toàn định dạng;

2) mã hóa theo chuẩn AES (khóa 256 bit) và hỗ trợ bất kỳ CSDL tương thích JDBC (Any JDBC compliant database).

Giải pháp này cung cấp khả năng truy vấn, tìm kiếm trên dữ liệu đã mã hóa.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.3. Một số giải pháp thương mại:

- **Giải pháp của Vormetric:**

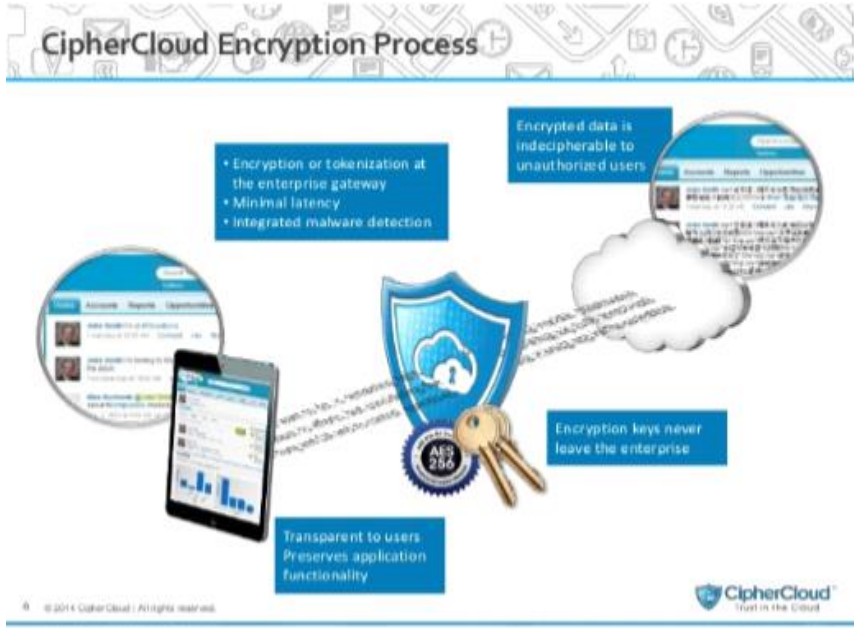
Cung cấp khả năng mã/giải mã trong suốt cho các hệ quản trị CSDL Oracle, DB2 and Microsoft SQL Database Server, Informix, Sybase, MySQL.

Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

❖4.3.3. Một số giải pháp thương mại:

- **Giải pháp của Porticor:**

Cung cấp khả năng quản lý khóa mã theo phương pháp mã hóa đồng cấu (Homomorphic Key Management) cho giải pháp mã/giải mã hầu hết các hệ quản trị CSDL như Oracle, MySQL, MS SQL và IBM DB2.



Một số giải pháp bảo mật CSDL hỗ trợ truy vấn trên dữ liệu mã

4.3.3. Một số giải pháp thương mại:

- **Giải pháp của SafeNet:**

Cung cấp khả năng mã hóa cho các hệ quản trị CSDL Oracle, MS SQL và IBM DB2. Nó hỗ trợ các thuật toán mật mã như: AES, 3DES, DES, RSA (signatures and encryption), RC4, SHA-1.


QUESTION