LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành nhất tới TS. Lại Minh Tuấn đã hướng dẫn em phát triển đồ án nghiên xây dựng ứng dụng thu thập cảnh báo trong hệ thống mạng cho điện thoại thông minh chạy hệ điều hành androidvà cho em những định hướng và những kiến thức quý báu về an toàn mạng và hiểu biết hơn về hệ điều ahnhf android.

Em cũng xin tỏ lòng biết ơn sâu sắc tới thầy cô, bạn bè cùng khóa đã giúp đỡ em học tập và rèn luyện trong suốt những năm học vừa qua.

Em xin cảm ơn gia đình và bạn bè, những người luôn khuyến khích và tạo mọi điều kiện hỗ trợ tốt nhất cho em trong mọi hoàn cảnh.

Em xin chân thành cảm ơn trường Học viện Kỹ thuật Mật Mã đã cho em một môi trường học tập lành mạnh và vững chắc, tạo cho em những điều kiện tốt nhất trong quá trình học tập và làm đồ án này.

Do thời gian hoàn thành đồ án có hạn cho nên em không tránh khỏi những khiếm khuyết, em rất mong có được những góp ý và giúp đỡ của các thầy cô giáo để em có thể tiếp tục đồ án này ở mức ứng dụng cao hơn trong tương lai.

Em xin chân thành cảm ơn!

*Hà Nội, ngày 01 tháng 06 năm 2018*

**Sinh viên thực hiện**

**Vũ Văn Minh**

**LỜI MỞ ĐẦU**

Hiện nay mạng Internet đã trở thành một phần không thể thiếu của con người. Internet ngày càng phổ biến rộng rãi cho mọi người để trao đổi thông tin trên mạng . Khả năng kết nối trên toàn thế giới đang mang lại thuận tiện cho tất cả mọi người, nhưng nó cũng tiềm ẩn những nguy cơ khó lường đe dọa tới mọi mặt của đời sống xã hội. Việc mất trộm thông tin trên mạng gây ảnh hưởng đến tính riêng tư cho các cá nhân, những vụ lừa đảo, tấn công từ chối dịch vụ gây ảnh hưởng lớn đến hoạt động kinh doanh cho công ti và gây phiền toái cho mọi người dung Internet… làm cho vấn đề bảo mật trên mạng luôn là một vấn đề nong hổi và được quan tâm đến trong mọi thời điểm.

Cho đến nay, các giải pháp bảo mật luôn được chú trọng và đã có những đóng góp lớn trong việc hạn chế và ngăn chặn những vấn đề bảo mật, ví dụ như Firewall ngăn chặn những kết nối không đáng tin cậy, mã hóa tang dộ an toàn cho việc truyền dữ liệu, các chương trình duyệt virus với cơ sở dữ liệu liên tục cập nhập về những loại virus mới nhất. Tuy nhiên hiện nay các vụ vi phạm bảo mật xảy ra càng ngày càng tinh vi hơn cùng với sự gia tang những vụ lạm dụng, dung sai xuất phát từ hệ thống mà những phương pháp bảo mật truyền thống không chống được. Những điều đó yêu cầu phải có một Phuong án kịp thời để sử lý ngăn chặn những cuộc tấn công, và kịp thời bảo vệ hệ thống mạng máy tính.

Nhằm giải quyết vấn đề xử lý phát hiện cảnh báo khi bị tấn công trên mạng dữ liệu. Chính vì vậy, em xin lựa chọn đồ án với tên đề tài là “xây dựng ứng dụng thu thập cảnh báo trong hệ thống mạng cho điện thoại thông minh chạy hệ điều hành android” nhằm mục đích phát hiện và cảnh báo mỗi khi mạng máy tính bị tấn công và gửi thông báo về điện thoại người quản lý mạng dữ liệu đó.

Em xin chân thành cảm ơn các thầy cô hướng dẫn em tận tình để em hoàn thành báo cáo thực tập này!

*Hà Nội ngày 01 tháng 03 năm 2018*

**Sinh viên thực hiện**

**Vũ Văn Minh**

MỤC LỤC

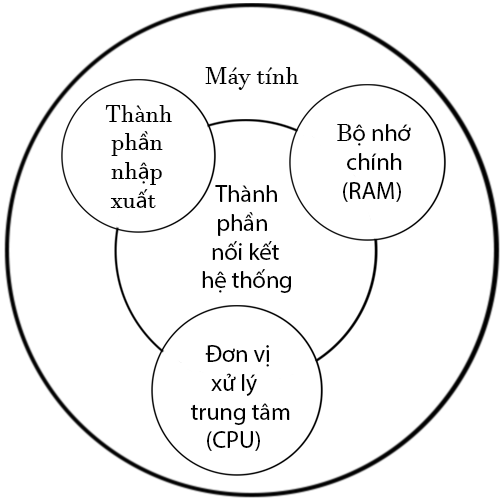
PHẦN I : TỔNG QUAN VỀ MẠNG MÁY TÍNH

**CHƯƠNG 1 : GIỚI THIỆU VỀ MÁY TÍNH VÀ MẠNG MÁY TÍNH**

**1.1.Lịch sử máy tính**

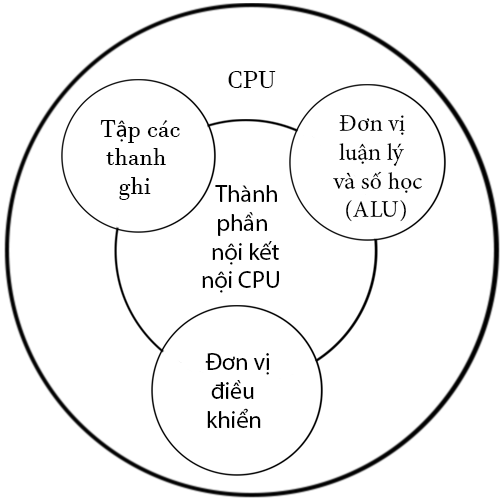
**1.1.1.Cấu trúc tổng quát của máy tính**

Máy tính là một hệ thống phức tạp với hang triệu thành phần điện tử cơ sở. Ở mức đơn giản nhất, máy tính có thể được xem như một thực thể tưởng tác theo mottj cách thức nào đó với môi trường bên ngoài. Một cách tổng quát, các mối quan hệ của nó môi trường bên ngoài có thể phân loại thành các thiết bị ngoại vi hay đường liên lạc.



Hình 1.1.1a: Cấu trúc tổng quát của máy tính

Thành phần chính , quan trọng nhất của máy tính là đơn vị xử lý trung tâm ( CPU – Central Processing Unit): Điều khiển hoạt động của máy tính và thực hiện các chức năng xử lý dữ liệu.



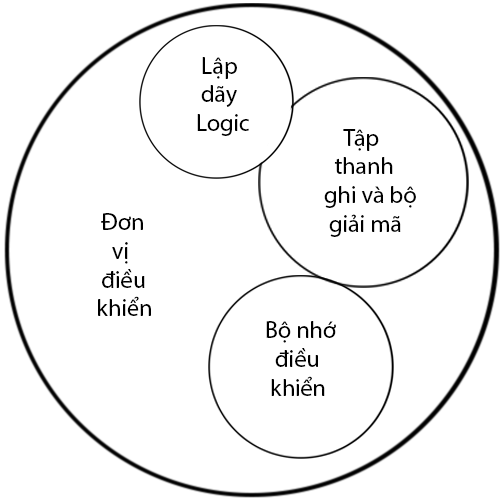
Hình 1.1.1b: Bộ xử lý trung tâm của máy tính (CPU)

CPU thường được đề cập đến với tên gọi bộ xử lý. Máy tính có thể có một hoặc nhiều thành phần nói trên, ví dụ như một hoặc nhiều CPU. Trước đây đa phần các máy tính chỉ có một CPU nhưng gần đây có sự gia tang sử dụng nhiều CPU trong một hệ thống máy đơn. CPU luôn luôn là đối tượng quan trọng vì đây là thành phần phức tạp nhất của hệ thống. Cấu trúc của CPU gồm các thành phần chính:

* Đơn vị điều khiển : Điều khiển hoạt động của CPU và do đó điều khiển hoạt động của máy tính.
* Đơn vị luận lý và số học (ALU – Arithmetic and Logic Unit) : Thực hiện các chức năng xử lý dữ liệu của máy tính.
* Tập thanh ghi : Cung cấp nơi lưu trữ bên trong CPU.
* Thành phần nối kết nội CPU : Cơ chế cung cấp khả năng liên lạc giữa đơn vị điều khiển, ALU và tập thanh ghi.

Trong các thành phần con nói trên của CPU, đơn vị điều khiển lại giữ vai trò quan trọng nhất. Sự cài đặt đơn vị này dẫn đến một khái niệm nền tảng trong chế tạo bộ vi xử lý máy tính. Đó là khái niệm vi lập trình. Hình dưới đây mô tả tổ chức bên trong một đơn vị điều khiển với ba thành phần chính gồm:

* Bộ lập dãy logic.
* Bộ giải mã và tập các thanh ghi điều khiển.
* Bộ nhớ điều khiển.



Hình 1.1.1c : Đơn vị điều khiển của CPU

Các thành phần khác của máy tính:

* Bộ nhớ chính : Dùng để lưu trữ dữ liệu.
* Các thành phần nhập xuất : Dùng để di chuyển dữ liệu giữa máy tính và môi trường bên ngoài.
* Các thành phần nối kết hệ thống : Cung cấp cơ chế liên lạc giữa CPU, bộ nhớ chính và các thành phần nhập xuất.

**1.1.2. Chức năng của máy tính**

Một cách tổng quát, một máy tính có thể thực hiện bốn chức năng cơ bản sau:

* Di chuyển dữ liệu.
* Điều khiển.
* Lưu trữ dữ liệu.
* Xử lý dữ liệu.
* Xử lý dữ liệu : Máy tính phải có khả năng xử lý dữ liệu. Diwx liệu có thể có rất nhiều dạng và phạm vi yêu cầu xử lý cũng rất rộng. Tuy nhiên chỉ có một số phương pháp cơ bản trong xử lý dữ liệu.
* Lưu trữ dữ liệu : Máy tính cũng cần phải có khả năng lưu trữ dữ liệu. Ngay cả khi máy tính đang xử lý . Do vậy cần thiết phải có chức năng lưu trữ ngắn hạn. Tuy nhiên, chwucs năng lưu trữ dài hạn cũng có tầm quan trọng tương đối với dữ liệu cần được lưu trữ trên máy cho những lần cập nhập và tìm kiếm kế tiếp.
* Di chuyển dữ liệu : Máy tính có phải có khả năng di chuyển dữ liệu giữa nó và thế giới bên ngoài. Khả năng này được thể hiện thông qua việc di chuyển dữ liệu giữa máy tính tính với các thiết bị nối kết trực tiếp hay từ xa đến nó. Tùy thuộc vào kiểu kết nối và cự ly di chuyển dữ liệu, mà có tiến trình nhập xuất dữ liệu hay truyền dữ liệu:

**1.2 Mạng máy tính**

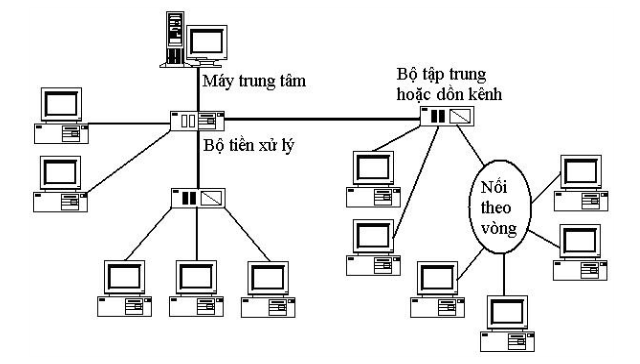
Mạng máy tính là một hệ thống kết nối các máy tính đơn lẻ thông qua các đường truyền vật lý theo một kiến trúc nào đó.

Đường truyền vật lý dung để chuyển các tín hiệu số hay tín hiệu tương tự giữa các máy tính. Đường truyền vật lý thường là:

* Đường dây điện thoại thông thường.
* Cáp đồng trục.
* Sóng vô tuyến điện tử.
* Cáp sợi quang.

**1.2.1. Lịch sử phát triển mạng máy tính**

Từ những năm 60, đã xuất hiện những mạng nối cá máy tính và các Terminal để sử dụng chung nguồn tài nguyên, giảm chi phí khi muốn thông tin, trao đổi số liệu và sử dụng trong công tác văn phòng một cách tiện lợi.



Hình 1.2.1: Mạng máy tính với bộ tiền xử lý.

Việc tăng nhanh các máy tính mini, các máy tính cá nhân làm tăng nhu cầu truyền số liệu giữa các máy tính, các Terminal và giữa các Terminal với các máy tính là một trong những động lực thúc đẩy sự ra đời và phát triển ngày càng mạnh mẽ các mạng máy tính. Quá trình hình thành mạng máy tính có thể tóm tắt qua một số thời điểm chính sau:

Những năm 60: Để tận dụng công suất của máy tính, người ta ghép nối các Terminal vào một máy tính được gọi là máy tính trung tâm (main frame). Máy tính trung tâm làm tất cả mọi việc từ quản lý các thủ tục truyền dữ liệu, quản lý quá trình đồng bộ của các trạm cuối, cho đến việc xử lý các ngắt từ các trạm cuối.

Những năm 70: Các máy tính đã được nối với nhau trực tiếp thành một mạng máy tính nhằm phân tán tài của hệ thống và tăng độ tin cậy và người ta bắt đầu xây dựng mạng truyền thông trong đó các thành phần chính của nó là các nút mạng(node) gọi là bộ chuyển mạch, dung để hướng thông tin tới đích.

Từ thập kỷ 80 trở đi: Việc kết nối mạng máy tính đã bắt đầu dược thực hiện rộng rãi nhờ tỷ lệ giữa giá thành máy tính và chuyển chi phí truyền tin đã giảm đi rõ rệt do sự bùng nổ của các thế hệ máy tính cá nhân.

**1.2.2. Nhu cầu và mục đích của việc kết nối các máy tính thành mạng**

Việc nối máy tính thành mạng từ lâu đã trở thành một nhu cầu khách quan bởi vì:

- Có rất nhiều công việc về bản chất là phân tán hoạc về thông tin, hoặc về xử lý hoặc cả hai đòi hỏi có sự kết hợp truyền thông với xử lý hoặc sử dụng phương tiện từ xa.

- Chia sẻ các tài nguyên trên mạng cho nhiều người sử dụng tại một thời điểm(ổ cứng, máy in, ổ CD ROM…).

- Nhu cầu liên lạc trao đổi thông tin nhờ phương tiện máy tính.

- Các ứng dụng phần mềm đòi hỏi tại một thời điểm cần có nhiều người sử dụng, truy cập vào cùng một cơ sở dữ liệu.

Chính vì vậy, việc kết nối các máy tính thành mạng nhằm mục đích:

* Chia sẻ tài nguyên:
* Chia sẻ dữ liệu: Về nguyên tắc, bất kỳ người sử dụng nào trên mạng đều có quyền truy cập, khai thác và sử dụng những tài nguyên chung của mạng( thường là server).
* Chia sẻ phần cứng: Tài nguyên chung của mạng cũng bao gồm các máy móc, thiết bị như: Máy in(Printer), máy quét(Scanner), ổ đĩa mềm(Floppy), ổ đĩa CD(CD Rom) được nối vào mạng. Thông qua mạng máy tính, người sử dụng có thể sử dụng những tài nguyên phần cứng này ngay cả khi máy tính của họ không có những phần cứng đó.
* Duy trì và bảo vệ dữ liệu: Một mạng máy tính có thể cho phép cá dữ liệu được tự động lưu trữ dự phòng tới một trung tâm nào đó trong mạng. Công việc này là hết sức khó khăn và tốn nhiều thời gian nếu phải làm trên từng máy độc lập. Hơn nữa, mạng máy tính còn cung cấp cơ chế bảo mật(security) bằng mật khẩu (password) đối với người sử dụng, hạn chế được việc sao chép, mất mát thông tin ngoài ý muốn.
* Nâng cao độ tin cậy của hệ thống nhờ kahr năng thay thế cho nhau khi xảy ra sự cố kỹ thuật đối với một máy tính nào đó trong mạng.
* Khai thác có hiệu quả các cơ sở dữ liệu tập trung và phân tán, nâng cao khả năng tích hợp và trao đổi các loại dữ liệu giữa các máy tính trên mạng.

**1.2.3. Đặc trưng kỹ thuật của mạng máy tính**

**1.2.3.1. Đường truyền**

Là thành tố quan trọng của một mạng máy tính, là phương tiện dung để truyền các tín hiệu điện tử giữa các máy tính. Các tín hiệu điện tử đó chính là các thông tin, dữ liệu được biểu thị dưới dạng các xung nhị phân(On-Off), mọi tín hiệu truyền giữa các máy tính với nhau đều thuộc song điện từ.

* Các tần số radio có thể truyền bằng cáp điện (dây xoắn đôi hoặc đồng trục) hoặc bằng phương tiện quảng bá (radio broadcasting).
* Sóng cực ngắn (viba) thường được dung để truyền giữa các trạm mặt đất và các vệ tinh. Chúng cũng được dung để truyền các tín hiệu quảng bá từ một trạm phát đến nhiều trạm thu. Mạng điện thoại “tổ ong” là một ví dụ cho cách dung này.
* Tia hồng ngoài là lý tưởng đối với nhiều laoij truyền thông mạng. Tia hồng ngoại và các tần số cao hơn của ánh sáng có thể được truyền qua cáp sợ quang. CÁc đặc trưng cơ bản của đường truyền là giải thông (bandwidth), độ suy hao và độ nhiễu điện tử.
* Dải thông của một đường truyền chính là độ đo phạm vi tần số mà nó có thể đáp ứng được, nó biểu thị khả năng truyền tải tín hiệu của đường truyền. Tốc độ truyền dữ liệu trên đường truyền được gọi là thông lượng(throughput) của đường truyền, thường được tính bằng số lượng bit được truyền đi trong một giây(bps). Giải thông của cáp truyền phụ thuộc vào độ dài cáp(nói chung cáp ngắn có thể có giải thông lớn hơn so với cáp dài). Bởi vậy, khi thiết kế cáp cho mạng cần thiết phải chỉ rõ độ dài chạy cáp tối đa vì ngoài giới hạn đó chất lượng truyền tín hiệu không còn được đảm bảo.
* Độ suy hao của một đường truyền là độ đo sự yếu đi của tín hiệu trên đường truyền đó, nó cũng phụ thuộc vào độ dài cáp. Còn độ nhiễn điện từ EMI (Electronmangetic Interference) gây ra bởi tiếng ồn từ bên ngoài làm ảnh hưởng đến tín hiệu trên đường truyền.

Thông thường người ta hay phân loại đường truyền thaeo hai loại:

* Đường truyền hữu tuyến: Cá máy tính được nối với nhau bằng các dây cáp mạng. Đường truyền hữu tuyến gồm có:
* Cáp đồng trục (Coaxial cable).
* Cáp xoắn đôi (Twisted pải cable) gồm 2 loại có bọc kim (stp- shieldel twisted pair) và không bọc kim (utp – Unshieldel twisted pair).
* Cáp sợi quang(Fiber optic cable).
* Đường truyền vô tuyến: các máy tính truyền tín hiệu với nhau thông qua các song vô tuyến với các thiết bị điều chế/ giải điều chế ở các đầu mút. Đường truyền vô tuyến gồm có:
* Radio.
* Sóng cực ngắn (Viba).
* Tia hồng ngoại (Infrared).

**1.2.3.2. Kiến trúc mạng**

Kiến trúc mạng(network architecture) thể hiện cách nối giữa các máy tính trong mạng và tập hợp các quy tắc, quy ước nào đó mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo để đảm bảo cho mạng hoạt động tốt.

**1.2.3.2.1. Hình tạng mạng**

Hình trạng mạng là cách kết nối các máy tính với nhau về mặt hình học mà ta gọi là “topology” của mạng.

Có 2 kiểu nối mạng chủ yếu là điểm – điểm (point to point) và điểm – đa điểm (point to multipoint).

* Theo kiểu điểm – điểm: Các đường truyền nối từng cặp nút với nhau và mỗi nút đều có trách nhiệm lưu trữ tạm thời sau đó chuyển tiếp dữ liệu đi cho tới đích. Một số mạng có cấu trúc điểm – điểm như: mạng hình sao, mạng chu trình…
* Theo kiểu điểm – đa điểm: Tất cả các nút phân chia chung một đường truyền vật lý. Dữ liệu gửi đi từ một nút nào đó sẽ có thể được tiếp nhận bởi tất cả các nút còn lại. Bởi vậy cần chỉ ra địa chỉ đích của dữ liệu để mỗi nút căn cứu vào đó kiểm tra xem dữ liệu có phải gửi cho mình hay không. Mạng trực tuyến tính (bú), mạng hình vòng(ring), mạng vệ tinh(satellite) hay radio… là những mạng có cấu trúc điểm – đa điểm phổ biến.

**1.2.3.2.2. Giao thức mạng**

Việc trao đổi thông tin dù là đơn giản nhất, cũng phải tuân theo những quy tắc nhất định. Đơn giản như khi hai người nói chuyện với nhau muốn cho cuộc nói chuyện có kết quả thì ít nhất cả hai cũng phải ngầm hiểu và tuân theo và tuân thủ quy ước : khi một người nói thì người kia phải nghe và ngược lại. Việc truyền thông trên mạng cũng vậy, cần có các quy tắc, quy ước truyền thông về nhiều mặt: khuôn dạng cú pháp của dữ liệu, các thủ tục gửi , nhận dữ liệu , kiểm soát hiệu quả và chất lượng truyền tin … Tập hợp những quy tắc quy ước truyền thông đó được gọi là giao thức của mạng (network protocol).

Có rất nhiều giao thức mạng, các mạng có thê sử dụng cá giao thức khác nhau tùy sự lựa chọn của người thiết kế. Tuy vậy, các giao thức thường gặp nhất là : TCP/IP, NETBIOS, IPX/SPX, …

**1.2.3.3. Hệ điều hành mạng**

Hệ điều hành mạng là một phần mềm hệ thống có các chức năng sau:

* Quản lý tài nguyên của hệ thống, các tài nguyên này gồm: