

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TRƯỜNG NGỌC HẠNH

**NGHIÊN CỨU MÔ HÌNH XỬ LÝ DỮ LIỆU MÃ
HÓA VÀ BẢO MẬT DỮ LIỆU TRONG ĐIỆN
TOÁN ĐÁM MÂY**

LUẬN VĂN THẠC SĨ: KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, NĂM 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TRƯƠNG NGỌC HẠNH

**NGHIÊN CỨU MÔ HÌNH XỬ LÝ DỮ LIỆU MÃ HÓA VÀ
BẢO MẬT DỮ LIỆU TRONG ĐIỆN TOÁN Đám MÂY**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

HƯỚNG DẪN KHOA HỌC

TS. TRẦN ĐỨC SỰ

THÁI NGUYÊN, NĂM 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn “*Nghiên cứu mô hình xử lý dữ liệu mã hóa và bảo mật dữ liệu trong điện toán đám mây*” là sản phẩm của riêng cá nhân, không sao chép lại của người khác. Trong toàn bộ nội dung của luận văn, những điều được trình bày hoặc là của cá nhân hoặc là được tổng hợp, nghiên cứu từ nhiều nguồn tài liệu. Tất cả các tài liệu tham khảo đều có xuất xứ và trích dẫn rõ ràng.

Nếu có gì sai sót, tôi xin chịu mọi trách nhiệm./.

Thái Nguyên, ngày tháng năm 2015

HỌC VIÊN

Trương Ngọc Hạnh

LỜI CẢM ƠN

Lời đầu tiên, tôi xin bày tỏ lòng biết ơn đến thầy TS.Trần Đức Sự người đã tận tình hướng dẫn, chỉ bảo và giúp đỡ tôi trong suốt quá trình nghiên cứu và hoàn thành luận văn này.

Tôi xin chân thành cảm ơn các thầy cô giáo trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên đã giảng dạy và cung cấp cho chúng tôi những kiến thức rất bổ ích trong thời gian học cao học, giúp tôi có nền tảng tri thức để phục vụ nghiên cứu khoa học sau này.

Tôi cũng xin cảm ơn Lãnh đạo và đồng nghiệp tại đơn vị đã tạo điều kiện và giúp đỡ tôi trong suốt quá trình nghiên cứu và hoàn thành luận văn. Tôi cũng xin bày tỏ lòng cảm ơn đến gia đình và bạn bè, những người luôn quan tâm, động viên và khuyến khích tôi trong quá trình học tập.

Thái Nguyên, ngày tháng năm 2015

Học viên

Trương Ngọc Hạnh

MỤC LỤC

	Trang
LỜI CAM ĐOAN.....	i
LỜI CẢM ƠN	ii
MỤC LỤC.....	iii
DANH MỤC CÁC TỪ VIẾT TẮT TRONG LUẬN VĂN.....	vi
DANH MỤC CÁC HÌNH ẢNH	vii
DANH MỤC CÁC BẢNG BIỂU	ix
MỞ ĐẦU.....	1
CHƯƠNG 1. TỔNG QUAN VỀ ĐIỆN TOÁN Đám Mây VÀ VẤN ĐỀ BẢO MẬT DỮ LIỆU TRONG ĐIỆN TOÁN Đám Mây	4
1.1. Giới thiệu chung về điện toán đám mây	4
1.2. Mô hình kiến trúc điện toán đám mây	5
1.2.1. Kiến trúc phân lớp dịch vụ.....	5
1.2.1.1. Dịch vụ ứng dụng (SaaS)	9
1.2.1.2. Dịch vụ nền tảng hệ thống (PaaS).....	11
1.2.1.3. Dịch vụ cơ sở hạ tầng (IaaS).....	14
1.2.2. Mô hình triển khai.....	15
1.2.2.1. Đám mây riêng (Private Cloud)	15
1.2.2.2. Đám mây công cộng (Public Cloud).....	17
1.2.2.3. Đám mây lai (Hybrid Cloud)	18
1.3. Vấn đề bảo mật trong điện toán đám mây	19
1.3.1. An toàn liên quan đến kiến trúc của điện toán đám mây.....	19
1.3.1.1. An ninh ở mức hạ tầng.....	19
1.3.1.2. An ninh ở mức dịch vụ nền tảng.....	20
1.3.1.3. An ninh ở mức dịch vụ phần mềm.....	21
1.3.2. Vấn đề quản lí an toàn hệ thống.....	22
CHƯƠNG 2. MÔ HÌNH XỬ LÝ DỮ LIỆU MÃ HÓA VÀ BẢO MẬT DỮ LIỆU TRONG ĐIỆN TOÁN Đám Mây	24

2.1. Dịch vụ cơ sở dữ liệu (DBaaS)	24
2.1.1. Khái niệm.....	24
2.1.2. Lợi ích của DBaaS so với các hệ cơ sở dữ liệu thông thường.....	25
2.1.3. Vấn đề bảo mật dữ liệu	26
2.2. CryptDB và mô hình xử lý dữ liệu mã hóa.....	27
2.2.1. Giới thiệu về CryptDB và mô hình.....	27
2.2.2. Môi đe dọa DBMS bị thỏa hiệp	29
2.2.3. Truy vấn trên dữ liệu mã hóa	31
2.2.3.1. Mã hóa trong CryptDB.....	31
2.2.3.2. Mã hóa lớp.....	34
2.2.3.3. Hàm người dùng định nghĩa: (User Defined Function – UDF)	37
2.2.3.4. Điều chỉnh mã hóa dựa theo truy vấn	38
2.2.3.5. Cấu trúc dữ liệu trong CryptDB.....	41
2.2.3.6. Thực thi truy vấn trên dữ liệu mã hóa.....	43
2.2.3.7. Tính toán liên kết giữa các cột	51
2.3. Áp dụng mô hình bảo mật dữ liệu trong điện toán đám mây	54
2.3.1. Thách thức và yêu cầu	54
2.3.2. Thiết kế hệ thống.....	58
2.3.3. Phân tích an ninh.....	60
CHƯƠNG 3. TRIỂN KHAI CÀI ĐẶT, THỬ NGHIỆM VÀ ĐÁNH GIÁ MÔ HÌNH	62
3.1. Mô hình triển khai.....	62
3.1.1. Mô hình triển khai hệ thống.....	62
3.1.2. Mô hình hoạt động hệ thống	63
3.2. Triển khai cài đặt và thử nghiệm.....	68
3.2.1. Triển khai cài đặt.....	68
3.2.2. Thử nghiệm mô hình.....	70
3.3. Đánh giá mô hình	75
3.3.1. Đánh giá về chức năng.....	75

3.3.2. Đánh giá về độ bảo mật dữ liệu	76
3.3.4. Đánh giá về hoạt động	76
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	79
TÀI LIỆU THAM KHẢO.....	81

DANH MỤC CÁC TỪ VIẾT TẮT TRONG LUẬN VĂN

Ký hiệu	Thuật ngữ	Ý nghĩa
IT	Information Technology	Công nghệ thông tin
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ
MIT	Massachusetts Institute of Technology	Viện Công nghệ Massachusetts
SLA	Service Level Agreement	Hợp đồng thỏa thuận dịch vụ
QoS	Quality of Service	Chất lượng dịch vụ
IaaS	Infrastructure-as-a-Service	Cơ sở hạ tầng như một dịch vụ
PaaS	Platform-as-a-Service	Nền tảng như một dịch vụ
SaaS	Software-as-a-Service	Phần mềm như một dịch vụ
DBaaS	Database-as-a-Service	Cơ sở dữ liệu như một dịch vụ
SPI	Software-Platform-Infrastructure	Phần mềm nền tảng cơ sở hạ tầng
VM	Virtual Machine	Máy ảo
CRM	Customer Relationship Management	Quản lý quan hệ khách hàng
ERP	Enterprise Resource Planning	hoạch định nguồn lực doanh nghiệp
SQL	Structured Query Language	Ngôn ngữ truy vấn cấu trúc
DBMS	Database Management System	Hệ quản trị cơ sở dữ liệu
UDF	User-Defined Function	Hàm người dùng định nghĩa
DBA	Database Administrator	Quản trị viên cơ sở dữ liệu
MK	Master Key	Khóa chính
PRP	Pseudo-Random Permutation	Hoán vị giả ngẫu nhiên
PRF	Pseudo-Random Function	Hàm giả ngẫu nhiên

DANH MỤC CÁC HÌNH ẢNH

	Trang
Hình 1.1. Điện toán đám mây	5
Hình 1.2. Mô hình kiến trúc dịch vụ điện toán đám mây của SOMF	5
Hình 1.3. Mô hình SPI	6
Hình 1.4. Mô hình SPI với các ứng dụng trong thực tế	7
Hình 1.5. Mức độ kiểm soát/trách nhiệm giữa client và nhà cung cấp dịch vụ....	9
Hình 1.6. SaaS cung cấp dịch vụ cho khách hàng	10
Hình 1.7. Phạm vi kiểm soát giữa nhà cung cấp/sử dụng dịch vụ SaaS.....	11
Hình 1.8. PaaS cho phép khách hàng truy cập vào một nền tảng trên điện toán đám mây	12
Hình 1.9. Phạm vi kiểm soát giữa nhà cung cấp/sử dụng dịch vụ PaaS.....	14
Hình 1.10. IaaS cho phép nhà cung cấp dịch vụ thuê những tài nguyên phần cứng	14
Hình 1.11. Phạm vi kiểm soát giữa nhà cung cấp/sử dụng dịch vụ IaaS.....	15
Hình 1.12. Mô hình triển khai điện toán đám mây	15
Hình 1.13. Các thành phần trong đám mây riêng	16
Hình 1.14. So sánh giữa đám mây riêng và đám mây công cộng.....	17
Hình 1.15. Đám mây công cộng.....	18
Hình 1.16. Mô hình đám mây lai	19
Hình 2.1. Kiến trúc của CryptDB.....	28
Hình 2.2. Môi đe dọa các DBA đánh cắp dữ liệu	30
Hình 2.3. EQ Onion.....	35
Hình 2.4. ORD Onion	36
Hình 2.5. SEARCH và ADD Onion	37
Hình 2.6. Các lớp mã hóa Onion và các lớp tính toán được phép	39
Hình 2.7. Các lớp mã hóa của các cột.....	46
Hình 2.8. Lớp mã hóa của các cột sau bước 1	47
Hình 2.9. Kiến trúc Relational Cloud.....	59

Hình 3.1. Mô hình hệ thống	62
Hình 3.2. Lưu đề hoạt động	63
Hình 3.3. Giao diện ứng dụng thử nghiệm.....	64
Hình 3.4. Cập nhật Ubuntu	68
Hình 3.5. Tải CryptDB về máy	69
Hình 3.6. Chạy kịch bản cài đặt CryptDB	69
Hình 3.7. Cài đặt CryptDB thành công.....	70
Hình 3.8. Chạy proxy trên Web server	71
Hình 3.9. Truy cập ứng dụng web.....	71
Hình 3.10. Đăng nhập vào mysql bằng tài khoản root.....	72
Hình 3.11. Tạo cơ sở dữ liệu trên ứng dụng	73
Hình 3.12. Hoạt động của CryptDB khi tạo cơ sở dữ liệu.....	73
Hình 3.13. Cơ sở dữ liệu được lưu trên Database server	73
Hình 3.14. Sử dụng một vài chức năng của ứng dụng web	74
Hình 3.15. Hoạt động tại CryptDB	74
Hình 3.16. Dữ liệu trên Database server được mã hóa hoàn toàn	75
Hình 3.17. So sánh thông lượng của phpBB.....	77