**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**======\*\*\*======**



BÁO CÁO BTL THUỘC HỌC PHẦN:

AN TOÀN VÀ BẢO MẬT THÔNG TIN

**ĐỀ TÀI: XÂY DỰNG CÁC GIẢI PHÁP VỀ CHÍNH SÁCH ĐẢM BẢO AN TOÀN, AN TOÀN MẠNG VÀ HẠ TẦNG CHO HỆ THỐNG QUẢN LÍ ĐIỀU HÀNH ĐÀO TẠO TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

|  |  |
| --- | --- |
| GVHD: | ThS.TRẦN PHƯƠNG NHUNG |
| Nhóm - Lớp: | 14 – KTPM2-K12 |
| Thành viên : | Nguyễn Ngọc Vinh |
|  | Lưu Tuấn Vũ |
|  | Vũ Đức Vượng |
|  | Nguyễn Thành Vy |
|  | Nguyễn Thị Yến |

Hà nội, Năm 2020

Mục Lục

[Phần 1: Tổng quan về hệ thống 4](#_Toc43910894)

[1. Tìm hiểu về hệ thống (Nguyễn Thành Vy) 4](#_Toc43910895)

[1.1. Mô hình mạng Client – Server 4](#_Toc43910896)

[1.2. Mô hình mạng ngang hàng 6](#_Toc43910897)

[2. Chỉ định các chính sách, quy định, chỉ dẫn cần phải có trong hệ thống, nội dung dự kiến của văn bản (Vũ Đức Vượng) 9](#_Toc43910898)

[3. Các văn bản chi tiết cho các chính sách, quy định, chỉ dẫn(Lưu Tuấn Vũ) 10](#_Toc43910899)

[4. Tìm hiểu các giải pháp an toàn mạng cho hệ thống mạng hỗ trợ quá trình hoạt động và điều hành (thiết bị, phần mềm, ...) (Nguyễn Ngọc Vinh) 10](#_Toc43910900)

[4.1. Thực trạng mất an toàn ninh an toàn mạng. 10](#_Toc43910901)

[4.2. Các nguy cơ gây mất an toàn an ninh mạng. 10](#_Toc43910902)

[4.3. Một số giải pháp an toàn mạng. 10](#_Toc43910903)

[4.3.1. Công nghệ tường lửa (Firewall). 10](#_Toc43910904)

[4.3.2. Công nghệ phát hiện và ngăn xâm nhập mạng IDS/IPS. 12](#_Toc43910905)

[4.3.3. Công nghệ mạng LAN ảo (VLAN) 13](#_Toc43910906)

[4.3.4. Một số giải pháp bảo mật mạng khác không nên bỏ qua 13](#_Toc43910907)

[5. Các hạ tầng mạng cần có nếu cần tách biệt mạng nội bộ và mạng internet (Nguyễn Thị Yến) 14](#_Toc43910908)

[5.1. Hub là gì ? 14](#_Toc43910909)

[5.2. Thiết bị chuyển mạch - Switch 14](#_Toc43910910)

[5.3. Router - Bộ định tuyến là gì ? 17](#_Toc43910911)

[5.4. Giải pháp thiết kế mở rộng hệ thống mạng được xây dựng để đáp ứng các yêu cầu sau: 18](#_Toc43910912)

[5.5. Xác định các nguy cơ gây nguy hiểm cho an toàn mạng 19](#_Toc43910913)

[5.6. Giải pháp cho phần cứng 19](#_Toc43910914)

[Phần 2: Ứng dụng cài đặt minh họa 20](#_Toc43910915)

[2. ….. 20](#_Toc43910916)

[3. ….. 20](#_Toc43910917)

[4. Cài đặt minh họa các chính sách đảm bảo an toàn cho hệ thống(Lưu Tuấn Vũ) 20](#_Toc43910918)

[4.1. Lớp sử lý MyCrypto 20](#_Toc43910919)

[4.2. Lớp sử lý sự kiện 23](#_Toc43910920)

[4.3. Kết Quả 24](#_Toc43910921)

[5. Cài đặt minh hoạ các chính sách đảm bảo an toàn cho hệ thống (Vũ Đức Vượng) 25](#_Toc43910922)

[5.1. Lớp xử lý với thuật toán DES 26](#_Toc43910923)

[} 26](#_Toc43910924)

[5.2. Lớp xử lý sự kiện 28](#_Toc43910925)

[5.3. Lớp xử lý khoá 30](#_Toc43910926)

[5.4. Kết quả 31](#_Toc43910927)

[6. ….. 33](#_Toc43910928)

**Lời mở đầu**

Thông tin là một tài sản vô cùng quý giá của chính phủ, tổ chức, doannh nghiệp hay bất cứ một cấ nhân nào. Chính vì vậy việc trao đổi và giữ bí mật thông tin là một vấn đề rất quan trọng. Ngày nay, sự xuất hiện Internet và mạng máy tínḥ đã giúp cho việc trao đổi thông tin trở nên nhanh gọn, dễ dàng. E-mail cho phép ng­ười ta nhận hay gửi thư­ ngay trên máy tính của mình, E-business cho phép thực hiện các giao dịch buôn bán trên mạng, ... Bảo mật mạng có thể hiểu là cách bảo vệ, đảm bảo an toàn cho các thành phần mạng bao gồm dữ liệu, thiết bị, cơ sở hạ tầng mạng và đảm bảo mọi tài nguyên trên mạng tránh bị đánh cắp thông tin, đồng thời đảm bảo an toàn, an toàn mạng và hạ tầng quản lý của trường.

Việc đảm bảo an toàn cho hệ thống cần đặt lên hàng đầu trước khi xây dựng một hệ thống cho mọi người sử dụng. Vậy nên việc sử dụng các thiết bị tường lửa trong hệ thống mạng để đảm bảo an toàn, an toàn mạng là rất cần thiết. Nhằm ngăn chặn các kết nối không mong muốn, giảm nguy cơ mất kiểm soát hệ thống hoặc tấn công và lây nhiễm các chương trình và mã độc hại, bảo đảm bí mật thông tin, bảo đảm toàn vẹn (bảo toàn) thông tin với người không được phép truy cập, bảo đảm xác thực nguồn gốc của thông tin, bảo đảm sẵn sàng cung cấp thông tin cho người được phép,… Để bảo đảm ATTT, người ta sử dụng nhiều công cụ như mã hóa, giấu tin, kiểm soát truy cập thông tin, tìm diệt Virus phá hoại thông tin, … Ngày nay người ta giao dịch từ xa qua mạng máy tính, để tránh những sự cố xảy ra khi giao dịch, người ta phải có luật giao dịch điện tử. Tại nhiều nước và nước ta đã có “luật giao dịch điện tử”. Nhờ mạng máy tính và Hệ thống bảo đảm ATTT, tại mọi nơi, mọi lúc, người ta có thể giao dịch với nhau để thực hiện các hoạt động kinh tế xã hội, như mua bán qua mạng, thanh toán qua mạng, đấu thầu từ xa,…

Trong bài báo cáo này chúng em xin được trình bày nghiên cứu về vấn đề: *Xây dựng các giải pháp về chính sách đảm bảo an toàn, an toàn mạng và hạ tầng cho hệ thống quản lý điều hành đào tạo trường đại học Công nghiệp Hà Nội.* Dù đã cố gắng rất nhiều trong quá trình tìm hiểu, nghiên cứu và viết báo cáo, nhưng chắc chắn không thể tránh khỏi những hạn chế và thiếu sót. Chúng em rất mong được những ý kiến đóng góp và chỉ bảo thêm từ thầy cô giáo giúp cho bài tập lớn của nhóm chúng em được hoàn thiện hơn.

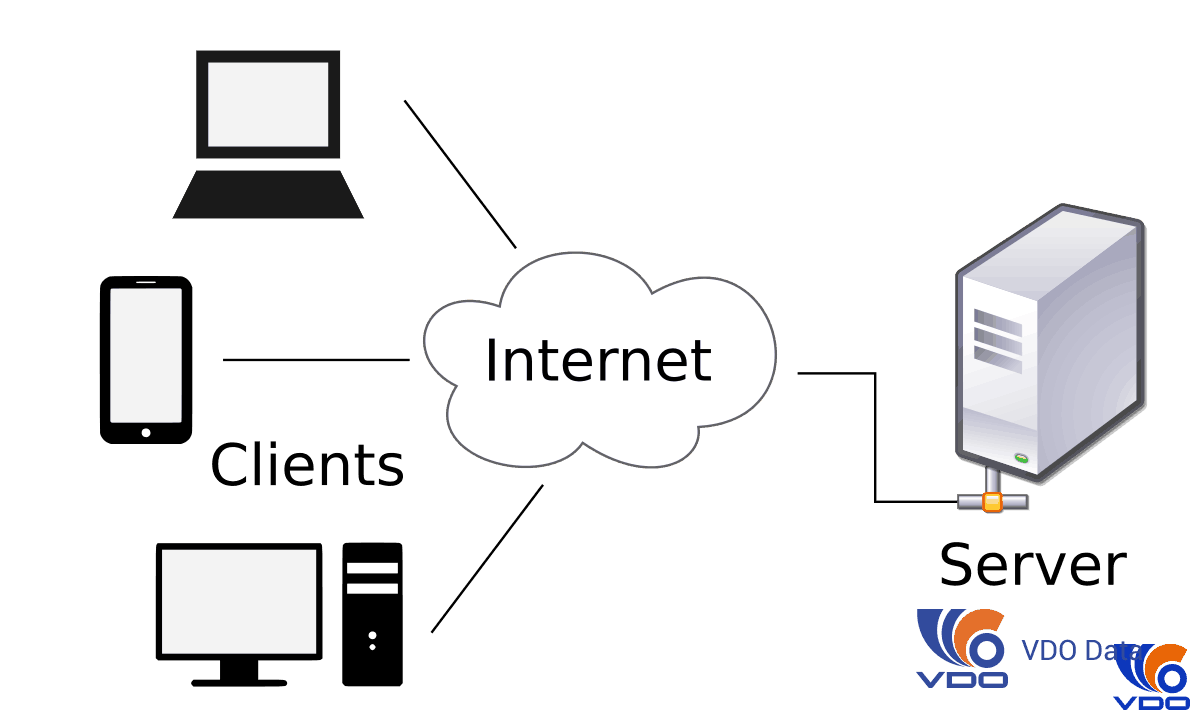
*Chúng em xin chân thành cảm ơn !*

# Phần 1: Tổng quan về hệ thống

## Tìm hiểu về hệ thống (Nguyễn Thành Vy)

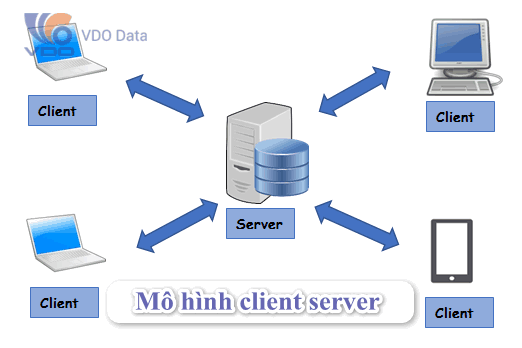
### Mô hình mạng Client – Server

* Client server là một mô hình thông dụng trong mạng máy tính bao gồm 2 thành phần chính là máy chủ server và máy khách client.



*Hình ảnh minh họa*

* [Mô hình client server](https://vdodata.vn/tim-hieu-ve-mo-hinh-client-server-va-client-server-la-gi/) hay còn được gọi là mô hình khách – chủ
* Trong mô hình client server thì máy khách là các máy tính, các thiết bị điện tử như máy in, máy fax,….các máy khách client gửi yêu cầu đến máy chủ server. máy chủ server tiếp nhận yêu cầu, xử lý các yêu cầu đó và trả về kết quả.



*Hình ảnh minh họa*

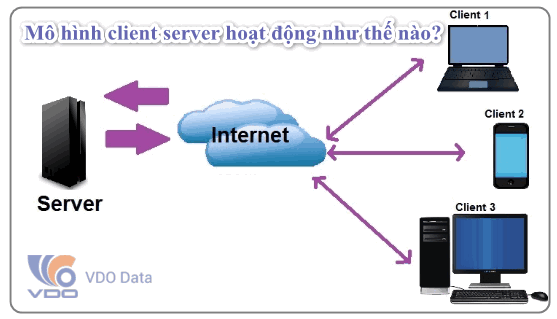
* Ưu điểm mô hình client server :

Ưu điểm của mô hình client server là với mô hình client server thì mọi thứ dường như đều nằm trên bàn của người sử dụng, nó có thể truy cập dữ liệu từ xa (bao gồm các công việc như gửi và nhận file, tìm kiếm thông tin,…) với nhiều dịch vụ đa dạng mà mô hình cũ không thể làm được. Mô hình client/server cung cấp một nền tảng lý tưởng cho phép tích hợp các kỹ thuật hiện đại như mô hình thiết kế hướng đối tượng, hệ chuyên gia, hệ thông tin địa lý (GIS)…

* Nhược điểm mô hình client server :

Một trong những vấn đề nảy sinh trong mô hình này đó là tính an toàn và bảo mật thông tin trên mạng. Do phải trao đổi dữ liệu giữa 2 máy ở 2 khu vực khác nhau cho nên dễ dàng xảy ra hiện tượng thông tin truyền trên mạng bị lộ.

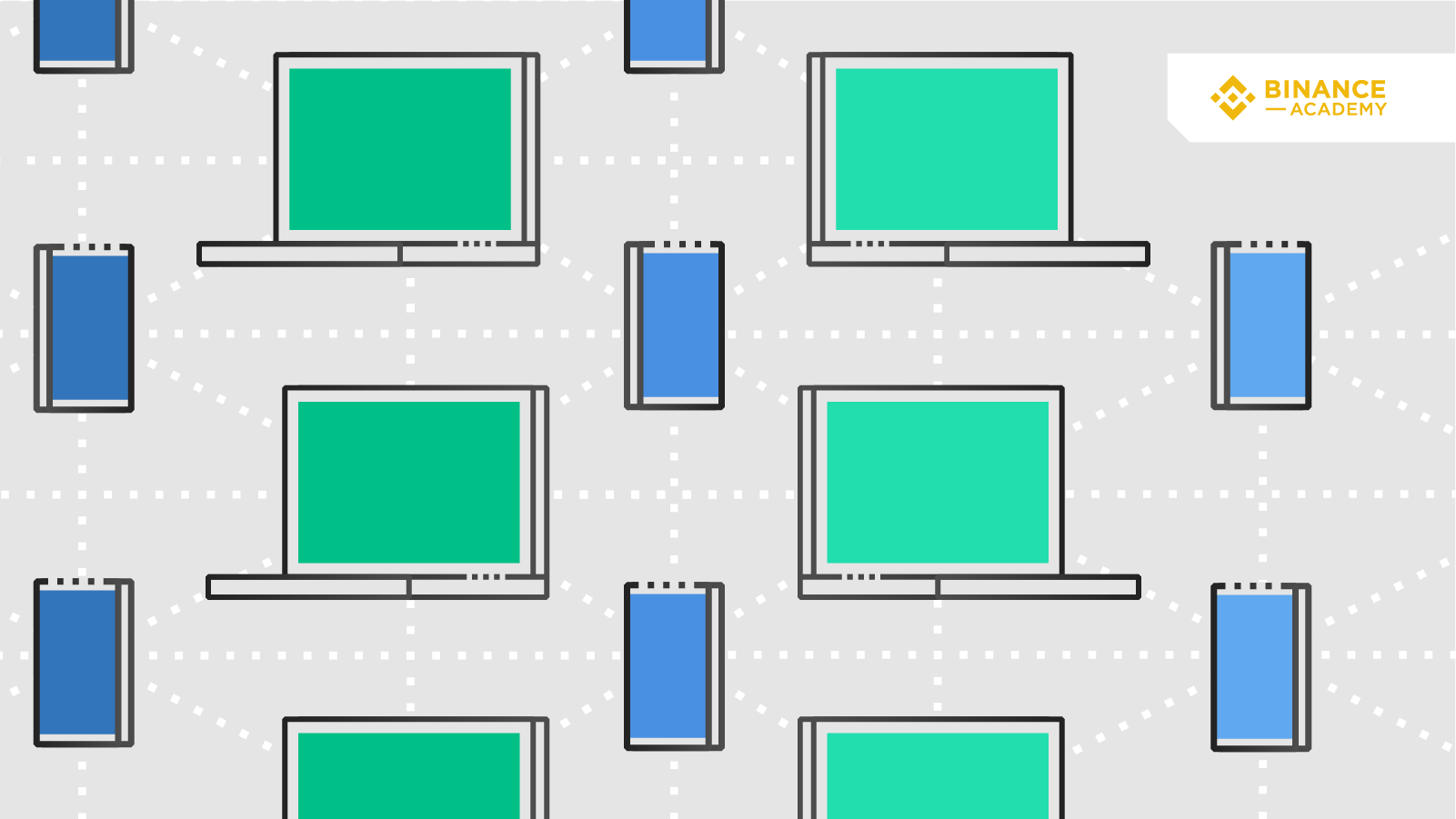
* Mô hình client server hoạt động :
* Client trong mô hình client/server, người ta còn định nghĩa cụ thể cho một máy client là một máy trạm mà chỉ được sử dụng bởi 1 người dùng với để muốn thể hiện tính độc lập cho nó. Máy client có thể sử dụng các hệ điều hành bình thường như Win9x, DOS, OS/2… Bản thân mỗi một client cũng đã được tích hợp nhiều chức năng trên hệ điều hành mà nó chạy, nhưng khi được nối vào một mạng LAN, WAN theo mô hình client/server thì nó còn có thể sử dụng thêm các chức năng do hệ điều hành mạng (NOS) cung cấp với nhiều dịch vụ khác nhau (cụ thể là các [dịch vụ máy chủ](https://vdodata.vn/thue-may-chu-chay-game-server/" \t "_blank) trên mạng này cung cấp), ví dụ như nó có thể yêu cầu lấy dữ liệu từ một server hay gửi dữ liệu lên server đó…
* Thực tế trong các ứng dụng của mô hình client/server, các chức năng hoạt động chính là sự kết hợp giữa client và server với sự chia sẻ tài nguyên, dữ liệu trên cả hai máy Vai trò của client Trong mô hình client/server, client được coi như là người sử dụng các dịch vụ trên mạng do một hoặc nhiều máy chủ cung cấp và server được coi như là người cung cấp dịch vụ để trả lời các yêu cầu của các clients. Điều quan trọng là phải hiểu được vai trò hoạt động của nó trong một mô hình cụ thể, một máy client trong mô hình này lại có thể là server trong một mô hình khác. Ví dụ cụ thể như một máy trạm làm việc như một client bình thường trong mạng LAN nhưng đồng thời nó có thể đóng vai trò như một máy in chủ (printer server) cung cấp dịch vụ in ấn từ xa cho nhiều người khác (clients) sử dụng. Client được hiểu như là bề nổi của các dịch vụ trên mạng, nếu có thông tin vào hoặc ra thì chúng sẽ được hiển thị trên máy client.



*Hình ảnh minh họa.*

### Mô hình mạng ngang hàng

* Khái niệm Mạng Ngang Hàng :
* Trong khoa học máy tính, mạng ngang hàng, hay mạng đồng đẳng (P2P) bao gồm một nhóm các thiết bị cùng lưu trữ và chia sẻ tập tin. Mỗi người tham gia (nút) hoạt động như một đồng đẳng riêng lẻ. Thông thường, tất cả các nút có sức mạnh như nhau và thực hiện các nhiệm vụ giống nhau.
* Trong công nghệ tài chính, thuật ngữ ngang hàng thường dùng để mô tả quá trình trao đổi tiền mã hóa hoặc tài sản kỹ thuật số thông qua mạng phân tán. Nền tảng P2P cho phép người mua và người bán thực hiện giao dịch mà không cần đến trung gian. Trong một số trường hợp, các trang web cũng có thể cung cấp một môi trường P2P để kết nối người cho vay với người vay.
* Kiến trúc P2P có thể phù hợp với nhiều trường hợp sử dụng khác nhau, nhưng nó trở nên đặc biệt phổ biến vào những năm 1990 khi các chương trình chia sẻ tệp đầu tiên được tạo. Ngày nay, mạng P2P là yếu tố cốt lõi của hầu hết các loại tiền mã hóa, chiếm một phần lớn trong ngành công nghiệp blockchain. Tuy nhiên, chúng cũng được khai thác trong các ứng dụng điện toán phân tán khác, bao gồm các công cụ tìm kiếm web, nền tảng phát trực tuyến, thị trường trực tuyến và giao thức web Hệ thống tệp tin liên hành tinh (IPFS).



*Hình ảnh minh họa.*

* Cách hoạt động :
* Về bản chất, hệ thống ngang hàng được duy trì bởi một mạng lưới người dùng phân tán. Mạng này thường không có quản trị viên trung tâm hoặc máy chủ vì mỗi nút lưu trữ một bản sao của các tệp và mỗi nút đóng vai trò như một máy khách và máy chủ cho các nút khác. Do đó, mỗi nút có thể tải tệp về từ các nút khác hoặc tải lên tệp cho các nút khác. Đây là điểm khác biệt giữa các mạng ngang hàng với các hệ thống máy chủ-máy khách truyền thống hơn, trong đó các thiết bị máy khách tải xuống các tệp từ một máy chủ tập trung.
* Trên mạng ngang hàng, các thiết bị được kết nối chia sẻ các tệp được lưu trữ trên ổ cứng của chúng. Sử dụng các ứng dụng phần mềm được thiết kế để làm trung gian cho việc chia sẻ dữ liệu, người dùng có thể truy vấn các thiết bị khác trên mạng để tìm và tải xuống các tệp. Khi người dùng đã tải xuống một tệp, họ có thể đóng vai trò là nguồn của tệp đó. Nói cách khác, khi một nút hoạt động như một máy khách, họ tải xuống các tệp từ các nút khác trên mạng. Nhưng khi họ hoạt động như một máy chủ, họ là nguồn mà các nút khác có thể tải xuống các tệp. Tuy nhiên, trên thực tế, các nút có thể thực hiện hai chức năng cùng một lúc (ví dụ: tải xuống tệp A và tải lên tệp B).
* Vì mỗi nút đều có chức năng lưu trữ, truyền và nhận tệp, mạng ngang hàng có xu hướng hoạt động nhanh và hiệu quả hơn khi cộng đồng người dùng của họ phát triển lớn hơn. Ngoài ra, kiến trúc phân tán của họ làm cho các hệ thống P2P có khả năng chống lại các cuộc tấn công mạng rất cao. Không giống như các mô hình truyền thống, mạng P2P không có sự hư hỏng tại một điểm.
* Ưu điểm của mạng ngang hàng :
* Trong mô hình máy chủ – máy khách, hiệu suất giảm xuống nếu có nhiều người dùng, vì băng thông sẽ được chia sẻ cho nhiều người dùng hơn. Trong các mạng ngang hàng, càng có nhiều người dùng thì càng làm cho mạng hiệu quả hơn. Càng nhiều người dùng tạo một file cụ thể có sẵn từ ổ cứng của họ thì người dùng mới có thể nhận file đó càng dễ dàng hơn. Thay vì lấy toàn bộ file từ một người dùng, bạn đang lấy các phần nhỏ hơn từ hàng trăm hoặc hàng nghìn người khác. Ngay cả khi họ chỉ có một chút băng thông trống cho bạn. Sau đó, đến lượt bạn đóng góp để phân phối các file một lần nữa.
* Các mạng ngang hàng có tính bảo mật cao hơn so với kiến trúc máy khách-máy chủ truyền thống. Việc phân phối các chuỗi khối trên một số lượng lớn các nút làm cho chúng hầu như có khả năng chống lại các cuộc tấn công đã được sử dụng để tấn công nhiều hệ thống. Tương tự như vậy, vì phần lớn các nút phải đạt được sự đồng thuận trước khi dữ liệu mới được thêm vào blockchain, nên kẻ tấn công gần như không thể thay đổi dữ liệu.
* Hạn chế của mạng ngang hàng:
* Vì sổ cái phân tán phải được cập nhật trên mỗi nút thay vì trên máy chủ trung tâm, nên việc thêm giao dịch vào blockchain đòi hỏi phải sử dụng những thuật toán phức tạp. Điều này mặc dù giúp tăng khả năng bảo mật, nhưng nó làm giảm đáng kể hiệu suất hoạt động và là một trong những trở ngại chính đến khả năng mở rộng và ứng dụng mạng rộng rãi.
* Hơn nữa, bản chất phân tán của mạng P2P khiến chúng tương đối khó kiểm soát và điều tiết, không chỉ trong phân khúc blockchain. Một số ứng dụng và công ty P2P đã tham gia vào các hoạt động bất hợp pháp và vi phạm bản quyền.

## Chỉ định các chính sách, quy định, chỉ dẫn cần phải có trong hệ thống, nội dung dự kiến của văn bản (Vũ Đức Vượng)

* Bảo mật tài khoản và phân quyền: sử dụng cách mã hóa MD5 cho mật khẩu của tài khoản.
* Phạm vi sử dụng cho mỗi loại tài khoản: ví dụ như giáo viên chỉ được quản lý thông tin sinh viên, nhập điểm và xem các chức năng khác trong phạm vi quyền sử dụng của giáo viên.
* Đối tượng sử dụng: đang công tác và hoạt động trong phạm vi của nhà trường như giáo viên, sinh viên, quản lý đào tạo, … Ngoài ra không ai có quyền xâm phạm vào thông tin có trên hệ thống.
* Lưu trữ thông tin: hệ thống cung cấp các dịch vụ dựa theo thông tin từ phía người dùng cung cấp.

## Các văn bản chi tiết cho các chính sách, quy định, chỉ dẫn(Lưu Tuấn Vũ)

* Chính sách, quy định, chỉ dẫn cần phải có:
* Bảo mật tài khoản và phân quyền: sử dụng cách mã hóa MD5 cho mật khẩu của tài khoản.
* Phạm vi sử dụng cho mỗi loại tài khoản: ví dụ như giáo viên chỉ được quản lý thông tin sinh viên, nhập điểm và xem các chức năng khác trong phạm vi quyền sử dụng của giáo viên.
* Đối tượng sử dụng: đang công tác và hoạt động trong phạm vi của nhà trường như giáo viên, sinh viên, quản lý đào tạo, … Ngoài ra không ai có quyền xâm phạm vào thông tin có trên hệ thống.
* Lưu trữ thông tin: hệ thống cung cấp các dịch vụ dựa theo thông tin từ phía người dùng cung cấp.

## Tìm hiểu các giải pháp an toàn mạng cho hệ thống mạng hỗ trợ quá trình hoạt động và điều hành (thiết bị, phần mềm, ...) (Nguyễn Ngọc Vinh)

## 4.1. Thực trạng mất an toàn ninh an toàn mạng.

Trong hệ thống mạng, vấn đề an toàn và bảo mật thông tin đóng một vai trò hết sức quan trọng. An toàn thiết bị, an toàn dữ liệu, tính bí mật, tin cậy (Condifidentislity), tính xác thực (Authentication), tính toàn vẹn (Integrity), không thể phủ nhận (Non repudiation), khả năng điều khiển truy nhập (Access Control), tính khả dụng, sẵn sàng (Availability).

## 4.2. Các nguy cơ gây mất an toàn an ninh mạng.

* Chèn mã độc, virus vào phần mềm, ứng dụng.
* Xâm nhập qua Internet.
* Xâm nhập từ mạng nội bộ.

## 4.3. Một số giải pháp an toàn mạng.

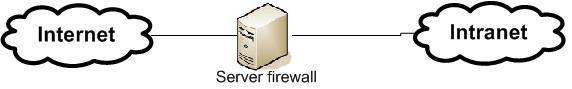
## 4.3.1. Công nghệ tường lửa (Firewall).

* Firewall mềm

Đặc điểm:

* Là những Firewall dưới dạng phần mềm được cài đặt trên Server.
* Tính linh hoạt cao: Có thể thêm bớt các quy tắc, chức năng.
* Firewall mềm hoạt động ở tầng cao hơn Firewall cứng(Tầng ứng dụng).
* Firewall mềm có thể kiểm tra được nội dung của gói tin(Thông qua các từ khóa).

Ví dụ Firewall mềm: Zone Alarm, Norton Firewall.

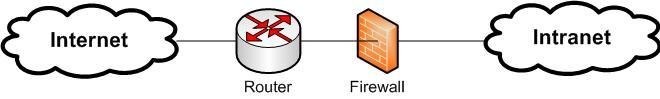


* Firewall cứng

Đặc điểm:

* Là những firewall được tích hợp vào thiết bị phần cứng.
* Không được linh hoạt như Firewall mềm.
* Firewall cứng hoạt động ở tầng thấp hơn Firewall mềm( Tầng Network và tầng Transport)
* Firewall cứng không thể kiểm tra được nội dung của gói tin.

Ví dụ Firewall cứng: NAT ( Network Address Translate).



* Chức năng của Firewall.

Chức năng chính của Firewall là kiểm soát luồng thông tin giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa Intranet và mạng Internet. Cụ thể là:

* Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài ( Từ Intranet ra Internet).
* Cho phép hoặc cấm những dịch vụ từ ngoài truy nhập vào trong( Từ Internet vào Intranet).
* Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.
* Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
* Kiểm soát người dùng và việc truy nhập của người dùng. Kiểm soát nội dung thông tin lưu truyền trên mạng.

### 4.3.2. Công nghệ phát hiện và ngăn xâm nhập mạng IDS/IPS.

* Hệ thống phát hiện xâm nhập(IDS):

Hệ thống phát hiện xâm nhập cung cấp thêm cho việc bảo vệ thông tin mạng ở mức độ cao hơn. IDS cung cấp thông tin về các cuộc tấn công vào hệ thống mạng. Tuy nhiên IDS không tự động cấm hoặc là ngăn chặn các cuộc tấn công.

* Hệ thống ngăn chặn xâm nhập(IPS):

Giải pháp ngăn ngừa xâm nhập nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe dọa tấn công bằng việc loại bỏ lưu lượng mạng bất hợp pháp, trong khi vẫn cho phép các hoạt động hợp pháp được tiếp tục.

IPS ngăn chặn những cuộc tấn công dưới dạng sau:

* Ứng dụng không mong muốn và tấn công kiểu “Trojan horse” nhằm vào mạng và ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và danh sách kiểm soát truy nhập.
* Các tấn công từ chối dịch vụ như “lụt” các gói tin SYN và ICMP bởi việc dùng các thuật toán dựa trên cơ sở “ngưỡng”.
* Sự lạm dụng các ứng dụng và giao thức qua việc sử dụng những qui tắc giao thức ứng dụng và chữ kí.
* Những tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng giới hạn tài nguyên dựa trên cơ sở ngưỡng.
* Những hạn chế của IDS/IPS
* So với Firewall, IDS/ IPS đã thể hiện được nhiều tính năng ưu việt. Nó không chỉ có khả năng phát hiện ra các cuộc tấn công, mà còn chống lại các cuộc tấn công này một cách hữu hiệu. Tuy vậy hệ thống này vẫn còn những hạn chế sau:
* Các sản phẩm IPS không thể nhận biết được trạng thái tầng ứng dụng (chỉ có thể nhận biết được các dòng thông tin trên tầng mạng). Do vậy các cuộc tấn công trên tầng ứng dụng sẽ không bị phát hiện và ngăn chặn.

### 4.3.3. Công nghệ mạng LAN ảo (VLAN)

* Khái niệm VLAN:
* VLAN là một mạng LAN ảo. Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch. Bình thường thì router đóng vai tạo ra miền quảng bá. VLAN là một kỹ thuật kết hợp chuyển mạch lớp 2 và định tuyến lớp 3 để giới hạn miền đụng độ và miền quảng bá. VLAN còn được sử dụng để bảo mật giữa các nhóm VLAN theo chức năng nhóm.
* VLAN là một nhóm các thiết bị mạng không giới hạn theo vị trí vật lý hoặc theo LAN switch mà chúng tham gia kết nối vào.
* VLAN là một segment mạng theo logic dựa trên chức năng, đội nhóm, hoặc ứng dụng của một tổ chức chứ không phụ thuộc vào vị trí vật lý hay kết nối vật lý trong mạng. Tất cả các trạm và server được sử dụng bởi cùng một nhóm làm việc sẽ được đặt trong cùng VLAN bất kể vị trí hay kết nối vật lý của chúng.
* Ưu điểm và ứng dụng của VLAN:
* Ưu điểm của VLAN:
* Lợi ích của VLAN là cho phép người quản trị mạng tổ chức mạng theo logic chứ không theo vật lý nữa. Nhờ đó những công việc sau thực hiện dễ dàng hơn:
* Có tính linh động cao: di chuyển máy trạm trong LAN dễ dàng.
* Thêm máy trạm vào LAN dễ dàng: Trên một switch nhiều cổng, có thể cấu hình VLAN khác nhau cho từng cổng, do đó dẽ dàng kết nối thêm các máy tính với các VLAN.
* Ứng dụng của VLAN:
* Sử dụng VLAN để tạo ra các LAN khác nhau của nhiều máy tính cùng văn phòng.
* Sử dụng VLAN để tạo mạng dữ liệu ảo (Virtual Data Network - VAN)

### 4.3.4. Một số giải pháp bảo mật mạng khác không nên bỏ qua

* Sử dụng phần mềm diệt virus trên hệ thống thường xuyên.
* Đây là hành động không thể thiếu đối với bật kì hệ thống mạng hay hệ thống website nào.
* Thay vì sử dụng những phần mềm diệt virus miễn phí có sẵn, bạn nên đăng kí gói dịch vụ an ninh mạng của các công ty lớn để cải thiện an ninh.
* Xây dựng chính sách an toàn thông tin toàn diện cho doanh nghiệp.
* Nhiều người cho rằng việc đảm bảo ATTT thuộc về đội ngũ kỹ thuật. Thực tế, điều này phải có sự kết hơp giữa đội ngũ kỹ thuật và những người quản lý. Nếu doanh nghiệp xây dựng một chính sách an ninh toàn diện cho cả người dùng và thiết bị, cho cả hiện tại và tương lai thì sẽ không bao giờ lo lắng trước những nguy cơ tấn công mạng.
* Bảo trì, nâng cấp thiết bị.
* Bảo trì định kì và nâng cấp nếu cần thiết những thiệt bị, phần mềm, công cụ liên quan tời hệ thống mạng và website . Ví dụ như nâng cấp phần mềm theo dõi hệ thống mạng, tăng cường bảo mật cho phần mềm quản trị website… nhằm tăng cường hiệu suất của hệ thống mạng tối đa.

## Các hạ tầng mạng cần có nếu cần tách biệt mạng nội bộ và mạng internet (Nguyễn Thị Yến)

* Hạ tầng mạng là tập hợp các thiết bị có chức năng chuyển mạch, định tuyến, xử lý đa dịch vụ được kết nối với nhau để tạo nên các hệ thống mạng như mạng LAN (Local Area Network) (bao gồm mạng có dây và không dây), mạng WAN (Wide Area Network), mạng MAN (Metro Area Network).
* Mạng phải đáp ứng phân phối các dịch vụ tối ưu cho người sử dụng. Phải đáp ứng được các nhu cầu về hoạt động và trao đổi số liệu, thông tin lớn giữa các thực thể tham gia kết nối. Các nhu cầu xử lý dữ liệu lớn của các ứng dụng đang chạy.

### 5.1. Hub là gì ?

Hub là điểm trung tâm kết nối cho các thiết bị trong hệ thống mạng. Chúng được dùng để kết nối các mạng LAN, chúng có rất nhiều các cổng để thực hiện công việc đó. Khi một gói tin đến một cổng, nó được sao chép đến các cổng khác với mục đích để cho các cổng khác có thể nhận dạng được gói tin.

### 5.2. Thiết bị chuyển mạch - Switch

* Khái niệm:
* Switch là một thiết bị chuyển mạch tối quan trọng trong mạng, dùng để kết nối các đoạn mạng với nhau theo mô hình hình sao (Star). Trong mô hình này, switch đóng vai trò trung tâm và tất cả các thiết bị vệ tinh khác kể cả máy tính đều được kết nối về đây, từ đó định tuyến tạo đường nối tạm trung chuyển dữ liệu đi. Ngoài ra, Switch được hỗ trợ công nghệ Full Duplex dùng để mở rộng băng thông của đường truyền, điều mà các thiết bị khác không làm được.
* Trên thị trường hiện nay có các loại Switch mạng được sử dụng phổ biến, rộng rãi trên các lĩnh vực khác nhau: Một loại là thiết bị Switch mạng có các cổng hoàn toàn là cổng quang ( Optical Switch) và một loại khác là loại chỉ **hỗ trợ thêm cổng quang** , các cổng SFP( Ethernet Support SFP).
* Có thể hiểu đơn giản thiết bị chuyển mạch Switch giống như cảnh sát giao thông phân luồng dữ liệu của một mạng cục bộ. Nó có khả năng chọn đường dẫn để quyết định chuyển frame (đơn vị của tầng liên kết dữ liệu) nên [mạng LAN](https://www.totolink.vn/article/151-lan-la-gi-tong-quan-kien-thuc-ve-lan-ma-ban-nen-biet.html) hoạt động hiệu quả hơn. Switch có khả năng nhận dạng máy được kết nối với nó nhờ cách đọc địa chỉ MAC nguồn trong frame nó nhận được. Khi hai máy trong mạng liên lạc với nhau, chính Switch sẽ tạo mạch ảo giữa hai cổng tương ứng mà không làm ảnh hưởng đến lưu thông trên các cổng khác.



Hình 1: Hình ảnh Switch

* Tầm quan trọng của Switch là gì?
* Hiểu được tầm quan trọng của thiết bị chuyển mạch là gì sẽ giải thích được tại sao Switch lại cần thiết phải có trong cơ sở mạng đến vậy. Mạng LAN hoạt động ổn định, hiệu suất cao là nhờ Switch có khả năng tạo đường dẫn kết nối ảo giữa hai thiết bị với nhau mà không làm ảnh hưởng đến những kết nối khác.
* Tương tự như Switch, một thiết bị khác khá phổ biến là Hub. Về cơ bản thì cả hai thiết bị chuyển mạch này có vai trò tương đương nhau, giúp kết nối nhiều máy tính và thiết bị với 1 mạng và chúng đóng vai trò là trung tâm. Tuy nhiên, thay vì tạo ra mạng ảo kết nối giữa hai thiết bị thì Hub sẽ chia sẻ bang thông trên cùng một đường truyền. Khi có hai máy trạm giao tiếp với nhau thì chúng sẽ chiếm dung lượng băng thông đáng kể, khi đó hoạt động của các thiết bị khác kết nối vào Hub sẽ bị giảm xuống. Nói như vậy để biết được thiết bị chuyển mạch Switch thông minh và ưu việt hơn hẳn nhờ khả năng tạo đường truyền ảo để kết nối riêng biệt giữa hai thiết bị, đảm bảo cung cấp trọn băng thông.
* Ích lợi của bộ chuyển mạch Switch
* Switch giúp cho các hoạt động diễn ra một cách song công (có thể đọc – ghi, nghe – nói) cùng lúc trên cùng một thiết bị. Ưu việt hơn khi không phải chia sẻ [băng thông](https://www.totolink.vn/article/88-bang-thong-mang-la-gi-don-vi-do-luong-bang-thong-la-gi.html) giống như các thiết bị tương tự khác, không ảnh hưởng đến kênh truyền khác cũng như không bị ảnh hưởng bởi chúng. Hơn nữa với cơ chế tự kiểm tra lỗi Frame nên sẽ giảm tỉ lệ lỗi trong frame, các gói tin tốt khi được nhận sẽ được lưu lại trước khi chuyển đi (công nghệ store-and-forward).
* Switch hoạt động chủ yếu ở tầng liên kết dữ liệu Layer 2 hay còn gọi là Switch Layer 2 trong mô hình tham chiếu OSI (mô hình lý giải một cách trừu tượng kỹ thuật kết nối truyền thông giữa các máy vi tính và thiết kế giao thức mạng giữa chúng). Nó có thể giới hạn lưu lượng truyền đi ở mức ngưỡng nào đó. Một Switch Layer 2 đi kèm với các loại giao diện khác nhau như 10Mbps, 100Mbps, 1Gbps, 10Gbps… Tất nhiên là nó cũng hỗ trợ giao tiếp Full-duplex trên mỗi cổng của nó.
* Không chỉ có thế, mỗi Switch đều tạo điều kiện để mở rộng mạng và kết nối với phần còn lại của mạng thông qua các cổng Uplink tốc độ cao, ở đây có thể kết nối với các thiết bị chuyển mạch Switch Layer 2 khác hay các Switch Layer 3 định tuyến. Tóm lại, một Switch hoạt động như một bộ điều khiển trung tâm, cho phép tất cả các thiết bị kết nối đến nó giao tiếp hiệu quả. Thông qua việc chia sẻ thông tin và phân bổ nguồn lực giúp tăng năng suất làm việc của nhân viên và tiết kiệm tiền bạc cho doanh nghiệp.
* Đặc điểm chính của Switch là gì?
* Nhìn chung Switch có đặc điểm giống như các thiết bị tương tự khác như Hub hay [Router](https://www.totolink.vn/router.html). Tuy nhiên Switch có hai đặc điểm riêng biệt:
* Phân chia kết nối riêng biệt trên mỗi đoạn mạng: Switch chia nhỏ hệ thống mạng thành những đơn vị cực nhỏ gọi là microsegment. Chính điều này cho phép nhiều người dùng trên nhiều segment khác nhau có thể giao tiếp và gửi dữ liệu cùng lúc mà không làm ảnh hưởng đến ai.
* Cung cấp băng thông lớn hơn cho mỗi người dùng bằng cách tạo ra các miền đụng độ nhỏ hơn. Switch chia nhỏ mạng LAN thành nhiều đoạn mạng nhỏ, tương ứng là một kết nối riêng giống như một làn đường riêng.

### 5.3. Router - Bộ định tuyến là gì ?

* Khái niệm
* Router hay còn được gọi là **bộ định tuyến**, là thiết bị chuyển tiếp các gói dữ liệu dọc theo mạng. Chúng được nối với ít nhất hai mạng, thông thường là hai mạng LAN hoặc WAN hoặc là kết nối một mạng LAN với nhà cung cấp dịch vụ internet (ISP - Internet Service Provider). Router được định vị ở cổng vào, nơi mà có hai hoặc nhiều mạng kết nối. Router sử dụng các tiêu đề và bảng chuyển tiếp để xác định đường đi tốt nhất để chuyển tiếp các gói tin, và chúng sử dụng các giao thức như ICMP để giao tiếp với nhau và xác định đường đi tốt nhất giữa hai máy trạm bất kỳ. Muốn sở hữu một Router chất lượng với giá cả phải chăng không thể không nghĩ ngay đến thiết bị mạng Cisco. Các loại Router Cisco thông dụng được kể tên sau đây: [Router cisco 2911-SEC/K9](https://thietbimangcisco.vn/cisco-2911-sec-k9-c-322-327-5241.html" \o "Router cisco 2911-SEC/K9), [Router cisco 1941-HSEC+/K9](https://thietbimangcisco.vn/cisco-1941-hsec+-k9-c-322-328-5211.html" \o "Router cisco 1941-HSEC+/K9), [Router cisco 1921-SEC/K9](https://thietbimangcisco.vn/cisco1921-sec-k9-c-322-328-5210.html" \o "Router cisco 1921-SEC/K9)
* Về cấu tạo: Router là một thiết có các cổng mạng LAN (có thể có 1 hoặc rất nhiều cổng LAN), hoặc bao gồm luôn cả ang-ten (râu) phát sóng wifi.



Hình 2: Hình ảnh router

* Chức năng của Router
* Router có chức năng gửi các gói dữ liệu mạng giữa 2 hoặc nhiều mạng, từ một tới nhiều điểm đích đến cuối cùng từ router.
* Nói một cách dễ hiểu là từ Router có thể cắm trực tiếp dây Lan đến máy tính, hoặc sử dụng sóng WiFi do Router phát ra.
* Router muốn phát sóng WiFi hoặc chuyền các gói tín hiệu (tức là tín hiệu mạng internet) cho chúng ta sử dụng thì Router phải được gắn với modem. Modem ở đây có thể là [modem 1 cổng](https://fpt123.net/Ho-tro-ky-thuat/Tim-hieu-ve-modem/Modem-1-cong.html), [modem 4 cổng](https://fpt123.net/Ho-tro-ky-thuat/Tim-hieu-ve-modem/Modem-4-cong.html), [modem wifi 1 cổng](https://fpt123.net/ho-tro-ky-thuat/tim-hieu-ve-modem/modem-wifi-1-cong.html) hay [modem wifi 4 cổng](https://fpt123.net/Ho-tro-ky-thuat/Tim-hieu-ve-modem/Modem-wifi-4-cong.html) đều được. Modem này đã được đấu nối với đường truyền Internet của nhà mạng.

### 5.4. Giải pháp thiết kế mở rộng hệ thống mạng được xây dựng để đáp ứng các yêu cầu sau:

* Đảm bảo tính an ninh, ổn định, bảo mật tốt đối với các dịch vụ và dữ liệu quan trọng chạy trên mạng - Mạng phải có tính dự phòng, đáp ứng được khi có sự cố về truyền thông và thiết bị xảy ra. Mạng phải có khả năng quản lý và theo dõi để đảm bảo chắc chắn sự hoạt động tin cậy và tính sẵn sàng của các tài nguyên mạng.
* Có cấu trúc và phân lớp rõ ràng các lớp mạng để dễ dàng trong việc quản lý và mở rộng sau này (theo mô hình 3 lớp) - Mạng phải tuân theo mô hình 3 lớp (lớp xương sống, lớp phân phối, lớp truy nhập) để đáp ứng được các yêu cầu đặc thù cho từng lớp, dễ dàng dự đoán sửa lỗi, mở rộng, hỗ trợ các giao thức khác nhau tại các lớp khác nhau.
* Mạng phải có tính mở - Mạng phải có tính đáp ứng cao với các công nghệ mới, như vậy sẽ bảo vệ được đầu tư trong tương lai khi công ty muốn đưa vào ứng dụng các công nghệ mới. Mạng phải đáp ứng được các thay đổi về mở rộng trong tương lai, với các thay đổi như thêm mới các mạng nhỏ, nâng cấp băng thông, mạng sẵn sàng hỗ trợ các dạng dịch vụ khác nhau ngoài Data như Voice, Fax, Video mà không cần phải thay thế các thiết bị mới
* Mạng LAN được thiết kế tuân theo mô hình 3 lớp của mạng LAN campus do Cisco Systems đưa ra. Mô hình này hiện nay cũng được rất nhiều hang sản xuất áp dụng phổ biến vì những lợi ích mà nó mang lại. Theo Cisco, mạng LAN campus có thể được phân thành 3 lớp cơ bản như sau: lớp Lõi (core layer), lớp Phân Phối (Distribution Layer) và lớp Truy Cập (Access Layer). Tuy nhiên, tùy theo quy mô của mạng LAN mà có thể có hay không có lớp Lõi. Dưới đây chúng tôi sẽ trình bày sơ lược về cả ba lớp của mô hình LAN Campus của Cisco.

### 5.5. Xác định các nguy cơ gây nguy hiểm cho an toàn mạng

* Tấn công xâm nhập mạng từ bên trong và bên ngoài nội bộ
* Đánh cắp dữ liệu, chèn mã độc, virus vào trong phần mềm, công cụ
* Mã độc lây nhiễm bắt nguồn từ Plug-in trình duyệt
* Không giống như ngày trước, Hacker bây giờ xâm nhập vào hệ thống mạng ngày càng tinh vi hơn. Thay vì việc tấn công một mình, hacker thường tổ chức theo nhóm, có kịch bản dựng sẵn,  và có 1 số kịch bản tương lai nhằm đề phòng trường hợp mã độc gửi đi bị chặn lại. Ví dụ điển hình như mã độc tống tiền WannaCry, lúc mới phát hiện mọi người tưởng rằng chỉ bị ảnh hưởng 1 hoặc 2 ngày, nhưng thực tế nó đã tác động tới cả thế giới gần 1 tuần liền.

### 5.6. Giải pháp cho phần cứng

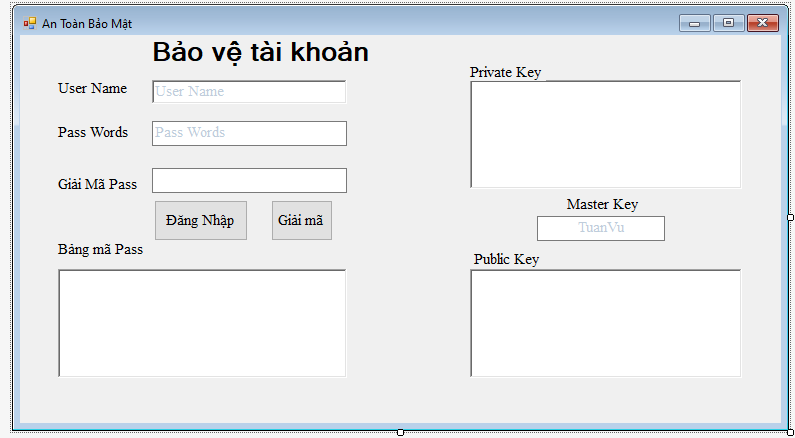
* Có sự đầu tư có chọn lọc trước khi mua bất kỳ phần mềm hoặc công cụ nào đó phục vụ cho việc bảo mật.
* Khi nâng cấp hệ thống, chọn nhà cung cấp dịch vụ có uy tín
* Nâng cấp bảo mật cho các thiết bị đầu vào và đầu ra. Ví dụ như cổng cắm USB, ổ cứng, ổ đĩa, …
* Tăng thêm độ bảo mật cho hệ thống tường lửa.

# Phần 2: Ứng dụng cài đặt minh họa

## …..

## …..

## Cài đặt minh họa các chính sách đảm bảo an toàn cho hệ thống(Lưu Tuấn Vũ)



Hình 1 : Giao diện mô phỏng

### Lớp sử lý MyCrypto

#### Hàm AssignNewKey

Hàm này tạo 1 khóa mới từ 1 chuỗi ký tự được chuyền vào

public class MyCrypto

{

RSACryptoServiceProvider RSA = null;

public string PrivateKeyXML;

public string PublicOnlyKeyXML;

public void AssignNewKey(string keymaster)

{

const int PROVIDER\_RSA\_FULL = 1;

string CONTAINER\_NAME = keymaster;

CspParameters cspParams;

cspParams = new CspParameters(PROVIDER\_RSA\_FULL);

cspParams.KeyContainerName = CONTAINER\_NAME;

cspParams.Flags = CspProviderFlags.UseMachineKeyStore;

cspParams.ProviderName = "Microsoft Strong Cryptographic Provider";

RSA = new RSACryptoServiceProvider(cspParams);

//Pair of public and private key as XML string.

//Do not share this to other party

PrivateKeyXML = RSA.ToXmlString(true);

//Private key in xml file, this string should be share to other parties

PublicOnlyKeyXML = RSA.ToXmlString(false);

}

* + 1. **Hàm Mã Hóa Encryp**

public byte[] Encrypt(string publicKeyXML, string dataToDycript)

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicKeyXML);

return rsa.Encrypt(ASCIIEncoding.ASCII.GetBytes(dataToDycript), true);

}

public string Encrypt\_string(string publicKeyXML, string dataToDycript)

{

try

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicKeyXML);

string EncryptedResult = System.Convert.ToBase64String(rsa.Encrypt(System.Text.Encoding.Unicode.GetBytes

(dataToDycript), true));

return EncryptedResult;

}

catch

{

return "Mã hóa thất bại";

}

}

* + 1. **Hàm Giải Mã Decrypt**

public string Decrypt(string publicPrivateKeyXML, byte[] encryptedData)

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicPrivateKeyXML);

return ASCIIEncoding.ASCII.GetString(rsa.Decrypt(encryptedData, true));

}

public string Decrypt\_string(string publicPrivateKeyXML, string encryptedData)

{

try

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.FromXmlString(publicPrivateKeyXML);

byte[] toDecryptData = System.Convert.FromBase64String(encryptedData);

return System.Text.Encoding.Unicode.GetString(rsa.Decrypt(toDecryptData, true));

}

catch {

return "Giải mã thất bại"; ;

}

}

* + 1. **Hàm sử lý chuỗi nhị phân**

public static string ByteArrayToHexString(byte[] Bytes)

{

StringBuilder Result = new StringBuilder(Bytes.Length \* 2);

string HexAlphabet = "0123456789ABCDEF";

foreach (byte B in Bytes)

{

Result.Append(HexAlphabet[(int)(B >> 4)]);

Result.Append(HexAlphabet[(int)(B & 0xF)]);

}

return Result.ToString();

}

* + 1. **Hàm sử lý chuỗi thập lục phân**

public static byte[] HexStringToByteArray(string Hex)

{

byte[] Bytes = new byte[Hex.Length / 2];

int[] HexValue = new int[] { 0x00, 0x01, 0x02, 0x03, 0x04, 0x05,

0x06, 0x07, 0x08, 0x09, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,

0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F };

for (int x = 0, i = 0; i < Hex.Length; i += 2, x += 1)

{

Bytes[x] = (byte)(HexValue[Char.ToUpper(Hex[i + 0]) - '0'] << 4 |

HexValue[Char.ToUpper(Hex[i + 1]) - '0']);

}

return Bytes;

}

### Lớp sử lý sự kiện

public partial class FormMain : Form

{

public FormMain()

{

InitializeComponent();

}

MyCrypto ATBM\_RSA = new MyCrypto();

private void Form2\_Load(object sender, EventArgs e)

{

ATBM\_RSA.AssignNewKey(txtMasterKey.Text);

}

private void btnLogin\_Click(object sender, EventArgs e)

{

if (txtUser.Text == "" || txtUser.Text.Length <= 3|| txtUser.Text == "User Name"||

txtPassWords.Text == "" || txtPassWords.Text.Length < 6||

txtPassWords.Text == "Pass Words")

{ txtMasterKey.Text = "Nhập đủ thông tin"; }

else {

txtMasterKey.Text = txtUser.Text.Substring(0, 4);

ATBM\_RSA.AssignNewKey(txtMasterKey.Text);

txtPublicKey.Text = ATBM\_RSA.PublicOnlyKeyXML;

txtPrivateKey.Text = ATBM\_RSA.PrivateKeyXML;

txtBangmaE.Text = ATBM\_RSA.Encrypt\_string(txtPublicKey.Text, txtPassWords.Text);

} }

private void txtGiaima\_Click(object sender, EventArgs e)

{

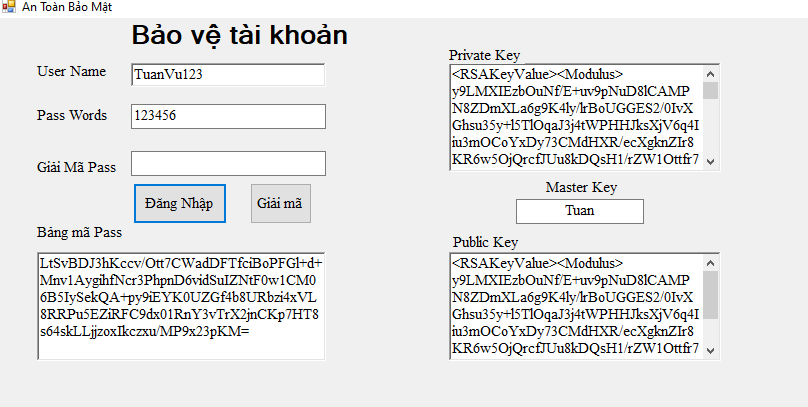
txtBangroD.Text = ATBM\_RSA.Decrypt\_string(txtPrivateKey.Text, txtBangmaE.Text);}

}

### **Kết Quả**

* + 1. **Kết quả khi nhấn “đăng nhập”**

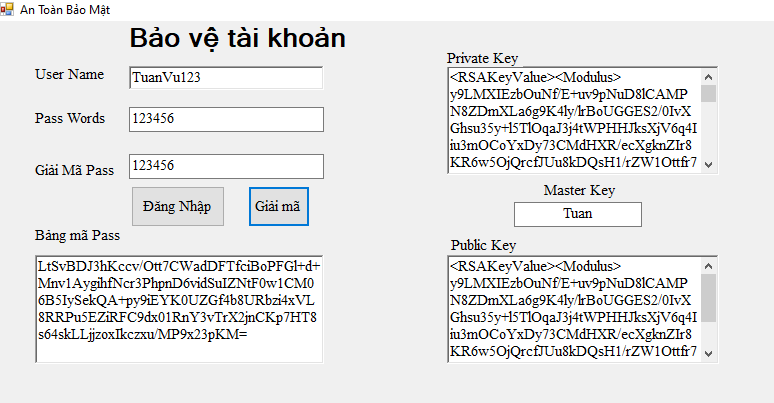
Hệ thống sẽ tự sinh khóa từ chuỗi gồm 4 kí tự đầu của tên tài khoản, Mật khẩu được mã hóa từ khóa được sinh trước khi gủi về Server bằng thuật toán RSA



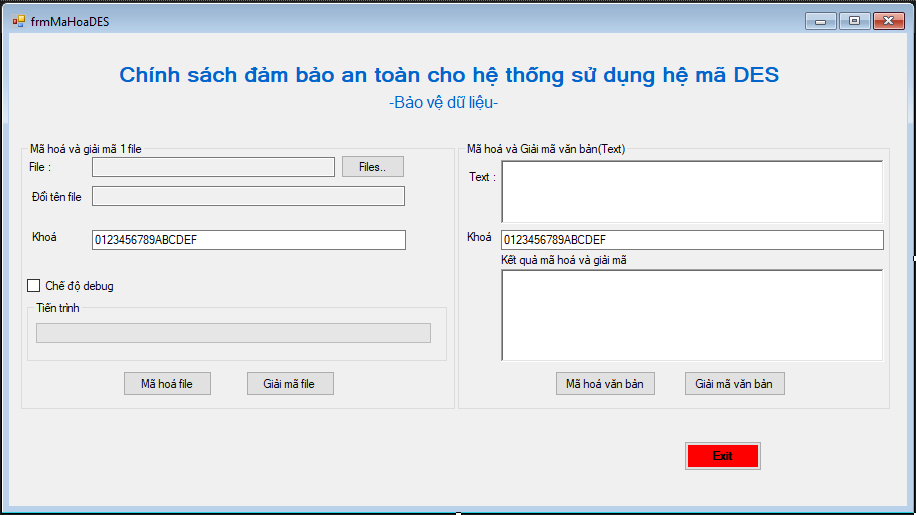
Hình 2: kết quả thực hiện 1

* + 1. **Kết quả khi nhấn “giải mã”**

Hệ thống tiến hành giải mã từ bảng mã của Mật khẩu . được mật khẩu và lưu vào CSDL



1. **Cài đặt minh hoạ các chính sách đảm bảo an toàn cho hệ thống (Vũ Đức Vượng)**



### Lớp xử lý với thuật toán DES

* + 1. **Hàm mã hoá và giải mã**

|  |
| --- |
| public ChuoiNhiPhan ThucHienDES(Khoa key,ChuoiNhiPhan ChuoiVaoDai, int MaHoaHayGiaiMa)// 1 ma hoa, -1 giai ma  {  this.KhoaDES = key;// lấy khóa chính  if(MaHoaHayGiaiMa==1) // nếu là mã hóa thì cần chỉnh lại độ dài của chúng sao cho chia hết cho 64  ChuoiVaoDai =ChuoiVaoDai.ChinhDoDai64() ;    KhoaDES.SinhKhoaCon( ); // sinh dẫy các khóa con  ChuoiNhiPhan[] DSChuoiVao = ChuoiVaoDai.Chia(ChuoiVaoDai.DoDai / 64);// chia dữ liệu vào thành từng khối 64 bit và xử lý dần dần  ChuoiNhiPhan ChuoiVao,ChuoiKQ;  ChuoiKQ = new ChuoiNhiPhan(0);  ChuoiNhiPhan[] ChuoiSauIP;  ChuoiNhiPhan ChuoiSauIP\_1;  ChuoiNhiPhan L, R, F, TG;  for (int k = 0; k < DSChuoiVao.Length; k++) // duyêt qua từng chuỗi được chai  {  //ChuoiVao = DSChuoiVao[k];    // b1: tính IP  ChuoiSauIP = CacThongSo.TinhIP(DSChuoiVao[k]);  // lấy giá trị L,R  L = ChuoiSauIP[0];  R = ChuoiSauIP[1];  for (int i = 0; i < 16; i++)  {  // tính hàm F giữa khóa phụ Right  F = HamF(R, KhoaDES.DayKhoaPhu[MaHoaHayGiaiMa==1?i:15-i]);  L = L.XOR(F);// tính XOR giữa L và giá trị hàm F  TG = L;// đổi L và R cho nhau  L = R;  R = TG;  }  // tính IP\_1  ChuoiSauIP\_1 = CacThongSo.TinhIP\_1( R,L);  // cộng thêm chuỗi đã ddc mã hóa vào  ChuoiKQ = ChuoiKQ.Cong(ChuoiSauIP\_1);  }  if (MaHoaHayGiaiMa == -1) // nếu là giải mã thì cần cắt bớt các bit bù vào ban đầu  ChuoiKQ = ChuoiKQ.CatDuLieu64();  return ChuoiKQ; } |

* + 1. **Hàm mã hoá, giải mã một chuỗi string đơn giản**

|  |
| --- |
| public string ThucHienDESText(Khoa key,string ChuoiVao, int MaHoaHayGiaiMa)// 1 ma hoa, -1 giai ma  {  ChuoiNhiPhan chuoiNhiPhan;  if (MaHoaHayGiaiMa == 1)  {  chuoiNhiPhan = ChuoiNhiPhan.ChuyenChuSangNhiPhan(ChuoiVao);  }  else  {  chuoiNhiPhan = ChuoiNhiPhan.ChuyenChuSangChuoiNhiPhan(ChuoiVao);  }  ChuoiNhiPhan KQ = ThucHienDES(key,chuoiNhiPhan, MaHoaHayGiaiMa);  if (MaHoaHayGiaiMa == 1)  {  return KQ.Text;  }  if (KQ == null)  {  MessageBox.Show("Lỗi giải mã . kiểm tra khóa ");  return "";  }  return ChuoiNhiPhan.ChuyenNhiPhanSangChu(KQ);// chueyren sang dạng text để hiện thị kết quả  } |

* + 1. **Hàm tính và đưa ra kết quả**

|  |
| --- |
| private ChuoiNhiPhan HamF(ChuoiNhiPhan chuoiVao, ChuoiNhiPhan KhoaCon)  {  ChuoiNhiPhan KQ=CacThongSo.TinhE(chuoiVao); // Tính E trước  KQ = KQ.XOR(KhoaCon); // tính XOR  KQ = CacThongSo.TinhSBox(KQ); // tính hộp s-box  KQ = CacThongSo.TinhP(KQ); // tính P là ok  return KQ;  } |

### Lớp xử lý sự kiện

* + 1. **Hàm thông báo kết quả và chạy tiến trình**

|  |
| --- |
| private void MaHoa()  {  MaHoaDES64 = new DES64Bit();  if (!ckbCheDoDebug.Checked)  {  EnableHoacDisableNut(false);  progressBar1.Value = 10;  timer1.Enabled = true;  }    TenTienTrinh = "";    GiaiDoan = 0;  Dem = 0;    if (FileHayChuoi)  {  Khoa = new Khoa(txtKhoaFile.Text);  if (MaHoaHayGiaiMa == 1)  {  GiaiDoan = 0;  ChuoiNhiPhan chuoi = DocFileTxt.FileReadToBinary(txtFileNguon.Text);  GiaiDoan = 1;  ChuoiNhiPhan KQ = MaHoaDES64.ThucHienDES(Khoa, chuoi, 1);  GiaiDoan = 2;  DocFileTxt.WriteBinaryToFile(txtFileDich.Text, KQ);  GiaiDoan = 3;  MessageBox.Show("Mã hóa file thành công");  }  else  {  GiaiDoan = 0;  ChuoiNhiPhan chuoi = DocFileTxt.FileReadToBinary(txtFileNguon.Text);  GiaiDoan = 1;  ChuoiNhiPhan KQ = MaHoaDES64.ThucHienDES(Khoa, chuoi, -1);  if (KQ == null)  {  MessageBox.Show("Lỗi giải mã . kiểm tra khóa ");  return;  }  GiaiDoan = 2;  DocFileTxt.WriteBinaryToFile(txtFileDich.Text, KQ);  GiaiDoan = 3;  MessageBox.Show("Giải mã file thành công");  }  }  else  {  Khoa = new Khoa(txtKhoaVanBan.Text);  if (MaHoaHayGiaiMa == 1)  {  MaHoaDES64 = new DES64Bit();  GiaiDoan = 0;  GiaiDoan = 1;  string kq=MaHoaDES64.ThucHienDESText(Khoa, txtVanBanNguon.Text, 1);  txtVanBanDich.Text = kq;  GiaiDoan = 2;  GiaiDoan = 3;  MessageBox.Show("Mã hóa chuỗi thành công");  }  else  {  MaHoaDES64 = new DES64Bit();  GiaiDoan = 0;  GiaiDoan = 1;  string kq = MaHoaDES64.ThucHienDESText(Khoa, txtVanBanNguon.Text, -1);  txtVanBanDich.Text = kq;  if (kq == "")  {  return;  }  GiaiDoan = 2;  GiaiDoan = 3;  MessageBox.Show("Giải mã chuỗi thành công");  }  }  if (!ckbCheDoDebug.Checked)  {  EnableHoacDisableNut(true);  timer1.Enabled = false;  }  } |

* + 1. **Hàm khi kích chọn các nút**

|  |
| --- |
| private void btnChonFile\_Click(object sender, EventArgs e)  {  txtFileNguon.Clear();  txtFileDich.Clear();  if (openFileDialog1.ShowDialog() == DialogResult.OK)  {  txtFileNguon.Text = openFileDialog1.FileName;  txtFileDich.Text = openFileDialog1.FileName.Replace(".", "\_2.");  }  }  private void btnMaHoaFile\_Click(object sender, EventArgs e)  {  FileHayChuoi = true;  MaHoaHayGiaiMa = 1;  EnableHoacDisableNut(false);  Chay();  if(ckbCheDoDebug.Checked)EnableHoacDisableNut(true);  }  private void btnGiaiMaFile\_Click(object sender, EventArgs e)  {  FileHayChuoi = true;  MaHoaHayGiaiMa = -1;  EnableHoacDisableNut(false);  Chay();  if (ckbCheDoDebug.Checked) EnableHoacDisableNut(true);  }  private void txtMaHoaVanBan\_Click(object sender, EventArgs e)  {  FileHayChuoi = false;  MaHoaHayGiaiMa = 1;  EnableHoacDisableNut(false);  MaHoa();  EnableHoacDisableNut(true);  } |

### Lớp xử lý khoá

* + 1. **Hàm kiểm tra khoá, khoá lỗi khi độ dài chia hết cho 64**

|  |
| --- |
| public bool KiemTraKhoa()  {  return (KhoaChinhNhiPhan.DoDai % 64==0);  } |

* + 1. **Hàm sinh khoá con (Sinh 16 khoá con từ khoá chính 64bit)**

|  |
| --- |
| public void SinhKhoaCon()  {  DayKhoaPhu = new ChuoiNhiPhan[16];  ChuoiNhiPhan C0,D0, MotKhoaPhu;  // b1: tính PC1  ChuoiNhiPhan[] ChuoiSauPC1 = CacThongSo.TinhPC1(KhoaChinhNhiPhan);  // sau khi qua PC1 sẽ có 56bit còn lại được chia thành 2 mảng C0 và D0  C0 = ChuoiSauPC1[0];  D0 = ChuoiSauPC1[1];  // thực hiện 16 vòng để được 16 khóa  for (int i = 0; i < 16; i++)  {  // dịch trái hai chuỗi nhị phân với số bít bị dịch được quy định trước  // vòng 1,2,9 là 1 bit  // còn lại dịch 2 bit  C0 = C0.DichTraiBit(CacThongSo.soBitDichTaiCacVong[i]);  D0 = D0.DichTraiBit(CacThongSo.soBitDichTaiCacVong[i]);  // Khóa phụ thu được sau khi tính PC2 từ C và D  MotKhoaPhu = CacThongSo.TinhPC2(C0, D0);  // thêm khóa phụ vào mảng khóa phụ  DayKhoaPhu[i] = MotKhoaPhu;  }// cứ thé 16 vòng ta thu được 16 khóa phụ  } |

* + 1. **Hàm tạo mới 1 khoá từ chuỗi 16 ký tự trong hệ thập lục phân**

|  |
| --- |
| public Khoa(string khoa)  {  KhoaChinhNhiPhan = new ChuoiNhiPhan(0);  foreach (var ch in khoa)  {  KhoaChinhNhiPhan=KhoaChinhNhiPhan.Cong(ChuoiNhiPhan.ChuyenSoSangNhiPhan(ChuoiHexa.ChuyenHexaSangHe10(ch), 4));  }  //KhoaChinhNhiPhan = ChuoiNhiPhan.ChuyenKhoaSangNhiPhan(khoa); // chuyển chuỗi ký tự sang nhị phân và gán cho khóa chính  } |

* Ngoài ra còn các lớp xử lý chuỗi thập lục phân và chuỗi nhị phân.

### Kết quả

* + 1. **Kết quả khi mã hoá và giải mã file**
* Để mã hoá file, người dùng trỏ đến file cần mã hoá bằng các ấn vào button “Files”, file mã hoá sẽ mặc định nằm cùng thư mục với file cần mã hoá và có tên mặc định là: “Tên file cần mã hoá\_2”, người dùng sẽ nhập vào khoá hoặc chọn khoá mặc định của hệ thống. Sau đó kích vào button “Mã hoá file”. Sau khi mã hoá file thành công sẽ có thông báo. File mã hoá đã được tạo.
* Để giải mã file, người dùng trỏ đến file cần giải mã theo các bước như mã hoá, tên file giải mã mặc định sẽ là: “Tên file mã hoá\_2”. Sau khi trỏ, người dùng nhập khoá và kích giải mã.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

* + 1. **Kết quả khi mã hoá và giải mã văn bản**
* Để mã hoá đoạn văn bản người dùng nhập đoạn văn bản cần mã hoá vào ô textbox, nhập khoá và kích vào button “Mã hoá văn bản”, đoạn văn bản sẽ được mã hoá và hiển thị thông báo mã hoá thành công.
* Để giải mã đoạn văn bản, người dùng nhập đoạn văn bản cần giải mã vào ô textbox, nhập khoá và kích vào button “Giải mã văn bản”, đoạn văn bản sẽ được giải mã và hiển thị thông báo giải mã thành công.

|  |  |
| --- | --- |
|  |  |

* Việc mã hoá dữ liệu này giúp người dùng bảo vệ được thông tin khi upload lên, việc giải mã giúp người dùng sử dụng lại được thông tin khi lấy về.

1. **…..**