

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

VŨ ĐỨC HÙNG

**NGHIÊN CỨU MỘT SỐ VẤN ĐỀ
BẢO VỆ THÔNG TIN TRONG HỆ THỐNG TÍNH TOÁN LƯỚI**

LUẬN VĂN THẠC SĨ: KHOA HỌC MÁY TÍNH

Thái Nguyên- 2012

LỜI CẢM ƠN

Trước tiên tôi xin gửi lời cảm ơn chân thành nhất đến thầy PGS. TS . Trịnh Nhật Tiến đã định hướng và nhiệt tình hướng dẫn, giúp đỡ tôi rất nhiều về mặt chuyên môn trong quá trình làm luận văn.

Tôi xin gửi lời biết ơn sâu sắc đến các thầy, các cô đã giảng dạy và truyền đạt những kinh nghiệm quý báu cho chúng tôi trong suốt hai năm học cao học tại trường Đại học CNTT&TT - Đại học Thái Nguyên.

Tôi xin cảm ơn các đồng nghiệp, những người luôn gần gũi động viên, chia sẻ cùng tôi trong suốt thời gian học tập và làm làm luận văn tốt nghiệp.

Xin cảm ơn gia đình và các bạn của tôi, những người đã luôn bên cạnh, động viên và khích lệ tôi để có được kết quả như ngày hôm nay.

Cuối cùng tôi chúc các thầy, các cô, các bạn, những người thân yêu nhất của tôi sức khỏe, hạnh phúc và thành đạt trong cuộc sống.

Thái Nguyên, tháng 10 năm 2012

Vũ Đức Hùng



LỜI CAM ĐOAN

Tôi là Vũ Đức Hùng, học viên lớp cao học khoá 2010-2012 ngành CNTT, chuyên ngành Khoa học máy tính. Tôi xin cam đoan bài luận văn "Nghiên cứu một số vấn đề Bảo vệ thông tin trong Hệ thống tính toán lưới" là do tôi nghiên cứu, tìm hiểu dưới sự hướng dẫn của PGS.TS.Trịnh Nhật Tiến, không phải sự sao chép của người khác. Tôi xin chịu trách nhiệm về lời cam đoan này.

Thái Nguyên, tháng 10 năm 2012

Tác giả

Vũ Đức Hùng

Lớp Cao học KHMT 2010-2012



MỤC LỤC

LỜI CẢM ƠN	i
LỜI CAM ĐOAN	ii
MỤC LỤC.....	iii
DANH MỤC BẢNG.....	v
DANH MỤC HÌNH	vi
MỞ ĐẦU	1
<i>Chương 1. KHÁI QUÁT VỀ HỆ THỐNG TÍNH TOÁN LƯỚI</i>	2
VÀ BẢO VỆ THÔNG TIN TRONG TÍNH TOÁN LƯỚI	2
1.1. KHÁI QUÁT VỀ HỆ THỐNG TÍNH TOÁN LƯỚI	2
1.1.1. Khái niệm Tính toán lưới	2
1.1.2. Lợi ích của tính toán lưới	4
1.1.2.1. Khai thác những nguồn tài nguyên chưa được sử dụng đúng mức	4
1.1.2.2. Giúp cân bằng trong sử dụng tài nguyên.....	4
1.1.2.3. Khả năng thực hiện tính toán song song	5
1.1.2.4. Chia sẻ nguồn tài nguyên đặc biệt.....	6
1.1.2.5. Phạm vi ứng dụng	6
1.1.3. Các thành phần của hệ thống tính toán lưới	7
1.1.4. Kiến trúc chung của lưới	8
1.2. BẢO VỆ THÔNG TIN TRONG TÍNH TOÁN LƯỚI.....	12
1.2.1. Vấn đề cơ bản của một hệ thống tính toán lưới.....	12
1.2.1.1. Bảo vệ thông tin	12
1.2.1.2. Lập lịch và quản lý tài nguyên.....	12
1.2.1.3. Dịch vụ thông tin.....	13
1.2.1.4. Quản lý dữ liệu.....	13
1.2.2. Hệ thống bảo vệ thông tin	13
1.2.2.1. Một số khái niệm.....	13
1.2.2.2. Yêu cầu an toàn thông tin trên lưới	15
1.2.2.3. Các chính sách bảo đảm an toàn thông tin	18
1.2.2.4. Kiến trúc bảo vệ thông tin.....	20
1.2.2.5. Cơ sở hạ tầng bảo vệ thông tin trong lưới tính toán	25
<i>Chương 2. VẤN ĐỀ BẢO VỆ THÔNG TIN</i>	28
TRONG HỆ THỐNG TÍNH TOÁN LƯỚI	28
2.1. VẤN ĐỀ XÁC THỰC THỰC THỂ SỬ DỤNG LƯỚI	28
2.1.1. Phương pháp sử dụng chữ ký số.....	28
2.1.1.1. Sơ đồ chữ ký số [2]	28
2.1.1.2. Chữ ký RSA	29
2.1.1.3. Chữ ký Elgamal.....	30
2.1.1.4. Quy trình tạo và kiểm tra chữ ký số.....	31
2.1.2. Sử dụng Chữ ký số xác thực người sử dụng	35
2.2. VẤN ĐỀ BẢO VỆ THÔNG TIN TRÊN ĐƯỜNG TRUYỀN LƯỚI.....	36
2.2.1. Phương pháp mã hoá	36
2.2.1.1. Hệ mã hoá [2]	36

2.2.1.2. Hệ mã hoá khoá đối xứng.....	37
2.2.1.3. Hệ mã hoá khoá phi đối xứng.....	49
2.2.1.4. Sử dụng phương pháp mã hoá bảo mật thông tin trên đường truyền lưới.....	54
2.2.2. Phương pháp tạo đại diện thông điệp.....	55
2.2.2.1. Cấu trúc hàm băm mật mã.....	55
2.2.2.2. Đặc tính của hàm băm.....	56
2.2.2.3. Thuật toán băm SHA.....	56
2.2.2.4. Sử dụng phương pháp tạo đại diện thông điệp để kiểm tra tính toàn vẹn.....	60
Chương 3. THỬ NGHIỆM CHƯƠNG TRÌNH BẢO VỆ THÔNG TIN	61
3.1. THỬ NGHIỆM CHƯƠNG TRÌNH MÃ HOÁ.....	61
3.1.1. Bài toán.....	61
3.1.2. Cài đặt chương trình.....	61
3.1.3. Các thành phần chương trình.....	61
3.1.4. Sử dụng chương trình.....	61
3.2. THỬ NGHIỆM CHƯƠNG TRÌNH KÝ SỐ.....	64
3.2.1. Bài toán.....	64
3.2.2. Cài đặt chương trình.....	64
3.2.3. Các thành phần chương trình.....	64
3.2.4. Sử dụng chương trình.....	65
KẾT LUẬN	67
TÀI LIỆU THAM KHẢO	68

DANH MỤC BẢNG

Bảng 2.1 Bảng hoán vị khởi đầu	42
Bảng 2.2 Bảng khoá chuyển đổi	42
Bảng 2.3 Bảng số bit dịch của một vòng	43
Bảng 2.4 Bảng hoán vị nén	43
Bảng 2.5 Bảng hoán vị mở rộng E	44
Bảng 2.6 Hộp S thứ nhất	44
Bảng 2.7 Hộp S thứ hai	45
Bảng 2.8 Hộp S thứ ba	45
Bảng 2.9 Hộp S thứ tư	45
Bảng 2.10 Hộp S thứ năm	45
Bảng 2.11 Hộp S thứ sáu	46
Bảng 2.12 Hộp S thứ bảy	46
Bảng 2.13 Hộp S thứ tám	46
Bảng 2.14 Hộp hoán vị P	47
Bảng 2.15 Bảng hoán vị cuối cùng	47

DANH MỤC HÌNH

Hình 1.1 Minh hoạ về tính toán lưới.....	3
Hình 1.2 Minh hoạ tổ chức ảo.....	5
Hình 1.3 Các thành phần theo mô hình chức năng.....	7
Hình 1.4 Kiến trúc phân tầng lưới.....	9
Hình 1.5 Miền tin tưởng chung của các tổ chức ảo.....	17
Hình 1.6 Mô hình kiến trúc bảo vệ thông tin trong hệ thống tính toán lưới.....	21
Hình 2.1 Sơ đồ tạo chữ ký số của thông điệp.....	32
Hình 2.2 Sơ đồ đọc và xác thực một tài liệu được ký bằng chữ ký số.....	34
Hình 2.3 Mã hoá với khoá mã và giải mã giống nhau.....	37
Hình 2.4 Sơ đồ mã hoá DES.....	39
Hình 2.5 Một vòng lặp của DES.....	41
Hình 2.6 Mã hoá với khoá mã và giải mã khác nhau.....	49
Hình 2.7 Bảo mật thông tin bằng mã hóa theo đường truyền.....	54
Hình 2.8 Xử lý thông tin trong SHA-1.....	59
Hình 2.9 Kiểm tra tính toàn vẹn bằng phương pháp tạo đại diện thông điệp.....	60
Hình 3.1 Chương trình mã hoá.....	62
Hình 3.2 Tạo khoá bí mật, công khai.....	62
Hình 3.3 Mã hoá chuỗi Hexadecimal.....	63
Hình 3.4 Giải mã dùng hệ mã hoá RSA.....	63
Hình 3.5 Mã hoá file dữ liệu dùng hệ DES.....	64
Hình 3.6 Giải mã file dữ liệu dùng hệ DES.....	64
Hình 3.7 Chương trình ký số RSA.....	65
Hình 3.8 Tạo khoá bí mật, công khai.....	65
Hình 3.9 Ký tài liệu.....	66
Hình 3.10 Xác thực chữ ký.....	66

MỞ ĐẦU

Ngày nay, với sự phát triển vượt bậc của khoa học kỹ thuật và công nghệ, đã xuất hiện những bài toán trong nhiều lĩnh vực đòi hỏi sức mạnh tính toán mà một máy tính riêng lẻ không thể đảm trách. Xuất phát từ những nhu cầu đó, các kỹ thuật tính toán song song, tính toán phân tán đã được đề xuất và đã phần nào đáp ứng được các yêu cầu này. Tuy nhiên, con người vẫn muốn có một sức mạnh tính toán lớn hơn, với khả năng chia sẻ tài nguyên giữa mọi người trên phạm vi toàn cầu, khả năng tận dụng các phần mềm cũng như tài nguyên vật lý phân tán cả về mặt địa lý. Tính toán lưới ra đời nhằm giải quyết yêu cầu trên.

Tính toán lưới đã mở ra các giải pháp mới cho các ứng dụng đòi hỏi khả năng tính toán lớn. Tính toán lưới có thể được sử dụng cho các bài toán nghiên cứu về sinh học, y học, vật lý, hoá học... cũng như các ứng dụng trong phân tích và đánh giá tài chính, khai thác dữ liệu và rất nhiều các loại ứng dụng khác.

Bảo vệ thông tin là một trong những vấn đề quan trọng nhất trong hệ thống tính toán lưới. Vì vậy, mục đích của luận văn là tìm hiểu, trình bày tổng quan về Hệ thống tính toán lưới. Trên cơ sở đó đi sâu tìm hiểu một số phương pháp bảo vệ thông tin trong hệ thống tính toán lưới.

Bố cục của luận văn gồm:

Chương 1. Khái quát về Hệ thống tính toán lưới và bảo vệ thông tin trong tính toán lưới, trình bày khái niệm, các thành phần, kiến trúc và lợi ích của tính toán lưới. Các vấn đề cơ bản của tính toán lưới và hệ thống bảo vệ thông tin.

Chương 2. Một số vấn đề bảo vệ thông tin trong hệ thống tính toán lưới, trình bày việc giải quyết hai vấn đề xác thực thực thể sử dụng lưới và bảo vệ thông tin trên đường truyền lưới.

Chương 3. Thử nghiệm chương trình bảo vệ thông tin, cài đặt chương trình mã hoá và chương trình ký số.

Phần kết luận, trình bày tóm tắt kết quả đạt được và hướng phát triển.

Chương 1. KHÁI QUÁT VỀ HỆ THỐNG TÍNH TOÁN LƯỚI VÀ BẢO VỆ THÔNG TIN TRONG TÍNH TOÁN LƯỚI

1.1.KHÁI QUÁT VỀ HỆ THỐNG TÍNH TOÁN LƯỚI

1.1.1. Khái niệm Tính toán lưới

Tùy theo quan niệm và cách xây dựng hệ thống trong thực tế, mỗi tổ chức hoặc cá nhân đưa ra những định nghĩa khác nhau về lưới.

Một định nghĩa về Lưới tính toán (Computing Grid) khá hoàn chỉnh được đưa ra bởi tiến sĩ Ian Foster như sau:

“ Lưới tính toán là một loại hệ thống song song, phân tán cho phép chia sẻ, lựa chọn. Kết hợp các tài nguyên phân tán theo địa lý, thuộc nhiều tổ chức khác nhau, dựa trên tính sẵn sàng, khả năng chi phí của chúng và yêu cầu về chất lượng dịch vụ (QoS) của người dùng để giải quyết các bài toán, ứng dụng có quy mô lớn trong khoa học, kỹ thuật và thương mại. Từ đó hình thành nên các “ tổ chức ảo” (Virtual Organization(VO)), các liên minh tạm thời giữa các tổ chức và tập đoàn, liên kết với nhau để chia sẻ tài nguyên và / hoặc kỹ năng nhằm đáp ứng tốt hơn các cơ hội kinh doanh hoặc các dự án có nhu cầu lớn về tính toán và dữ liệu, toàn bộ việc liên minh này dựa trên các mạng máy tính”.

Còn dưới quan điểm của một số công ty và liên minh phát triển lưới trên thế giới thì tính toán lưới được định nghĩa như sau [8]:

Định nghĩa của Oracle: Tính toán lưới là việc liên kết nhiều máy chủ và thiết bị lưu trữ thành một siêu máy tính nhằm tối ưu hóa được tính ưu việt của các hệ thống máy chủ cũng như hệ thống ứng dụng, nhờ đó giảm thiểu đến mức thấp nhất chi phí.

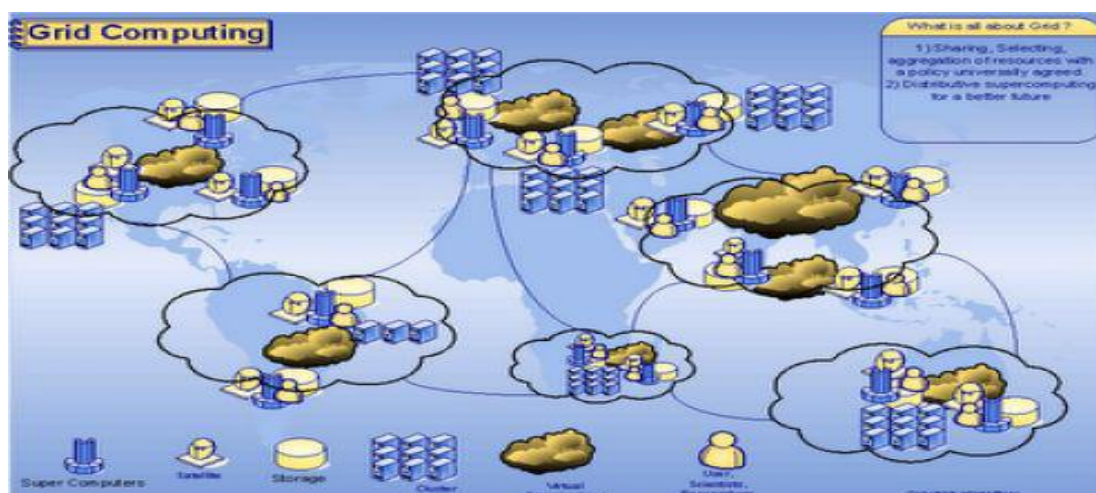
Định nghĩa của IBM: Tính toán lưới là một môi trường tính toán ảo. Môi trường này cho phép bố trí song song, linh hoạt, chia sẻ, tuyển lựa, tập hợp các nguồn tài nguyên hỗn hợp về mặt địa lý, tùy theo mức độ sẵn sàng, hiệu suất, chi phí của các tài nguyên tính toán và yêu cầu về chất lượng dịch vụ của người sử dụng.

Định nghĩa của liên minh điện toán lưới: Môi trường tính toán lưới được hiểu như một hạ tầng kết nối hệ thống máy tính, hệ thống mạng, hệ thống cơ sở dữ liệu được sở hữu và quản lý bởi nhiều tổ chức, cá nhân nhằm cung cấp môi trường tính toán ảo duy nhất với hiệu năng cao cho người sử dụng.

Trong luận văn sẽ không đưa ra định nghĩa nào, nhưng để có một cái nhìn toàn diện về tính toán lưới, ta xem xét khái niệm tính toán lưới theo một số đặc điểm chung sau:

- *Kích thước lớn:* Theo số lượng tài nguyên và khoảng cách địa lý giữa chúng.
- *Phân tán:* Có độ trễ đáng kể trong truyền dữ liệu, tài nguyên trải dài trên các vùng địa lý khác nhau.
- *Động:* Các tài nguyên có thể thay đổi khi ứng dụng đang được thực hiện.
- *Hỗn tạp:* Kiến trúc và tính chất của các nút lưới có thể là hoàn toàn khác nhau. Tài nguyên lưới có thể là các máy đơn hoặc mạng con khác nhau.
- *Vượt qua phạm vi một tổ chức:* Có nhiều trạm và các chính sách truy nhập có thể khác nhau trên các trạm, tổng thể lưới sẽ tạo ra một tổ chức ảo thống nhất.

Có thể hình dung đơn giản một lưới bao gồm một tập các tài nguyên đa dạng (còn gọi là nút lưới có thể là PC, hệ thống lưu trữ....) thuộc về nhiều tổ chức khác nhau nhằm giải quyết một bài toán nào đó.



Hình 1.1 Minh họa về tính toán lưới