# Summary

Mã hóa là một kỹ thuật phổ biến nhằm đảm bảo tính cơ mật của dữ liệu, đặc biệt là dữ liệu nhạy cảm. Việc mã hóa dữ liệu ngày càng cải thiện cũng đồng nghĩa với việc ảnh hưởng tới hiệu suất hệ thống ngày càng lớn. Do đó, quá trình quản lý dữ liệu mã hóa sẽ phải đối mặt với các vấn đề như lựa chọn giải thuật mã hóa thích hợp, kiến trúc quản lý, giao thức phân phối khóa, lưa trữ và lấy dữ liệu một cách hiệu quả, xác định kỹ thuật truy vấn và tìm kiếm dữ liệu mã hóa, đảm bảo ràng buộc dữ liệu. Trong bài viết này, ứng dụng để minh họa là Database as a service (DAS). Bài viết tập trung vào các công nghệ truy vấn dữ liệu mã hóa và tổng kết các công nghệ cơ bản cho việc truy vấn bằng SQL tới các lược đồ quan hệ bị mã hóa, tìm kiếm từ khóa trên dữ liệu mã hóa, .

# Introduction

# DAS – Lưu trữ và truy vấn dữ liệu mã hóa

Mô hình DAS hỗ trợ nhiều chức năng quản lý dữ liệu dưới dạng service. Đây là một giải pháp thay thế cho cách quản lý dữ liệu trực tiếp của chủ quản là các công ty để giải quyết các thách thức đối với kiến trúc truyền thống. Vấn đề hàng đầu dặt ra là tính bảo mật dữ liệu ở server sẽ như thế nào? Dữ liệu quan trọng luôn cần được bảo vệ khỏi các truy cập trái phép ở server. Đó có thể là truy cập của hacker hoặc là truy cập hợp phép nhưng không có dụng ý tốt như quản trị database. Giải pháp đó là mã hóa toàn bộ hoặc một phần dữ liệu quan trọng và chỉ có chủ sở hữu mới có khóa. Và giải pháp này tồn tại một số vấn đề khác như giải thuật mã hóa, quản lý khóa, truy vấn. Đặc biệt, việc truy vấn là thách thức lớn nhất. Nhiều công nghệ truy vấn dữ liệu quan hệ, văn bản hoặc xml được phát triển.

## Thiết lập và mô hình bảo mật DAS

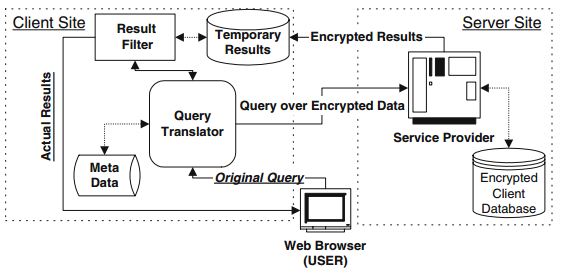
Đối với case study này, tồn tại một số thực thể là người chủ dữ liệu, client và server. Người chủ lưu trữ dữ liệu ở phía server và client truy vấn, xử lý dữ liệu từ xa bằng quyền truy cập của họ. Một phần dữ liệu có thể quan trọng và phải được bảo vệ khỏi truy cập trái phép – những người, tổ chức nhắm vào dữ liệu đó. Giả định tình huống là phía client/ chủ an toàn và đáng tin cậy nên mối đe dọa đến từ chính những truy cập phía server; nhà cung cấp dịch vụ cũng đáng tin cậy. Do đó, dữ liệu phải được mã hóa và key chỉ có người chủ sở hữu. Dữ liệu được giải mã ở phía client. Chống lại các tấn công rất khó khăn và cần sự nổ lực từ phía client để đảm bảo chức năng hệ thống hoạt động đúng yêu cầu. Đồng thời, cơ chế xác nhận và hệ thống tích hợp cũng đóng vai trò quan trọng trong tình huống này.

## Truy vấn dữ liệu quan hệ mã hóa

Approaches based on new encryption techniques

Information-hiding based Approaches

Kiến trúc quá trình truy vấn trong DAS



Lược đồ trên mô tả luồng thực thi của câu truy vấn trong DAS. Trong mô hình DAS, có 3 thực thể tồn tại: user, client và server. Client lưu trữ database ở server. Server được quản lý bởi service provider. Cả hai được gọi chung là server side. Dữ liệu mã hóa được lưu trữ kèm theo các thông tin bổ sung để việc truy vấn không ảnh hưởng tới dữ liệu. Client cũng sẽ lưu trữ metadata để dịch câu truy vấn của user thành dạng tương thích với server và thực thi post processing để query trên server. Do đó, câu truy vấn khi thực thi sẽ chia thành 2 phần: 1 phần truy vấn server lấy dữ liệu mã hóa bằng những thông tin bổ sung, 1 phần truy vấn phía client và post preprocess kết quả trả về từ server. Để làm được điều đó, cần phải phát triển một khung đại số để câu truy vấn được phân rã thích hợp.

## Mô hình lưu trữ và mã hóa lược đồ quan hệ

Điều kiện ánh xạ

## Tìm kiếm từ khóa trên dữ liệu văn bản được mã hóa

## Tìm kiếm trên dữ liệu XML mã hóa

## Privacy Aware Bucketization

# Độ tin cậy, mã hóa, quản lý khóa, tích hợp và bảo mật dữ liệu

## Mã hóa dữ liệu quan hệ

## Vấn đề xác thực và toàn vẹn

## Quản lý khóa trên DAS

# Tổng kết và công việc liên quan