THÔNG TIN TÓM TẮT NHỮNG ĐÓNG GÓP MỚI CỦA LUẬN ÁN

Đề tài luận án: **Nghiên cứu phát triển giải pháp xác thực an toàn và quản lý khoá cho cơ sở dữ liệu thuê ngoài**

Chuyên ngành: Cơ sở toán học cho tin học

Mã số: 9 46 01 10

Họ và tên Nghiên cứu sinh: Hồ Kim Giàu

Tập thể hướng dẫn khoa học: PGS.TS Nguyễn Hiếu Minh.

Cơ sở đào tạo: Học viện Kỹ thuật Quân sự

Tóm tắt những đóng góp mới của luận án

Những kết quả chính của luận án bao gồm:

1. Đề xuất thuật toán giảm thời gian truy vấn trên dữ liệu mã dựa trên xử lý song song. Phương pháp đề xuất sẽ giảm thời gian trong các tiến trình giải mã và tính toán dữ liệu từ đó giảm thời gian thực hiện truy vấn;
2. Đề xuất hai thuật toán xác thực lô dựa trên hai bài toán khó. Thuật toán đề xuất giúp xác thực nhiều chữ ký cùng một lúc trong một phương trình xác thực. Đề xuất mô hình, thuật toán xác thực dữ liệu khi truy vấn trên cơ sở dữ liệu mã thuê ngoài dựa trên xác thực lô;
3. Đề xuất cây KMT (Key management tree) để quản lý khoá mã của cơ sở dữ liệu. Đề xuất phương pháp mã hoá hệ thống tệp tin (KVEFS), sử dụng để lưu trữ dữ liệu nhạy cảm, bảo vệ dữ liệu trong suốt đối với người dùng bằng lưu trữ khóa-giá trị. Đề xuất mô hình quản lý truy cập giúp chủ sở hữu dữ liệu kiểm soát quyền người dùng khi truy vấn dữ liệu. Đề xuất thuật toán đổi khoá mã của cơ sở dữ liệu thuê ngoài ở mức cột dựa trên MapReduce.

Hà Nội, ngày 22 tháng 09 năm 2021

NGƯỜI HƯỚNG DẪN KHOA HỌC **NGHIÊN CỨU SINH**

PGS.TS Nguyễn Hiếu Minh **Hồ Kim Giàu**

SUMMARY INFORMATION ON NEW FINDINGS
IN DOCTORAL THESIS

Thesis title: **Research and development of secure authentication and key management for outsourced databases**

Major: Mathematical Foundations for Informatics

Major code: 9 46 01 10

PhD Student: Ho Kim Giau

Supervisors: Ass. Prof. Dr Nguyen Hieu Minh

Educational institution: Military Technical Academy

The new findings of the research:

The main results of this dissertation include:

1. Proposing an algorithm to reduce query time on encrypted outsourced database based on parallel processing. The proposed method will reduce the time in the processes of decrypting and calculating data, thereby reducing query execution time;
2. Proposing two batch verification algorithms based on two hard problems. The proposed algorithm helps to verify multiple signatures at the same time in a verification equation. Propose models and algorithms for data verification when querying on an encrypted outsourced database based on batch verification;
3. Proposing a KMT tree to manage the database's keys. Proposing a new architecture of encrypted file system (KVEFS), used to store and protect sensitive data. Proposing an access control model that helps data owners manage access rights of user when querying data. Proposing the key changed algorithm at the column level of the encrypted outsourced database based on MapReduce..

Hanoi, September 22, 2021

Supervisor	**PhD Student**
Ass. Prof. Dr Nguyen Hieu Minh	**Ho Kim Giau**