BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

LÊ HOÀNG TRUNG THÔNG

NGHIÊN CỨU NEURAL CRYPTOGRAPHY VÀ ỨNG DỤNG BẢO MẬT TÀI LIỆU CHO CÔNG TY KIÊN NHẪN

LUẬN VĂN THẠC SĨ

Chuyên ngành : Công Nghệ Thông Tin

Mã số ngành: 60480201

TP. Hồ Chí Minh, Tháng 09 Năm 2016

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

LÊ HOÀNG TRUNG THÔNG

NGHIÊN CỨU NEURAL CRYPTOGRAPHY VÀ ỨNG DỤNG BẢO MẬT TÀI LIỆU CHO CÔNG TY KIÊN NHẪN

LUẬN VĂN THẠC SĨ

Chuyên ngành : Công Nghệ Thông Tin

Mã số ngành: 60480201

CÁN BỘ HƯỚNG DẪN KHOA HỌC: TS LƯ NHẬT VINH

TP. Hồ Chí Minh, Tháng 06 Năm 2016

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

Cán bộ hướng dẫn khoa học : TS Lư Nhật Vinh
(Ghi rõ họ, tên, học hàm, học vị và chữ ký)

Luận văn Thạc sĩ được bảo vệ tại Trường Đại học Công nghệ TP. HCM ngày … tháng … năm …

Thành phần Hội đồng đánh giá Luận văn Thạc sĩ gồm:

TT	Họ và tên	Chức danh Hội đồng
1	PGS.TS. Võ Đình Bảy	Chủ tịch
2	TS. Lê Văn Quốc Anh	Phản biện 1
3	TS. Văn Thiên Hoàng	Phản biện 2
4	PGS.TS. Quản Thành Thơ	Ủy viên
5	TS. Cao Tùng Anh	Ủy viên, Thư ký

Xác nhận của Chủ tịch Hội đồng đánh giá Luận sau khi Luận văn đã được sửa chữa (nếu có).

Chủ tịch Hội đồng đánh giá LV

TRƯỜNG ĐH CÔNG NGHỆ TP. HCM

PHÒNG QLKH – ĐTSĐH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

TP.HCM, Ngày……tháng……năm…..

NHIỆM VỤ LUẬN VĂN THẠC SĨ

Họ tên học viên: .....LÊ HOÀNG TRUNG THÔNG.....Giới tính: ..Nam

Ngày, tháng, năm sinh: 10-05-1992.....Nơi sinh:..An Giang ....

Chuyên ngành: .....Công nghệ thông tin.....MSHV:1441860038....

I- Tên đề tài:

NGHIÊN CỨU NEURAL CRYPTOGRAPHY
VÀ ỨNG DỤNG BẢO MẬT TÀI LIỆU CHO CÔNG TY KIÊN NHẪN

II- Nhiệm vụ và nội dung:

- Nghiên cứu và tìm hiểu về mạng nơron nhân tạo. Tìm hiểu về các thuật toán trao đổi khóa, mã hóa , giải mã. Từ đó xây dựng chương trình mã hóa các văn bản tài liệu dựa vào mạng nơron nhân tạo.
    - Nghiên cứu về Neural Cryptography
    - Nghiên cứu về mô hình ứng dụng Neural Cryptography vào mã hóa bảo mật.
    - Cuối cùng phát triển thuật toán vào chương trình mã hóa các tài liệu bí mật của công ty.

III- Ngày giao nhiệm vụ: *20/01/2016*

IV- Ngày hoàn thành nhiệm vụ: 20/07/2016

V- Cán bộ hướng dẫn: TS LƯ NHẬT VINH .....

CÁN BỘ HƯỚNG DẪN
(Họ tên và chữ ký)

Lư Nhật Vinh

KHOA QUẢN LÝ CHUYÊN NGÀNH
(Họ tên và chữ ký)

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các số liệu, kết quả nêu trong Luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tôi xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện Luận văn này đã được cảm ơn và các thông tin trích dẫn trong Luận văn đã được chỉ rõ nguồn gốc.

Học viên thực hiện Luận văn

(Ký và ghi rõ họ tên)

Lê Hoàng Trung Thông

LỜI CẢM ƠN

Trước tiên, tôi xin được gửi lời cảm ơn đến Ban Giám Hiệu, toàn thể cán bộ nhân viên, giảng viên trường Đại Học HUTECH, Ban lãnh đạo Phòng Quản Lý Khoa Học và Đào Tạo Sau Đại Học, khoa Công Nghệ Thông Tin đã tạo điều kiện thuận lợi cho chúng tôi học tập và nghiên cứu trong suốt học trình cao học. Xin được gửi lời cảm ơn đến tất cả quý thầy cô đã giảng dạy trong chương trình Đào tạo thạc sĩ chuyên ngành Công nghệ thông tin, , lớp 14SCT21 - Trường Đại học Công Nghệ TPHCM, những người đã truyền đạt cho tôi những kiến thức hữu ích để làm cơ sở cho tôi thực hiện tốt luận văn này.

Với lòng kính trọng và biết ơn, tôi xin bày tỏ lời cảm ơn đến TS Lư Nhật Vinh đã tận tình hướng dẫn cho tôi trong thời gian thực hiện luận văn, những gì thầy đã hướng dẫn, chỉ bảo đã cho tôi nhiều kinh nghiệm trong thời gian thực hiện luận văn.

Sau cùng tôi xin gửi lời biết ơn sâu sắc đến bạn bè, gia đình, các anh chị trong tập thể lớp 14SCT21 đã luôn tạo điều kiện tốt nhất cho tôi trong suốt quá trình học cũng như thực hiện luận văn.

Do thời gian có hạn và kinh nghiệm nghiên cứu khoa học chưa nhiều nên luận văn còn nhiều thiếu sót, rất mong nhận được ý kiến góp ý của Thầy/Cô và các anh chị học viên.

TÓM TẮT

Ngày nay trong mọi hoạt động của con người thông tin đóng một vai trò quan trọng không thể thiếu. Xã hội càng phát triển nhu cầu trao đổi thông tin giữa các thành phần trong xã hội ngày càng lớn. Mạng máy tính ra đời đã mang lại cho con người rất nhiều lợi ích trong việc trao đổi và xử lý thông tin một cách nhanh chóng và chính xác. Chính từ những thuận lợi này đã đặt ra cho chúng ta một câu hỏi, liệu thông tin đi từ nơi gửi đến nơi nhận có đảm bảo tuyệt đối an toàn, ai có thể đảm bảm thông tin của ta không bị truy cập bất hợp pháp.

Mã hóa được coi là thành phần cực kì quan trọng trong việc bảo mật những tài liệu bí mật của các tổ chức, công ty nhằm tránh lộ ra những thông tin mật thiết cho các đối thủ cạnh tranh trực tiếp hoặc những thành phần mang tính phá hoại.

Trong nghiên cứu này chúng tôi xây dựng một chương trình mã hóa các tài liệu dựa trên mạng neural nhân tạo. Nhằm tạo ra một hướng mã hóa mới so với những phương thức đã có trước đây.

ABSTRACT

Nowadays in all activities information has an important role indispensable. The more society developed needs to exchange information between people the more developed.

Computer networks launched to bring people a lot of benefits in the exchange and processing information quickly and accurately. Therefore, these advantages has posed us a question, whether the information away from the place where sent to recipients has ensured absolute safety. Who can guarantee that without anyone can access illegally our information ?

Encryption is considered extremely important component in security the secret documents of the organizations, companies to avoid revealing confidential information for the direct competitors or components destructive.

In this research I created a coded program documents based on Neural networks, purpose to create a new encryption direction than previous methods had.

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Kí hiệu		
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
ANN	Artificial Nơron Network	Mạng nơron nhân tạo
DES	Data Encryption Standard	Tiêu chuẩn mã hoá dữ liệu
IDEA	International Data Encryption Algorithm	Thuật toán mật mã hóa dữ liệu quốc tế
GPG	GNU Privacy Guard	
NN	Nơron Network	Mạng nơron
NIST	National Institute of Standards and Technology	Viện tiêu chuẩn và công nghệ
RSA		Tên của thuật toán lấy từ 3 chữ cái của 3 tác giả Ron Rivest, Adi Shamir và Len Adleman
SSL	Secure Sockets Layer	
PE	Processing Elements	Các yếu tố xử lý
PGP	Pretty Good Privacy	
MLP	Multi Layer Perceptron	Mạng nơron nhiều tầng truyền thẳng
TPM	Tree Parity Machines	

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH

MỞ ĐẦU

1. Đặt vấn đề

Ngày nay trong mọi hoạt động của con người thông tin đóng một vai trò quan trọng không thể thiếu. Xã hội càng phát triển nhu cầu trao đổi thông tin giữa các thành phần trong xã hội ngày càng lớn. Mạng máy tính ra đời đã mang lại cho con người rất nhiều lợi ích trong việc trao đổi và xử lý thông tin một cách nhanh chóng và chính xác. Chính từ những thuận lợi này đã đặt ra cho chúng ta một câu hỏi, liệu thông tin đi từ nơi gửi đến nơi nhận có đảm bảo tuyệt đối an toàn, ai có thể đảm bảm thông tin của ta không bị truy cập bất hợp pháp. Thông tin được lưu giữ, truyền dẫn, cùng sử dụng trên mạng lưới thông tin công cộng có thể bị nghe trộm, chiếm đoạt, xuyên tạc hoặc phá huỷ dẫn đến sự tổn thất không thể lường được. Đặc biệt là đối với những số liệu của hệ thống ngân hàng, hệ thống thương mại, cơ quan quản lý của chính phủ hoặc thuộc lĩnh vực quân sự được lưu giữ và truyền dẫn trên mạng. Nếu như vì nhân tố an toàn mà thông tin không dám đưa lên mạng thì hiệu suất làm việc cũng như hiệu suất lợi dụng nguồn dữ liệu đều sẽ bị ảnh hưởng. Trước các yêu cầu cần thiết đó, việc mã hoá thông tin sẽ đảm bảo an toàn cho thông tin tại nơi lưu trữ cũng như khi thông tin được truyền trên mạng.

Mã hóa cũng được coi là thành phần cực kì quan trọng trong việc bảo mật những tài liệu bí mật của các tổ chức, công ty nhằm tránh lộ ra những thông tin mật thiết cho các đối thủ cạnh tranh trực tiếp hoặc những thành phần mang tính phá hoại.

2. Lý do chọn đề tài

Hiện nay đã có khá nhiều phương pháp mã hóa đã được ứng dụng và cho thấy được những ưu nhược điểm tùy theo nhu cầu sử dụng của khách hàng như mã hóa cổ điển(mật mã Caesar , mã thay thế, mã vigenère, mã hoán vị, DES (Data Encryption Standard)..), thuật toán mã hóa công khai(hệ mã RSA, hệ mật Elgamal, …).

Trong nghiên cứu này tôi xây dựng một chương trình mã hóa các tài liệu dựa trên mạng neural nhân tạo. Nhằm thay thế và tối ưu các phương pháp mã hóa đã có trước đây.

Những câu hỏi đặt ra khi nghiên cứu:

Mạng neural nhân tạo có đảm bảo tính bảo mật?

Mạng neural nhân tạo có ưu điểm gì so với các phương pháp mã hóa khác?

Độ phức tạp của mạng neural nhân tạo là bao nhiêu, tính bảo mật có độ hiệu quả là bao nhiêu?

3. Mục tiêu, nội dung và phương pháp nghiên cứu

Nghiên cứu được tiến hành trên đối tượng : Mạng neural nhân tạo

Phạm vi nghiên cứu : ứng dụng vào mã hóa các tài liệu mật của công ty.

❖ Mục tiêu của đề tài

Trong đề tài tôi đặt ra 3 mục tiêu cần giải quyết như sau;

- Nghiên cứu về Neural Crytography
- Nghiên cứu về mô hình ứng dụng Neural Crytography vào mã hóa bảo mật.
- Cuối cùng phát triển thuật toán vào chương trình mã hóa các tài liệu bí mật của công ty.

❖ Đối tượng và phạm vi nghiên cứu

Đề tài cần nghiên cứu các yếu tố chính sau:

- Nghiên cứu mạng neural, đặc trưng, cách xây dựng và huấn luyện neural nhân tạo.
- Nghiên cứu cách thức và thuật toán ứng dụng vào mã hóa văn bản của mạng neural nhân tạo.
- Đánh giá ưu nhược điểm của thuật toán.

❖ Phương pháp nghiên cứu

Phương pháp nghiên cứu lý thuyết:

Tiến hành thu thập và nghiên cứu các tài liệu liên quan đến đề tài.
Nghiên cứu mạng neural nhân tạo.
Nghiên cứu đặc trưng, cách xây dựng và huấn luyện neural nhân tạo.
Nghiên cứu ứng dụng của mạng neural nhân tạo vào việc mã hóa văn bản .

Phương pháp nghiên cứu thực nghiệm:

Nghiên cứu cách xây dựng chương trình mã hóa các loại văn bản , tài liệu dựa trên mạng nerual nhân tạo.
Ngôn ngữ sử dụng : C# trong bộ Visual studio 2015
Thử nghiệm trong nội bộ công ty Kiên Nhẫn
Đánh giá kết quả đạt được

❖ **Cấu trúc của luận văn**

Nội dung báo cáo gồm những chương sau:

MỞ ĐẦU

CHƯƠNG 1: Cơ sở lý thuyết

CHƯƠNG 2: Ứng dụng mạng nơron vào bảo mật

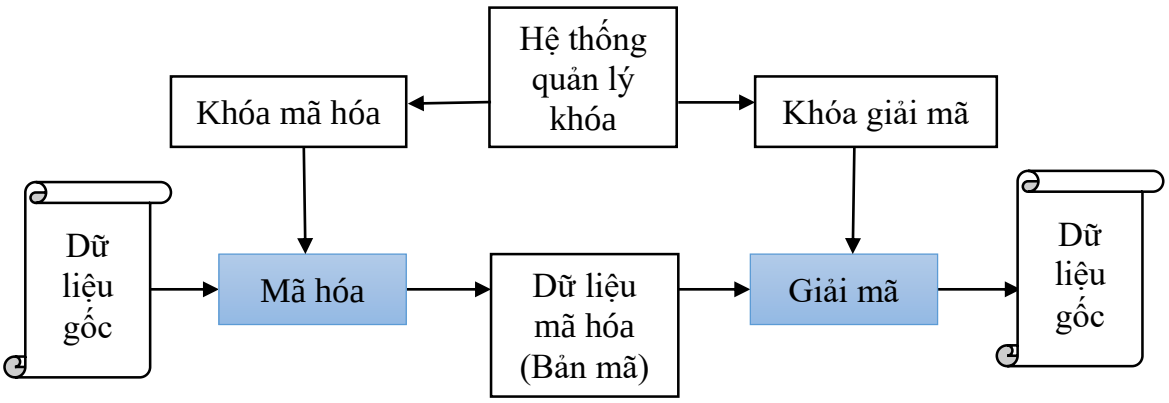
CHƯƠNG 3: Cài đặt chương trình thử nghiệm

CHƯƠNG 1: CƠ SỞ LÝ THUYẾT

1.1 MẬT MÃ HỌC (CRYPTOGRAPHY)

1.1.1 Giới thiệu chung

Mật mã học là ngành khoa học ứng dụng toán học vào việc biến đổi thông tin thành một dạng khác với mục đích che giấu nội dung, ý nghĩa thông tin cần mã hoá. Đây là một ngành quan trọng và có nhiều ứng dụng trong đời sống xã hội. Ngày nay, các ứng dụng mã hóa và bảo mật thông tin đang được sử dụng ngày càng phổ biến hơn trong các lĩnh vực khác nhau trên thế giới, từ các lĩnh vực an ninh, quân sự, quốc phòng…cho đến các lĩnh vực dân sự như thương mại điện tử, ngân hàng…



Hình 1.1 Sơ đồ mã hóa và giải mã

Cùng với sự phát triển của khoa học máy tính và internet, các nghiên cứu và ứng dụng của khoa học mật mã ngày càng trở nên đa dạng hơn, mở ra nhiều hướng nghiên cứu chuyên sâu vào từng lĩnh vực ứng dụng đặc thù với những đặc trưng riêng.

Ứng dụng của khoa học mật mã không chỉ đơn thuần là mã hóa và giải mã thông tin mà còn bao gồm nhiều vấn đề khác nhau cần được nghiên cứu và giải quyết: chứng thực nguồn gốc nội dung thông tin (kỹ thuật chữ ký điện tử), chứng nhận tính xác thực về người sở hữu mã khóa (chứng nhận khóa công

cộng), các quy trình trao đổi thông tin và thực hiện giao dịch điện tử an toàn trên mạng…

Những kết quả nghiên cứu về mật mã cũng đã được đưa vào trong các hệ thống phức tạp hơn, kết hợp với những kỹ thuật khác để đáp ứng các yêu cầu đa dạng của các hệ thống ứng dụng khác nhau trong thự tế, ví dụ như hệ thống bỏ phiếu bầu cử qua mạng, hệ thống đào tạo từ xa, hệ thống quản lý an ninh của các đơn vị với hướng tiếp cận sinh trắc học, hệ thống cung cấp dịch vụ multimedia trên mạng với yêu cầu cung cấp dịch vụ và bảo vệ bản quyền sở hữu trí tuệ đối với thông tin số…

1.1.2 Định nghĩa:

Mật mã học là sự nghiên cứu các phương pháp toán học, liên quan đến một số khía cạch của thông tin như an toàn, sự toàn vẹn dữ liệu, sự xác nhận tồn tại và sự xác nhận tính nguyên bản của thông tin. [10]

1.2 MÃ HÓA

1.2.1 Khái niệm

Mã hóa (Encryption): là quá trình chuyển thông tin có thể đọc được (gọi là bản rõ) thành thông tin " khó " có thể đọc được theo cách thông thường (gọi là bản mã) đó là một trong những kỹ thuật để bảo mật thông tin.

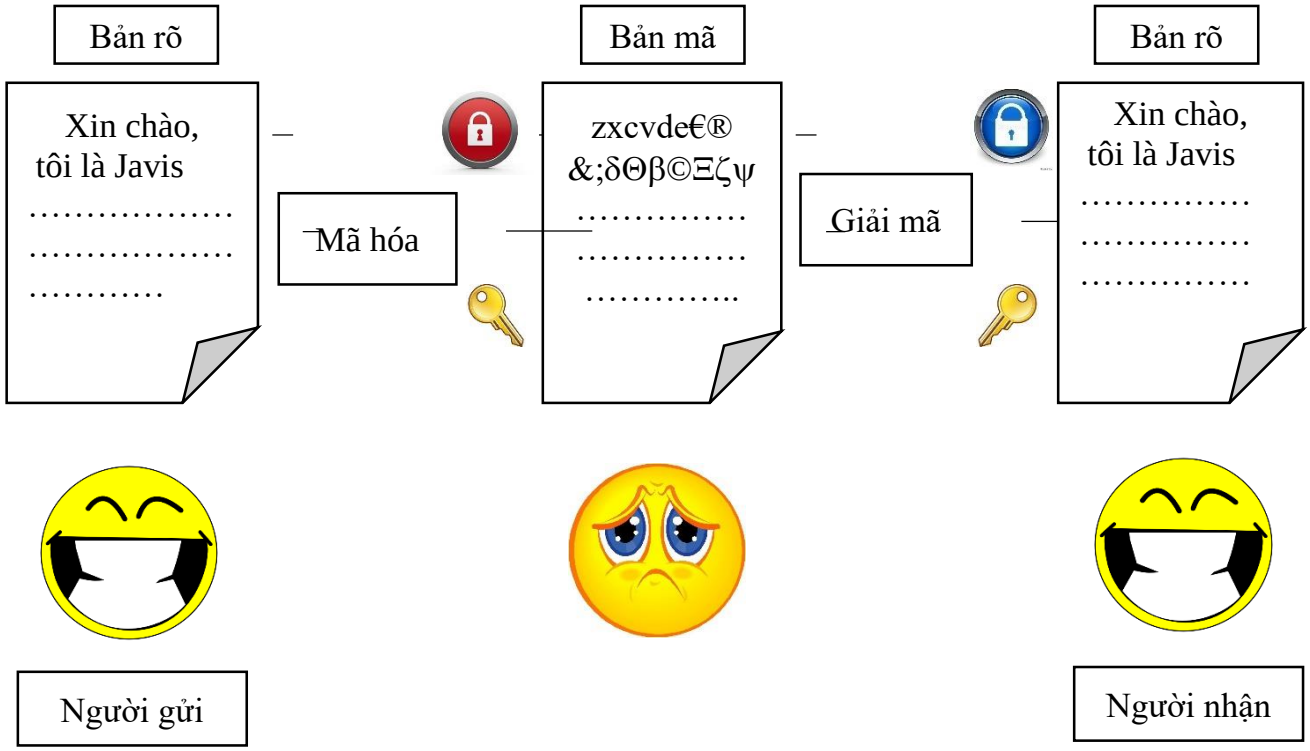
Giải mã (Decryption): là quá trình chuyển thông tin ngược lại từ bản mã thành bản rõ. Thuật toán mã hóa hay giải mã là thủ tục để thực hiện mã hóa hay giải mã.

Mã hóa đối xứng : Khóa E = Khóa D

Mã hóa bất đối xứng : Khóa E ≠ Khóa D

Khóa mã hóa là giá trị làm cho thuật toán mã hóa thực hiện theo cách riêng biệt và sinh ra bản rõ riêng. Thông thường khóa càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể có của khóa được gọi là không gian khóa.

Hệ mã hóa là tập các thuật toán, các khóa nhằm che giấu thông tin cũng như làm rõ nó.



Hình 1.2 Sơ đồ hệ thống mã hóa

Cryptography (hay crypto) – mật mã học – ngành khoa học nghiên cứu về việc giấu thông tin. Cụ thể hơn, mật mã học là ngành học nghiên cứu về những cách chuyển đổi thông tin từ dạng "có thể hiểu được" thành dạng "không thể hiểu được" và ngược lại. Cryptography giúp đảm bảo những tính chất sau cho thông tin:

Tính bí mật (confidentiality): thông tin chỉ được tiết lộ cho những ai được phép.

Tính toàn vẹn (integrity): thông tin không thể bị thay đổi mà không bị phát hiện.

Tính xác thực (authentication): người gửi (hoặc người nhận) có thể chứng minh đúng họ.

Tính không chối bỏ (non-repudiation): người gửi hoặc nhận sau này không thể chối bỏ việc đã gửi hoặc nhận thông tin.

Mật mã có rất nhiều ứng dụng trong thực tế như bảo vệ giao dịch tài chính (rút tiền ngân hàng, mua bán qua mạng), bảo vệ bí mật cá nhân… Nếu kẻ tấn công đã vượt qua tường lửa và các hệ thống bảo vệ khác thì mật mã chính là hàng phòng thủ cuối cùng cho dữ liệu của bạn.

Cần phân biệt khái niệm cryptography với khái niệm steganography (tạm dịch là giấu thông tin). Điểm khác nhau căn bản nhất giữa hai khái niệm này là: cryptography là việc giấu nội dung của thông tin, trong khi steganography là việc giấu sự tồn tại của thông tin đó.

Cryptosystem (viết tắt của cryptographic system): hệ thống mã hóa thông tin, có thể là phần mềm như PGP, Ax-Crypt, Truecrypt… giao thức như SSL, IPsec… hay đơn giản là một thuật toán như DES.

Encrypt (encipher): mã hóa – quá trình biến đổi thông tin từ dạng ban đầu -> có thể hiểu được thành dạng không thể hiểu được, với mục đích giữ bí mật thông tin đó.

Decrypt (decipher): giải mã – quá trình ngược lại với mã hóa, khôi phục lại thông tin ban đầu từ thông tin đã được mã hóa.

Plaintext (cleartext): dữ liệu gốc (chưa được mã hóa).

Ciphertext: dữ liệu đã được mã hóa.

Cipher (hay cypher): thuật toán dùng để thực hiện quá trình mã hóa hay giải mã. Trong khuôn khổ bài viết này gọi tắt là thuật toán.

Key: chìa khóa – thông tin dùng cho qui trình mã hóa và giải mã.

Code: cần phân biệt code trong mật mã học với code trong lập trình hay code trong Zip code… Trong cryptography, code (mã) có ý nghĩa gần như là cipher (thuật toán). Chúng chỉ khác nhau ở chỗ: code biến đổi thông tin ở tầng nghĩa (từ, cụm từ) còn cipher biến đổi thông tin ở tầng thấp hơn, ví dụ chữ cái (hoặc cụm chữ cái) đối với các thuật toán cổ điển hay từng bit (hoặc nhóm bit) đối với các thuật toán hiện đại.

Cryptanalysis: nếu coi mật mã học là việc cất dữ liệu của bạn vào một cái hộp sau đó dùng chìa khóa khóa lại, thì cryptanalysis là ngành nghiên cứu những phương pháp mở hộp để xem dữ liệu khi không có chìa khóa.

1.2.2 Các kỹ thuật mã hóa :

1.2.2.1 Mã hóa đối xứng (mã hóa không công khai)

Là lớp thuật toán các mã hóa trong đó việc mã hóa và giải mã đều dùng chung cho một khóa (secret key).

❖ *Các loại thuật toán khóa đối xứng*

Thuật toán đối xứng có thể được chia ra làm hai thể loại, mật mã luồng (stream ciphers) và mật mã khối (block ciphers). Mật mã luồng mã hóa từng bit của thông điệp trong khi mật mã khối gộp một số bit lại và mã hóa chúng như một đơn vị. Cỡ khối được dùng thường là các khối 64 bit. Thuật toán AES được NIST công nhận tháng 12 năm 2001, sử dụng các khối gồm 128 bit.

Các thuật toán đối xứng thường không được sử dụng độc lập. Trong thiết kế của các hệ thống mật mã hiện đại, cả hai thuật toán bất đối xứng và thuật toán đối xứng được sử dụng phối hợp để tận dụng các ưu điểm của cả hai. Những hệ thống sử dụng cả hai thuật toán bao gồm những cái như SSL, PGP và GPG v.v. Các thuật toán chìa khóa bất đối xứng được sử dụng để phân phối chìa khóa mật cho thuật toán đối xứng có tốc độ cao hơn.

❖ *Tốc độ*

Các thuật toán đối xứng nói chung đòi hỏi công suất tính toán ít hơn các thuật toán khóa bất đối xứng. Trên thực tế, một thuật toán khóa bất đối xứng có khối lượng tính toán nhiều hơn gấp hằng trăm, hằng ngàn lần một thuật toán khóa đối xứng có chất lượng tương đương.

❖ *Hạn chế*

Hạn chế của các thuật toán khóa đối xứng bắt nguồn từ yêu cầu về sự phân hưởng chìa khóa bí mật, mỗi bên phải có một bản sao của chìa. Do khả

năng các chìa khóa có thể bị phát hiện bởi đối thủ mật mã, chúng thường phải được bảo an trong khi phân phối và trong khi dùng. Hậu quả của yêu cầu về việc lựa chọn, phân phối và lưu trữ các chìa khóa một cách không có lỗi, không bị mất mát là một việc làm khó khăn, khó có thể đạt được một cách đáng tin cậy.

Để đảm bảo giao thông liên lạc an toàn cho tất cả mọi người trong một nhóm gồm n người, tổng số lượng chìa khóa cần phải có là $\frac{n(n-1)}{2}$

Hiện nay người ta phổ biến dùng các thuật toán bất đối xứng có tốc độ chậm hơn để phân phối chìa khóa đối xứng khi một phiên giao dịch bắt đầu, sau đó các thuật toán khóa đối xứng tiếp quản phần còn lại . Vấn đề về bảo quản sự phân phối chìa khóa một cách đáng tin cậy cũng tồn tại ở tầng đối xứng, song ở một điểm nào đấy, người ta có thể kiểm soát chúng dễ dàng hơn. Tuy thế, các khóa đối xứng hầu như đều được sinh tạo tại chỗ.

Các thuật toán khóa đối xứng không thể dùng cho mục đích xác thực (authentication) hay mục đích chống thoái thác (non-repudiation) được.

1.2.2.2 *Mã hóa bất đối xứng* (Mã hóa công khai)

Là thuật toán trong đó việc mã hóa và giãi mã dùng hai khóa khác nhau là pulic key (khóa công khai) và private key (khóa riêng).

Nếu dùng public key để mã hóa thì private key sẽ dùng để giải mã và ngược lại

❖ *An toàn*

Về khía cạnh an toàn, các thuật toán mật mã hóa bất đối xứng cũng không khác nhiều với các thuật toán mã hóa đối xứng. Có những thuật toán được dùng rộng rãi, có thuật toán chủ yếu trên lý thuyết; có thuật toán vẫn được xem là an toàn, có thuật toán đã bị phá vỡ… Cũng cần lưu ý là những thuật toán được dùng rộng rãi không phải lúc nào cũng đảm bảo an toàn. Một số thuật toán có những chứng minh về độ an toàn với những tiêu chuẩn khác nhau. Nhiều chứng minh gắn việc phá vỡ thuật toán với những bài toán nổi tiếng vẫn được cho là không có lời giải trong thời gian đa thức. Vì vậy, cũng giống như

tất cả các thuật toán mật mã nói chung, các thuật toán mã hóa khóa công khai cần phải được sử dụng một cách thận trọng.

❖ *Ứng dụng*

Ứng dụng rõ ràng nhất của mật mã hóa khóa công khai là bảo mật: một văn bản được mã hóa bằng khóa công khai của một người sử dụng thì chỉ có thể giải mã với khóa bí mật của người đó.

Các thuật toán tạo chữ ký số khóa công khai có thể dùng để nhận thực. Một người sử dụng có thể mã hóa văn bản với khóa bí mật của mình. Nếu một người khác có thể giải mã với khóa công khai của người gửi thì có thể tin rằng văn bản thực sự xuất phát từ người gắn với khóa công khai đó.

❖ *Hạn chế*

Tồn tại khả năng một người nào đó có thể tìm ra được khóa bí mật. Không giống với hệ thống mật mã sử dụng một lần (one-time pad) hoặc tương đương, chưa có thuật toán mã hóa khóa bất đối xứng nào được chứng minh là an toàn trước các tấn công dựa trên bản chất toán học của thuật toán. Khả năng một mối quan hệ nào đó giữa 2 khóa hay điểm yếu của thuật toán dẫn tới cho phép giải mã không cần tới khóa hay chỉ cần khóa mã hóa vẫn chưa được loại trừ. An toàn của các thuật toán này đều dựa trên các ước lượng về khối lượng tính toán để giải các bài toán gắn với chúng. Các ước lượng này lại luôn thay đổi tùy thuộc khả năng của máy tính và các phát hiện toán học mới.

Khả năng bị tấn công dạng kẻ tấn công đứng giữa (man in the middle attack): kẻ tấn công lợi dụng việc phân phối khóa công khai để thay đổi khóa công khai. Sau khi đã giả mạo được khóa công khai, kẻ tấn công đứng ở giữa 2 bên để nhận các gói tin, giải mã rồi lại mã hóa với khóa đúng và gửi đến nơi nhận để tránh bị phát hiện. Dạng tấn công kiểu này có thể phòng ngừa bằng các phương pháp trao đổi khóa an toàn nhằm đảm bảo nhận thực người gửi và toàn vẹn thông tin.

❖ *Khối lượng tính toán*

Để đạt được độ an toàn tương đương đòi hỏi khối lượng tính toán nhiều hơn đáng kể so với thuật toán mật mã hóa đối xứng. Vì thế trong thực tế hai dạng thuật toán này thường được dùng bổ sung cho nhau để đạt hiệu quả cao. Trong mô hình này, một bên tham gia trao đổi thông tin tạo ra một khóa đối xứng dùng cho phiên giao dịch. Khóa này sẽ được trao đổi an toàn thông qua hệ thống mã hóa khóa bất đối xứng. Sau đó 2 bên trao đổi thông tin bí mật bằng hệ thống mã hóa đối xứng trong suốt phiên giao dịch.

1.3 TỔNG QUAN VỀ MẠNG NƠRON NHÂN TẠO

Sự phát triển của mạng nơron trải qua cả quá trình đưa ra các khái niệm mới lẫn thực thi những khái niệm này.

Dưới đây là các mốc đáng chú ý trong lịch sử phát triển của mạng nơron.

Cuối TK 19, đầu TK 20, sự phát triển chủ yếu chỉ là những công việc có sự tham gia của cả ba ngành Vật lý học, Tâm lý học và Thần kinh học, bởi các nhà khoa học như Hermann von Hemholtz, Ernst Mach, Ivan Pavlov. Các công trình nghiên cứu của họ chủ yếu đi sâu vào các lý thuyết tổng quát về HỌC (Learning), NHÌN (vision) và LẬP LUẬN (conditioning),... và không hề đưa ra những mô hình toán học cụ thể mô tả hoạt động của các nơron.

Mọi chuyện thực sự bắt đầu vào những năm 1940 với công trình của Warren McCulloch và Walter Pitts. Họ chỉ ra rằng về nguyên tắc, mạng của các nơron nhân tạo có thể tính toán bất kỳ một hàm số học hay logic nào.

Tiếp theo hai người là Donald Hebb, ông đã phát biểu rằng việc thuyết lập luận cổ điển (classical conditioning) (như Pavlov đưa ra) là hiện thực bởi do các thuộc tính của từng nơron riêng biệt. Ông cũng nêu ra một phương pháp học của các nơron nhân tạo.

Ứng dụng thực nghiệm đầu tiên của các nơron nhân tạo có được vào cuối những năm 50 cùng với phát minh của mạng nhận thức (perceptron network) và luật học tương ứng bởi Frank Rosenblatt. Mạng này có khả năng nhận dạng các mẫu. Điều này đã mở ra rất nhiều hy vọng cho việc nghiên cứu

mạng nơron. Tuy nhiên nó có hạn chế là chỉ có thể giải quyết một số lớp hữu hạn các bài toán.[7]

Cùng thời gian đó, Bernard Widrow và Ted Hoff đã đưa ra một thuật toán học mới và sử dụng nó để huấn luyện cho các mạng nơron tuyến tính thích nghi, mạng có cấu trúc và chức năng tương tự như mạng của Rosenblatt. Luật học Widrow-Hoff vẫn còn được sử dụng cho đến nay.

Tuy nhiên cả Rosenblatt và Widrow-Hoff đều cùng vấp phải một vấn đề do Marvin Minsky và Seymour Papert phát hiện ra, đó là các mạng nhận thức chỉ có khả năng giải quyết các bài toán khả phân tuyến tính. Họ cố gắng cải tiến luật học và mạng để có thể vượt qua được hạn chế này nhưng họ đã không thành công trong việc cải tiến luật học để có thể huấn luyện được các mạng có cấu trúc phức tạp hơn.

Do những kết quả của Minsky-Papert nên việc nghiên cứu về mạng nơron gần như bị đình lại trong suốt một thập kỷ do nguyên nhân là không có được các máy tính đủ mạnh để có thể thực nghiệm.

Mặc dù vậy, cũng có một vài phát kiến quan trọng vào những năm 70. Năm 1972, Teuvo Kohonen và James Anderson độc lập nhau phát triển một loại mạng mới có thể hoạt động như một bộ nhớ. Stephen Grossberg cũng rất tích cực trong việc khảo sát các mạng tự tổ chức (Self organizing networks).

Năm 1974 Paul Werbos đã phát triển và ứng dụng phương pháp học lan truyền ngược (back-propagation). Tuy nhiên phải mất một vài năm thì phương pháp này mới trở lên phổ biến. Các mạng lan truyền ngược được biết đến nhiều nhất và được áp dụng rộng dãi nhất nhất cho đến ngày nay.

Vào những năm 80, việc nghiên cứu mạng nơron phát triển rất mạnh mẽ cùng với sự ra đời của PC. Có hai khái niệm mới liên quan đến sự hồi sinh này, đó là:

1. Việc sử dụng các phương pháp thống kê để giải thích hoạt động của một lớp các mạng hồi quy (recurrent networks) có thể được dùng như bộ nhớ

liên hợp (associative memory) trong công trình của nhà vật lý học Johh Hopfield.

2. Sự ra đời của thuật toán lan truyền ngược (back-propagation) để luyện các mạng nhiều lớp được một vài nhà nghiên cứu độc lập tìm ra như: David Rumelhart, James McCelland,.... Đó cũng là câu trả lời cho Minsky-Papert.

Thật không may, những thành công ban đầu này khiến cho con người nghĩ quá lên về khả năng của các mạng nơron. Chính sự cường điệu quá mức đã có những tác động không tốt đến sự phát triển của khoa học và kỹ thuật thời bấy giờ khi người ta lo sợ rằng đã đến lúc máy móc có thể làm mọi việc của con người. Những lo lắng này khiến người ta bắt đầu phản đối các nghiên cứu về mạng neuron. Thời kì tạm lắng này kéo dài đến năm 1981.

Năm 1982 trong bài báo gửi tới viện khoa học quốc gia, John Hopfield bằng sự phân tích toán học rõ ràng, mạch lạc, ông đã chỉ ra cách thức các mạng nơron làm việc và những công việc chúng có thể thực hiện được. Cống hiến của Hopfield không chỉ ở giá trị của những nghiên cứu khoa học mà còn ở sự thúc đẩy trở lại các nghiên cứu về mạng neuron.

Cũng trong thời gian này, một hội nghị với sự tham gia của Hoa Kỳ và Nhật Bản bàn về việc hợp tác/cạnh tranh trong lĩnh vực mạng nơron đã được tổ chức tại Kyoto, Nhật Bản. Sau hội nghị, Nhật Bản đã công bố những nỗ lực của họ trong việc tạo ra máy tính thế hệ thứ 5. Tiếp nhận điều đó, các tạp chí định kỳ của Hoa Kỳ bày tỏ sự lo lắng rằng nước nhà có thể bị tụt hậu trong lĩnh vực này. Vì thế, ngay sau đó, Hoa Kỳ nhanh chóng huy động quĩ tài trợ cho các nghiên cứu và ứng dụng mạng neuron.

Năm 1985, viện vật lý Hoa Kỳ bắt đầu tổ chức các cuộc họp hàng năm về mạng neuron ứng dụng trong tin học (Nơron Networks for Computing).

Ngày nay, không chỉ dừng lại ở mức nghiên cứu lý thuyết, các nghiên cứu ứng dụng mạng nơron để giải quyết các bài toán thực tế được diễn ra ở khắp mọi nơi. Các ứng dụng mạng nơron ra đời ngày càng nhiều và ngày càng hoàn thiện hơn. Điển hình là các ứng dụng: xử lý ngôn ngữ (Language

Processing), nhận dạng kí tự (Character Recognition), nhận dạng tiếng nói (Voice Recognition), nhận dạng mẫu (Pattern Recognition), xử lý tín hiệu (Signal Processing), Lọc dữ liệu (Data Filtering),…..

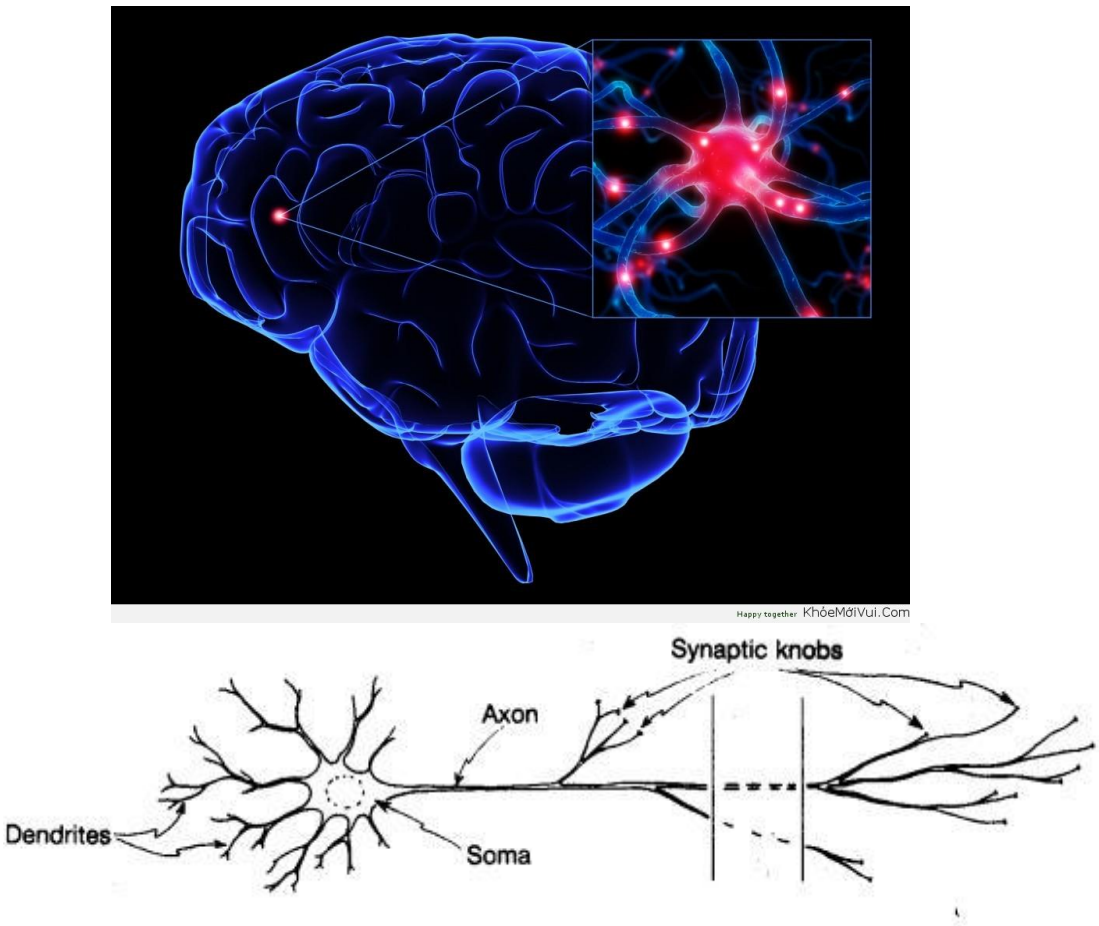
1.4 KHÁI NIỆM VỀ MẠNG NƠRON

1.4.1 Tìm hiểu về nơron

1.4.1.1*Nơron sinh học*:

Qua quá trình nghiên cứu về bộ não, người ta thấy rằng: bộ não con người bao gồm khoảng 10^{11} nơron tham gia vào khoảng 10^{15} kết nối trên các đường truyền. Mỗi đường truyền này dài khoảng hơn một mét. Các nơron có nhiều đặc điểm chung với các tế bào khác trong cơ thể, ngoài ra chúng còn có những khả năng mà các tế bào khác không có được, đó là khả năng nhận, xử lý và truyền các tín hiệu điện hóa trên các đường mòn nơron, các con đường này tạo nên hệ thống giao tiếp của bộ não.

Nơron sinh học được cấu tạo từ những thành phần chính sau: Soma, Dendrites, Axon như hình 1.3.



Hình 1.3 Mô hình nơron sinh học

Soma là thân của nơron .

Các Dendrites là các dây mảnh, dài, gắn liền với soma, chúng truyền dữ liệu (dưới dạng sung điện thế) đến cho soma xử lý. Bên trong soma các dữ liệu đó được tổng hợp lại.

Một loại dây dẫn tính hiệu khác cũng gắn với soma đó là các axon. Khác với dendrites, axon có khả năng phát các xung điện thế, chúng là các dây dẫn tính hiệu đi từ nơron đến các nơi khác. Chỉ khi nào điện thế trong soma vượt quá một giá trị ngưỡng nào đó thì axon mới phát xung điện thế, cón nếu không thì nó ở trạng thái nghỉ.

Axon nối với các Dendrites của một nơron khác qua một mối nối đặc biệt gọi là Synaptic knobs. Khi điện thế của synaptic knobs tăng lên do các

xung phát ra từ axon, thì synaptic knobs sẽ tạo ra một số chất hóa học mà các chất này sẽ mở ‘ cửa’ trên dendrites cho các ions truyền qua. Chính dóng ions này làm thay đổi điện thế tren dendrites, tạo ra các sung dữ liệu lan truyền đến các nơron khác.

Có thể tóm tắt hoạt động của một nơron như sau : nơron lấy tổng tất cả các điện thế vào mà nó nhận được, và phát ra một xung điện thế nếu tổng ấy lớn hơn một ngưỡng nào đó. Các nơron nối với nhau bởi các synaptic knobs. Synaptic knobs được gọi là mạnh khi nó cho phép truyền dẫn dễ dàng tín hiệu qua các nơron khác. Ngược lại, một synaptic knobs yếu sẽ truyền dẫn tín hiệu rất khó khăn.

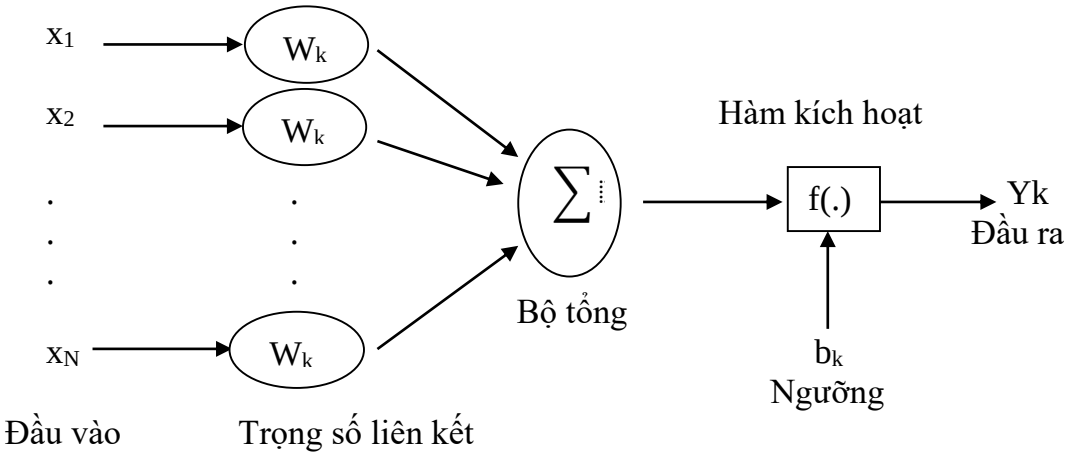
Các synaptic knobs đóng vai trò rất quan trọng trong sự học học tập. Khi chúng ta học tập thì hoạt động của các synaptic knobs tăng cường, tạo nên nhiều liên kết mạnh giữa các nơron. Có thể nói người nào học giỏi thì càng có nhiều synaptic knobs và các synaptic knobs ấy mạnh mẽ, nói cách khác thì liên kết giữa các nơron càng nhiều, càng nhạy bén.

Dựa trên những hiểu biết về nơron sinh học, con người xây dựng nơron nhân tạo với hy vọng tạo nên một mô hình có sức mạnh như bộ não.

1.4.1.2*Nơron nhân tạo*:

Nơron nhân tạo là một đơn vị tính toán có nhiều đầu vào và một đầu ra, mỗi đầu vào đến từ một liên kết. Đặc trưng của nơron là một hàm kích hoạt phi tuyến tính chuyển đổi tổ hợp tuyến tính của tất cả các tính hiệu đầu vào thành tính hiệu đầu ra. Hàm kích hoạt này đảm bảo tính chất phi tuyến tính cho tính toán của mạng nơron.

Một nơron là một đơn vị xử lý thông tin và là thành phần cơ bản của một mạng nơron.



Hình 1.4 Mô hình nơron nhân tạo

Các thành phần cơ bản của một nơron nhân tạo bao gồm:

♦ Tập các đầu vào: Là các tín hiệu vào (input signals) của nơron, các tín hiệu này thường được đưa vào dưới dạng một vector N chiều.

♦ Tập các liên kết: Mỗi liên kết được thể hiện bởi một trọng số (gọi là trọng số liên kết). Trọng số liên kết giữa tín hiệu vào thứ j với nơron k thường được kí hiệu là w_{kj}. Thông thường, các trọng số này được khởi tạo một cách ngẫu nhiên ở thời điểm khởi tạo mạng và được cập nhật liên tục trong quá trình học mạng.

♦ Bộ tổng (Summing function): Thường dùng để tính tổng của tích các đầu vào với trọng số liên kết của nó.

♦ Ngưỡng (còn gọi là một độ lệch - bias): Ngưỡng này thường được đưa vào như một thành phần của hàm kích hoạt.

♦ Hàm kích hoạt (Transfer function) : Hàm này được dùng để giới hạn phạm vi đầu ra của mỗi nơron. Nó nhận đầu vào là kết quả của hàm tổng và ngưỡng đã cho. Thông thường, phạm vi đầu ra của mỗi nơron được giới hạn

trong đoạn [0,1] hoặc [-1, 1]. Các hàm kích hoạt rất đa dạng, có thể là các hàm tuyến tính hoặc phi tuyến. Việc lựa chọn hàm kích hoạt nào là tuỳ thuộc vào từng bài toán và kinh nghiệm của người thiết kế mạng.

♦ Đầu ra: Là tín hiệu đầu ra của một nơron, với mỗi nơron sẽ có tối đa là một đầu ra.

Bảng 1.4.1 Một số hàm kích hoạt cơ bản trong mạng nơron

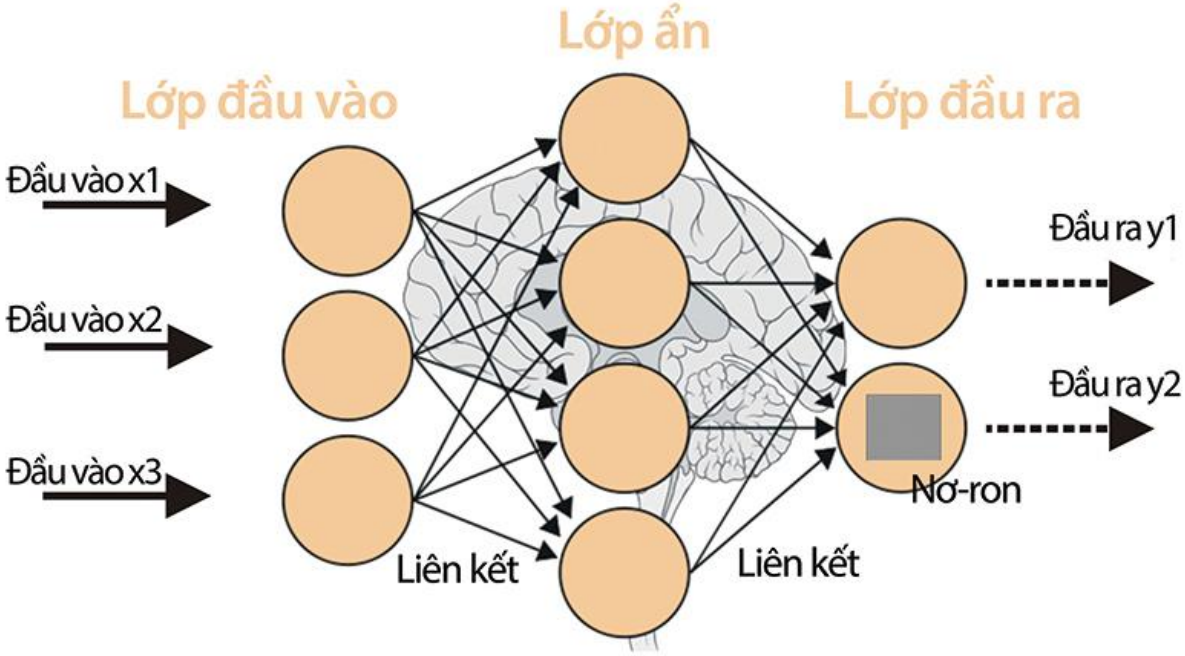
Tên hàm	Công thức
hardlim	a = 0 với n < 0 a = 1 với n ≥ 0
Hardlims (SGN)	a = -1 với n < 0 a = 1 với n ≥ 0
purelin	a = n
Satlin	a = 0 với n < 0 a = n với 0 ≤ n ≤ 1 a = 1 với n > 1
satlins	a = -1 với n < 0 a = n với 0 ≤ n ≤ 1 a = 1 với n > 1
tansig	$a = \frac{e^n - e^{-n}}{1 + e^{-n}}$
poslin	a = 0 với n < 0 a = n với n ≥ 0
compet	a = 1 với nơron có n lớn nhất a = 0 với các nơron còn lại
Logsig	$a = \frac{1}{1 + e^{-n}}$

2 Mạng nơron nhân tạo

Mạng nơron nhân tạo, Artificial Nơron Network (ANN) gọi tắt là mạng nơron, nơron network, là một mô hình xử lý thông tin phỏng theo cách thức xử lý thông tin của các hệ nơron sinh học. Nó được tạo lên từ một số lượng lớn các phần tử (gọi là phần tử xử lý hay nơron) kết nối với nhau thông qua các liên kết (gọi là trọng số liên kết) làm việc như một thể thống nhất để giải quyết một vấn đề cụ thể nào đó.

Một mạng nơron nhân tạo được cấu hình cho một ứng dụng cụ thể (nhận dạng mẫu, phân loại dữ liệu, ...) thông qua một quá trình học từ tập các mẫu huấn luyện. Về bản chất học chính là quá trình hiệu chỉnh trọng số liên kết giữa các nơron.

Là một hệ thống bao gồm nhiều phần tử xử lý đơn giản, giống như nơron thần kinh của não người, hoạt động song song và được nối với nhau bởi các liên kết nơron. Mỗi liên kết kèm theo một trọng số liên kết.



Hình 1.5 Mô hình đơn giản về một ANN

Mô hình một ANN trên gồm 3 lớp: lớp đầu vào (Input), lớp ẩn (Hidden) lớp đầu ra (Output). Mỗi nút trong lớp nhập nhận một giá trị của một biến độc lập và chuyển vào lớp mạng.

1.5 ĐẶC TRƯNG VỀ MẠNG NƠRON

1.5.1 Tính phi tuyến:

Một nơron có thể tính toán một cách tuyến tính hay phi tuyến tính. Một mạng nơron, cấu thành bởi sự kết nối các nơron phi tuyến tính thì tự nó sẽ có tính phi tuyến. Hơn nữa, điều đặc biệt là tính phi tuyến này được phân tán trên toàn mạng. Tính phi tuyến là một thuộc tính rất quan trọng, nhất là khi các cơ chế vật lý sinh ra các tín hiệu đầu vào (ví dụ tín hiệu tiếng nói) vốn là phi tuyến.

1.5.2 Tính chất tương ứng đầu vào đầu ra:

Mặc dù khái niệm "học" hay "huấn luyện" chưa được bàn đến nhưng để hiểu được mối quan hệ đầu vào – đầu ra của mạng nơron, chúng ta sẽ đề cập sơ qua về khái niệm này. Một mô hình học phổ biến được gọi là học với một người dạy hay học có giám sát liên quan đến thay đổi các trọng số liên kết của mạng nơron bằng việc áp dụng một tập hợp các mẫu tích lũy hay các ví dụ tích lũy. Mỗi một ví dụ tích lũy bao gồm một tín hiệu đầu vào và một đầu ra mong muốn tương ứng. Mạng nơron nhận một ví dụ lấy một cách ngẫu nhiên từ tập nói trên tại đầu vào của nó, và các trọng số liên kết của mạng được biến đổi sao cho có thể cực tiểu hóa sự sai khác giữa đầu ra mong muốn và đầu ra thực sự của mạng theo một tiêu chuẩn thống kê thích hợp. Sự tích lũy của mạng được lặp lại với nhiều ví dụ trong tập hợp cho tới khi mạng đạt tới mạng trạng thái ổn định mà ở đó không có một sự thay đổi đáng kể nào của các trọng số liên kết. Các ví dụ tích lũy được áp dụng trước có thể được áp dụng lại trong thời gian của phiên tích lũy nhưng theo một thứ tự khác. Như vậy mạng nơron học từ các ví dụ bằng cách xây dựng nên một tương ứng đầu vào-đầu ra cho vấn đề cần giải quyết.

1.5.3 Tính chất thích nghi.

Các mạng nơron có một khả năng mặc định là biến đổi các trọng số liên kết tùy theo sự thay đổi của môi trường xung quanh. Đặc biệt, một mạng nơron đã được tích lũy để hoạt động trong một môi trường xác định có thể được tích

lũy lại một cách dễ dàng khi có những thay đổi nhỏ của các điều kiện môi trường hoạt động.

1.5.4 Tính chất đưa ra lời giải có bằng chứng.

Trong ngữ cảnh phân loại mẫu, một mạng nơron có thể được thiết kế để đưa ra thông tin không chỉ về mẫu được phân loại, mà còn về sự tin cậy của quyết định đã được thực hiện. Thông tin này có thể được sử dụng để loại bỏ các mẫu mơ hồ hay nhập nhằng.

1.5.5 Tính chất chấp nhận sai xót.

Một mạng nơron, được cài đặt dưới dạng phần cứng, vốn có khả năng chấp nhận lỗi, hay khả năng tính toán thô, với ý nghĩa là tính năng của nó chỉ thoái hóa khi có những điều kiện hoạt động bất lợi. Ví dụ, nếu một nơron hay các liên kết kết nối của nó bị hỏng, việc nhận dạng lại một mẫu được lưu trữ sẽ suy giảm về chất lượng.

1.5.6 Khả năng cài đặt VLSI (Very-large-scale-intergrated).

Bản chất song song đồ sộ của một mạng nơron làm cho nó rất nhanh trong tính toán đối với một số công việc. Đặc tính này cũng tạo ra cho một mạng nơron khả năng phù hợp cho việc cài đặt sử dụng kỹ thuật Very-large-scale-intergrated (VLSI). Kỹ thuật này cho phép xây dựng những mạch cứng tính toán song song quy mô lớn. Chính vì vậy mà ưu điểm nổi bật của VLSI là mang lại những phương tiện hữu hiệu để có thể xử lý được những hành vi có độ phức tạp cao.

1.5.7 Tính chất đồng dạng trong phân tích và thiết kế.

Về cơ bản, các mạng nơron có tính chất chung như là các bộ xử lý thông tin. Chúng ta nêu ra điều này với cùng ý nghĩa cho tất cả các lĩnh vực có liên

quan tới việc ứng dụng mạng nơron. Đặc tính này thể hiện ở một số điểm như sau:

Các nơron, dưới dạng này hoặc dạng khác, biểu diễn một thành phần chung cho tất cả các mạng nơron.

Tính thống nhất này đem lại khả năng chia sẻ các lý thuyết và các thuật toán học trong nhiều ứng dụng khác nhau của mạng nơron.

Các mạng tổ hợp (modular) có thể được xây dựng thông qua một sự tích hợp các mô hình khác nhau.

1.6 PHÂN LOẠI MẠNG NƠRON NHÂN TẠO

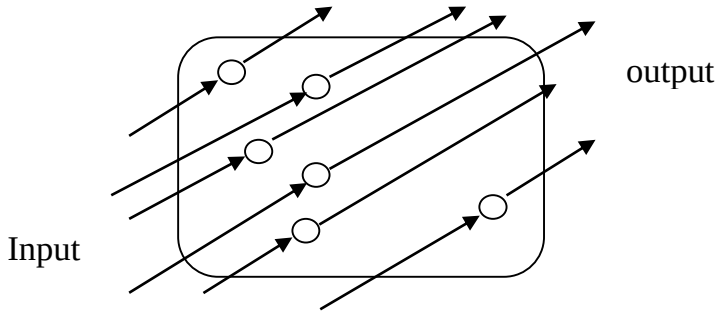
Mặc dù mỗi nơron đơn lẻ có thể thực hiện những chức năng xử lý thông tin nhất định, sức mạnh của tính toán nơron chủ yếu có được nhờ sự kết hợp các nơron trong một kiến trúc thống nhất. Một mạng nơron là một mô hình tính toán được xác định qua các tham số: kiểu nơron (như là các nút nếu ta coi cả mạng nơron là một đồ thị), kiến trúc kết nối (sự tổ chức kết nối giữa các nơron) và thuật toán học (thuật toán dùng để học cho mạng).

Về bản chất một mạng nơron có chức năng như là một hàm ánh xạ F: $X \rightarrow Y$, trong đó X là không gian trạng thái đầu vào (input state space) và Y là không gian trạng thái đầu ra (output state space) của mạng. Các mạng chỉ đơn giản là làm nhiệm vụ ánh xạ các vector đầu vào $x \in X$ sang các vector đầu ra $y \in Y$ thông qua "bộ lọc" các trọng số. Tức là $y = F(x) = s(W, x)$, trong đó W là ma trận trọng số liên kết. Hoạt động của mạng thường là các tính toán số thực trên các ma trận.

1.6.1 Các kiểu mô hình mạng nơron

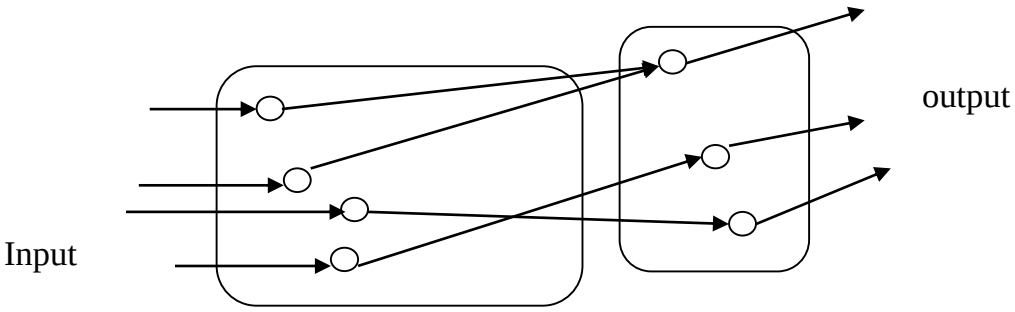
Cách thức kết nối các nơron trong mạng xác định kiến trúc của mạng. Các nơron trong mạng có thể kết nối đầy đủ có nghĩa là mỗi nơron đều được kết nối với tất cả các nơron khác, hoặc kết nối cục bộ chẳng hạn chỉ kết nối giữa các nơron trong các tầng khác nhau. Người ta chia ra hai loại kiến trúc mạng chính:

♦ Tự kết hợp (autoassociative): là mạng có các nơron đầu vào cũng là các nơron đầu ra. Mạng Hopfield là một kiểu mạng tự kết hợp.



Hình 1.6 Mạng tự kết hợp

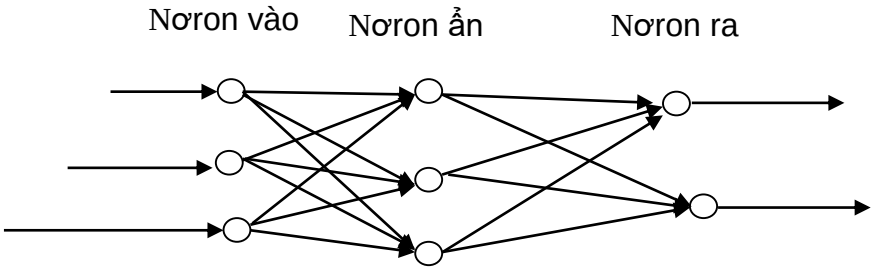
♦ Kết hợp khác kiểu (heteroassociative): là mạng có tập nơron đầu vào và đầu ra riêng biệt. Perceptron, các mạng Perceptron nhiều tầng (MLP: Multi Layer Perceptron), mạng Kohonen, … thuộc loại này.



Hình 1.7 Mạng kết hợp khác kiểu

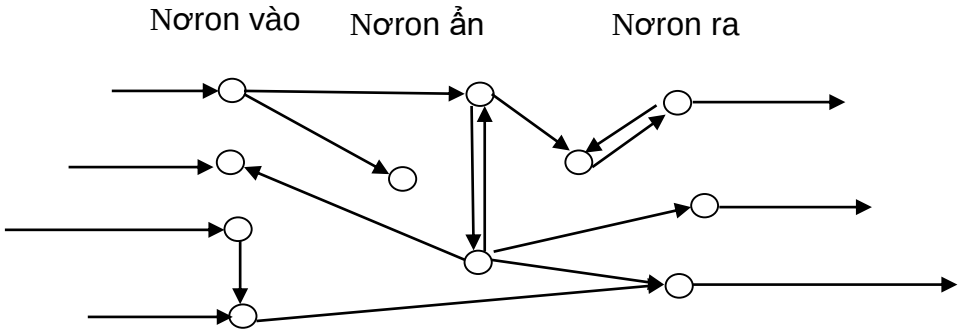
Ngoài ra tùy thuộc vào mạng có các kết nối ngược (feedback connections) từ các nơron đầu ra tới các nơron đầu vào hay không, người ta chia ra làm 2 loại kiến trúc mạng:

♦ Kiến trúc truyền thẳng (feedforward architechture): là kiểu kiến trúc mạng không có các kết nối ngược trở lại từ các nơron đầu ra về các nơron đầu vào; mạng không lưu lại các giá trị output trước và các trạng thái kích hoạt của nơron. Các mạng nơron truyền thẳng cho phép tín hiệu di chuyển theo một đường duy nhất; từ đầu vào tới đầu ra, đầu ra của một tầng bất kì sẽ không ảnh hưởng tới tầng đó. Các mạng kiểu Perceptron là mạng truyền thẳng.



Hình 1.8 Mạng truyền thẳng

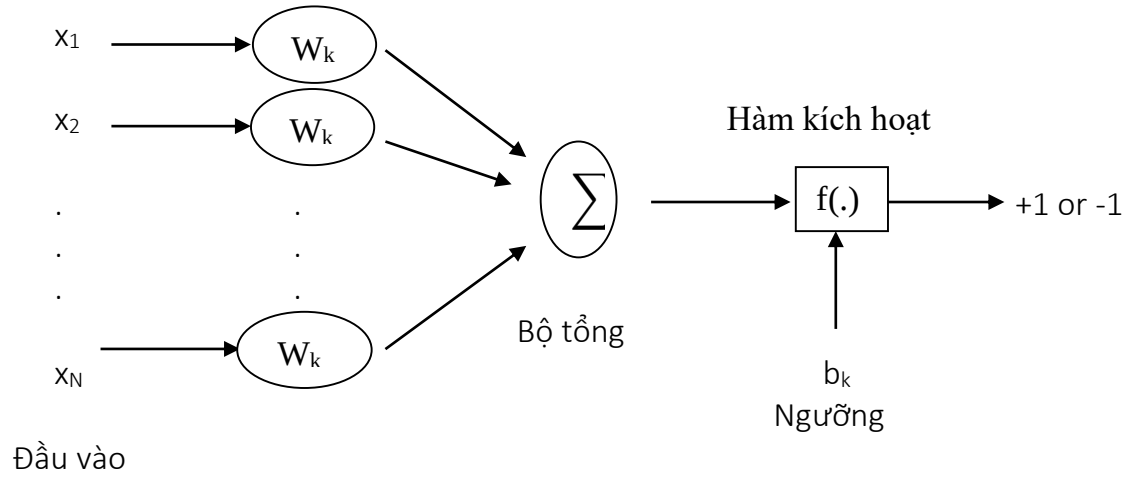
♦ Kiến trúc phản hồi (Feedback architecture): là kiểu kiến trúc mạng có các kết nối từ nơron đầu ra tới nơron đầu vào. Mạng lưu lại các trạng thái trước đó, và trạng thái tiếp theo không chỉ phụ thuộc vào các tín hiệu đầu vào mà còn phụ thuộc vào các trạng thái trước đó của mạng. Mạng Hopfield thuộc loại này.



Hình 1.9 Mạng phản hồi

1.6.2 Perceptron

Perceptron là mạng nơron đơn giản nhất, nó chỉ gồm một nơron, nhận đầu vào là vector có các thành phần là các số thực và đầu ra là một trong hai giá trị +1 hoặc -1.



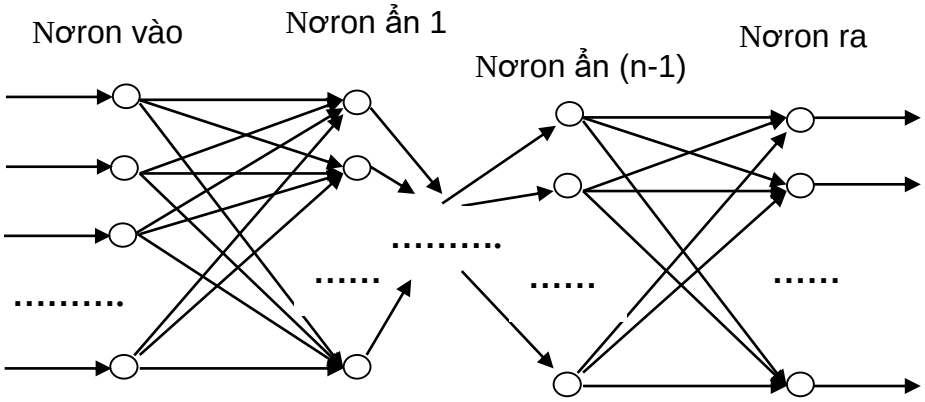
Hình 1.10 Perceptron

Đầu ra của mạng được xác định như sau: mạng lấy tổng có trọng số các thành phần của vector đầu vào, kết quả này cùng ngưỡng b được đưa vào hàm truyền (Perceptron dùng hàm Hard-limit làm hàm truyền) và kết quả của hàm truyền sẽ là đầu ra của mạng.

Perceptron cho phép phân loại chính xác trong trường hợp dữ liệu có thể phân chia tuyến tính (các mẫu nằm trên hai mặt đối diện của một siêu phẳng). Nó cũng phân loại đúng đầu ra các hàm AND, OR và các hàm có dạng đúng khi n trong m đầu vào của nó đúng ($n \leq m$). Nó không thể phân loại được đầu ra của hàm XOR.

1.6.3 Mạng nhiều tầng truyền thẳng (MLP):

Mô hình mạng nơron được sử dụng rộng rãi nhất là mô hình mạng nhiều tầng truyền thẳng (MLP: Multi Layer Perceptron). Một mạng MLP tổng quát là mạng có n ($n \geq 2$) tầng (thông thường tầng đầu vào không được tính đến): trong đó gồm một tầng đầu ra (tầng thứ n) và (n-1) tầng ẩn.



Hình 1.11 Mạng MLP tổng quát

Kiến trúc của một mạng MLP tổng quát có thể mô tả như sau:

♦ Đầu vào là các vector (x1, x2, ..., xp) trong không gian p chiều, đầu ra là các vector (y1, y2, ..., yq) trong không gian q chiều. Đối với các bài toán phân loại, p chính là kích thước của mẫu đầu vào, q chính là số lớp cần phân loại. Xét ví dụ trong bài toán nhận dạng chữ số: với mỗi mẫu ta lưu tọa độ (x,y) của 8 điểm trên chữ số đó, và nhiệm vụ của mạng là phân loại các mẫu này vào một trong 10 lớp tương ứng với 10 chữ số 0, 1, …, 9. Khi đó p là kích thước mẫu và bằng 8 x 2 = 16; q là số lớp và bằng 10.

♦ Mỗi nơron thuộc tầng sau liên kết với tất cả các nơron thuộc tầng liền trước nó.

♦ Đầu ra của nơron tầng trước là đầu vào của nơron thuộc tầng liền sau nó.

Hoạt động của mạng MLP như sau: tại tầng đầu vào các nơron nhận tín hiệu vào xử lý (tính tổng trọng số, gửi tới hàm truyền) rồi cho ra kết quả (là kết quả của hàm truyền); kết quả này sẽ được truyền tới các nơron thuộc tầng ẩn thứ nhất; các nơron tại đây tiếp nhận như là tín hiệu đầu vào, xử lý và gửi kết quả đến tầng ẩn thứ 2;…; quá trình tiếp tục cho đến khi các nơron thuộc tầng ra cho kết quả.

Một số kết quả đã được chứng minh:

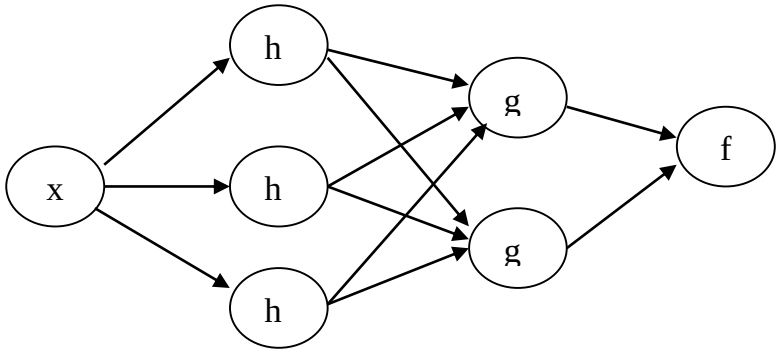
♦ Bất kì một hàm Boolean nào cũng có thể biểu diễn được bởi một mạng MLP 2 tầng trong đó các nơron sử dụng hàm truyền sigmoid.

♦ Tất cả các hàm liên tục đều có thể xấp xỉ bởi một mạng MLP 2 tầng sử dụng hàm truyền sigmoid cho các nơron tầng ẩn và hàm truyền tuyến tính cho các nơron tầng ra với sai số nhỏ tùy ý.

♦ Mọi hàm bất kỳ đều có thể xấp xỉ bởi một mạng MLP 3 tầng sử dụng hàm truyền sigmoid cho các nơron tầng ẩn và hàm truyền tuyến tính cho các nơron tầng ra.

1.7 XÂY DỰNG MẠNG NƠRON

Về cơ bản ta có thể hiểu mạng nơron là một đồ thị có hướng như hình 1.12. Trong đó các đỉnh của đồ thị là các nơron và các cạnh của đồ thị là các liên kết giữa các nơron.



Hình 1.12 Sơ đồ đồ thị có hướng đơn giản

Vì vậy để xây dựng một mạng nơron ta xây dựng một đồ thị có hướng: số đỉnh của đồ thị bằng số nơron trong mạng, giá trị của các cạnh chính là trọng số liên kết nơron.

1.8 HUẤN LUYỆN MẠNG NƠRON

Học là quá trình thay đổi hành vi của các vật theo một cách nào đó làm cho chúng có thể thực hiện tốt hơn trong tương lai.

Một mạng nơron được huyấn luyện sao cho với một tập các vector đầu vào X, mạng có khả năng tạo ra tập các vector đầu ra mong muốn Y của nó.

Tập X được sử dụng cho huấn luyện mạng được gọi là tập huấn luyện (training set). Các phần tử x thuộc X được gọi là các mẫu huấn luyện (training example). Quá trình huấn luyện bản chất là sự thay đổi các trọng số liên kết của mạng. Trong quá trình này, các trọng số của mạng sẽ hội tụ dần tới các giá trị sao cho với mỗi vector đầu vào x từ tập huấn luyện, mạng sẽ cho ra vector đầu ra y như mong muốn

Có ba phương pháp học phổ biến là học có giám sát , học không giám sát và học tăng cường.

1.8.1 Học có giám sát

Là quá trình học có sự tham gia giám sát của một "thầy giáo". Cũng giống như việc ta dạy một em nhỏ các chữ cái. Ta đưa ra một chữ "a" và bảo với em đó rằng đây là chữ "a". Việc này được thực hiện trên tất cả các mẫu chữ cái. Sau đó khi kiểm tra ta sẽ đưa ra một chữ cái bất kì (có thể viết hơi khác đi) và hỏi em đó đây là chữ gì?

Với học có giám sát, tập mẫu huấn luyện được cho dưới dạng

$D = \{(x,t) \mid (x,t) \in [IR^N \times R^K]\}$ trong đó: $x = (x_1, x_2, ..., x_N)$ là vector đặc trưng N chiều của mẫu huấn luyện và $t = (t_1, t_2, ..., t_K)$ là vector mục tiêu K chiều tương ứng, nhiệm vụ của thuật toán là phải thiết lập được một cách tính toán trên mạng như thế nào đó để sao cho với mỗi vector đặc trưng đầu vào thì sai số giữa giá trị đầu ra thực sự của mạng và giá trị mục tiêu tương ứng là nhỏ nhất. Chẳng hạn mạng có thể học để xấp xỉ một hàm $t = f(x)$ biểu diễn mối quan hệ trên tập các mẫu huấn luyện (x, t).

Như vậy với học có giám sát, số lớp cần phân loại đã được biết trước. Nhiệm vụ của thuật toán là phải xác định được một cách thức phân lớp sao cho với mỗi vector đầu vào sẽ được phân loại chính xác vào lớp của nó.

1.8.2 Học không giám sát

Là việc học không cần có bất kỳ một sự giám sát nào.

Trong bài toán học không giám sát, tập dữ liệu huấn luyện được cho dưới dạng: D = {(x_1, x_2, ..., x_N)}, với (x_1, x_2, ..., x_N), là vector đặc trưng của mẫu huấn luyện. Nhiệm vụ của thuật toán là phải phân chia tập dữ liệu D thành các nhóm con, mỗi nhóm chứa các vector đầu vào có đặc trưng giống nhau.

Như vậy với học không giám sát, số lớp phân loại chưa được biết trước, và tùy theo tiêu chuẩn đánh giá độ tương tự giữa các mẫu mà ta có thể có các lớp phân loại khác nhau.

1.8.3 Học tăng cường

Là sự tổ hợp của cả hai mô hình trên. Phương pháp này cụ thể như sau: với vector đầu vào, quan sát vector đầu ra do mạng tính được. Nếu kết quả được xem là "tốt" thì mạng sẽ được thưởng theo nghĩa tăng các trọng số kết nối lên; ngược lại mạng sẽ bị phạt, các trọng số kết nối không thích hợp sẽ được giảm xuống. Do đó học tăng cường là học theo nhà phê bình (critic), ngược với học có giám sát là học theo thầy giáo (teacher).

1.9 BIỂU DIỄN TRI THỨC CHO MẠNG NƠRON

Do cấu trúc một mạng nơron là vô cùng đa dạng, nên để có thể biểu diễn tri thức một cách có hiệu quả, người ta đưa ra bốn quy tắc chung sau:

Quy tắc 1: Các đầu vào tương tự các lớp tương tự cần phải luôn tạo ra những biểu diễn tương tự trong mạng, và như vậy nên được phân lớp thuộc về cùng loại. Trong tiêu chuẩn này, người ta thường sử dụng một số thước đo để xác định độ "tương tự" giữa các đầu vào (ví dụ khoảng cách euclide).

Quy tắc 2: Các phân tử mà có thể phân ra thành các lớp riêng biệt thì nên có những biểu diễn khác nhau đáng kể trong mạng.

Quy tắc 3: Nếu một đặc trưng nào đó đặc biệt quan trọng thì nên có một số lượng lớn nơron liên quan đến việc biểu diễn đặc trưng này trong mạng. Số lượng lớn các nơron bảo đảm mức độ chính xác cao trong việc thực hiện các quyết định và nâng cao khả năng chịu đựng các nơron hỏng.

Quy tắc 4: Thông tin ban đầu và các tính chất bất biến nên được đưa vào trong thiết kế ban đầu của mạng neural, và như vậy sẽ giảm bớt gánh nặng cho quá trình học. Quy tắc 4 đặc biệt quan trọng vì nếu chúng ta áp dụng nó một cách thích hợp sẽ dẫn đến khả năng tạo ra các mạng nơron với một kiến trúc chuyên biệt. Điều này thực sự được quan tâm do một số nguyên nhân sau:

1. Các mạng nơron thị giác và thính giác sinh học được biết là rất chuyên biệt.
2. Một mạng nơron với cầu trúc chuyên biệt thường có một số lượng nhỏ các tham số tự do phù hợp cho việc chỉnh lý hơn là một mạng kết nối đầy đủ. Như vậy mạng nơron chuyên biệt cần một tập hợp dữ liệu nhỏ hơn cho việc tích lũy; nó học sẽ nhanh hơn, và thường có khả năng tổng quát hóa tốt hơn.
3. Tốc độ chuyển thông tin qua một mạng chuyên biệt là nhanh hơn.
4. Giá của việc xây dựng một mạng chuyên biệt sẽ nhỏ hơn do kích thước nhỏ của nó so với mạng kết nối đầy đủ.

1.10 ỨNG DỤNG CỦA MẠNG NƠRON

Mạng nơron trong một vài năm trở lại đây đã được nhiều người quan tâm và đã áp dụng thành công trong nhiều lĩnh vực khác nhau, như tài chính, y tế, địa chất, vật lý. Thật vậy, bất cứ ở đâu có vấn đề về dự báo, phân loại và điều khiển, mạng nơron đề có thể ứng dụng được. Ví dụ như khả năng nhận dạng mặt người trong các hệ thống quản lý thông tin liên quan đến con người (quản lý nhân sự ở các công sở, doanh nghiệp; quản lý học sinh, sinh viên trong các trường trung học, đại học, cao đẳng…); các ngành khoa học hình sự, tội phạm; khoa học tướng số, tử vi…

Kết hợp chặt chẽ với logic mở, mạng nơron nhân tạo đã tạo nên cuộc cách mạng thực sự trong việc thông minh hóa và vạn năng hóa các bộ điều khiển kỹ thuật cao cho cả hiện nay và trong tương lai. Ví dụ như ứng dụng tự động điều khiển hệ thống lái tàu, hệ thống dự báo sự cố,…

1.11 TỔNG QUAN VỀ GIẢI THUẬT DI TRUYỀN

1.11.1 Lịch sử phát triển của Giải thuật di truyền

Giải thuật di truyền (GAs) là một trong những mô hình tính toán phổ biến và thành công nhất trong lĩnh vực tính toán thông minh. Cùng với các kỹ thuật tính toán thông minh khác như tính toán mờ (fuzzy computing), mạng Nơ-ron (neural networks), hệ đa tác tử (multiagent systems), trí tuệ bầy đàn (swarm intelligence), giải thuật di truyền ngày càng phát triển, được áp dụng rộng rãi trong các lĩnh vực của cuộc sống. Có thể nói, GAs đã bước đầu được áp dụng thành công trong các trường hợp, mà việc mô tả toán học cho bài toán gặp rất nhiều khó khăn.

Ví dụ: Các hệ thống phức hợp (complex systems) với các hàm mục tiêu ẩn và các mối ràng buộc phức tạp, các bài toán thiết kế với các hàm mục tiêu quá phức tạp không tuyến tính, hay các bài toán lập kế hoạch/lập lịch với không gian tìm kiếm NP-khó (NP-hard).

- *Khái niệm:*

Giải thuật di truyền (hay giải thuật tiến hóa nói chung) là một trong những phát triển quan trọng của những nhà nghiên cứu về tính toán ứng dụng cuối thế kỷ trước trong việc giải xấp xỉ các bài toán tối ưu toàn cục. Việc khai thác nguyên lý tiến hóa như là một định hướng heuristics đã giúp cho giải thuật di truyền giải quyết hiệu quả các bài toán tối ưu (với các lời giải chấp nhận được) mà không cần sử dụng các điều kiện truyền thống (liên tục hay khả vi) như là điều kiện tiên quyết. Một trong những đặc tính quan trọng của giải thuật di truyền là làm việc theo quần thể các giải pháp. Việc tìm kiếm bây giờ được thực hiện song song song trên nhiều điểm (multipoints).

Tuy nhiên, đây không phải là là thuật toán tìm kiếm đa điểm đơn thuần vì các điểm có tương tác với nhau theo nguyên lí tiến hóa tự nhiên. Trong ngữ cảnh sử dụng giải thuật di truyền, người ta có thể dùng khái niệm “cá thể” tương đương với khái niệm “giải pháp”. Các bước cơ bản của giải thuật di truyền được mô tả như sau:

• Bước 1: t=0; Khởi tạo P(t) = {x_1,x_2 ,. . . ,x_n }, với N là tổng số lượng cá thể.

• Bước 2: Tính giá trị các hàm mục tiêu cho P(t).

• Bước 3: Tạo bể lai ghép MP = se{P(t)} với se là toán tử lựa chọn.

• Bước 4: Xác định P'(t) = cr{MP}, với cr là toán tử lai ghép.

• Bước 5: Xác định P"(t) = mu{P'(t)}, với mu là toán tử đột biến.

• Bước 6: Tính giá trị các hàm mục tiêu cho P"(t)

• Bước 7: Xác định P(t+1) = P"(t) và đặt t = t+1

• Bước 8: Quay lại Bước 3, nếu điều kiện dừng chưa thỏa mãn.

- Biểu diễn giải pháp:

Đây là một trong những công việc quan trọng trong thiết kế giải thuật di truyền, quyết định việc áp dụng các toán tử tiến hóa. Một trong những biểu diễn truyền thống của GAs là biểu diễn nhị phân. Với phép biểu diễn này, giải pháp cho một bài toán được biểu diễn như là một vector bit, còn gọi là nhiễm sắc thể. Mỗi nhiễm sắc thể bao gồm nhiều gen, trong đó một gen đại diện cho một tham số thành phần của giải pháp. Một kiểu biểu diễn khác cũng thường dùng là biểu diễn số thực. Với phép biểu diễn này, các toán tử tiến hóa sẽ thực hiện trực tiếp trên các giá trị số thực (genes).

- Lựa chọn: Việc lựa chọn các cá thể được thực hiện khi cần một số cá thể để thực hiện sinh sản ra thế hệ sau. Mỗi cá thể có một giá trị thích nghi (fitness). Giá trị này được dùng để quyết định xem lựa chọn cá thể nào. Một số phương pháp lựa chọn thường dùng bao gồm:

+ Roulette wheel: Dựa trên xác suất (tỷ lệ thuận với giá trị hàm thích nghi) để lựa chọn cá thể.

+ Giao đấu (nhị phân): Chỉ định ngẫu nhiên 2 cá thể, sau đó chọn cá thể tốt hơn trong hai cá thể đó.

- Lai ghép: Toán tử lai ghép được áp dụng nhằm sinh ra các cá thể con mới từ các cá thể cha mẹ, thừa hưởng các đặc tính tốt từ cha mẹ. Trong ngữ cảnh tìm kiếm thì toán tử lai ghép thực hiện tìm kiếm xung quanh khu vực của các giải pháp biểu diễn bởi các cá thể cha mẹ.

- Đột biến: Tương tự như lai ghép, đột biến cũng là toán tử mô phỏng hiện tượng đột biến trong sinh học. Kết quả của đột biến thường sinh ra các cá thể mới khác biệt so với cá thể cha mẹ. Trong ngữ cảnh tìm kiếm, toán tử đột biến nhằm đưa quá trình tìm kiếm ra khỏi khu vực cục bộ.

1.11.2 Nhiễm sắc thể

Các GAs cũng như các thuật toán tiến hoá khác hình thành dựa trên quan niệm cho rằng quá trình tiến hoá tự nhiên là quá trình hợp lý, hoàn hảo. Tự nó đã mang tính tối ưu. Quan điểm trên như một tiên đề, không chứng minh, nhưng phù hợp với thực tế khách quan.

Mục tiêu nghiên cứu của GAs có thể được khái quát như sau: Trừu tượng hoá và mô phỏng quá trình thích nghi trong hệ thống tự nhiên. Thiết kế phần mềm, chương trình mô phỏng, nhằm duy trì các cơ chế quan trọng của hệ thống tự nhiên. Giải thuật di truyền sử dụng một số thuật ngữ của ngành di truyền học như: nhiễm sắc thể, quần thể (Population), Gen.... Nhiễm sắc thể được tạo thành từ các Gen (được biểu diễn của một chuỗi tuyến tính). Mỗi Gen mang một số đặc trưng và có vị trí nhất định trong nhiễm sắc thể. Mỗi nhiễm sắc thể sẽ biểu diễn một lời giải của bài toán.

Các toán tử di truyền, Toán tử sinh sản gồm hai quá trình:

Quá trình sinh sản (phép tái sinh), quá trình chọn lọc (phép chọn). Phép tái sinh là quá trình các nhiễm sắc thể được sao chép trên cơ sở độ thích nghi. Độ thích nghi là một hàm được gán giá trị thực, tương ứng với mỗi nhiễm sắc thể trong quần thể. Quá trình này, được mô tả như sau:

Xác định độ thích nghi của từng nhiễm sắc thể trong quần thể ở thế hệ thứ t, lập bảng cộng dồn các giá trị thích nghi (theo thứ tự gán cho từng nhiễm sắc thể). Giả sử, quần thể có n cá thể. Gọi độ thích nghi của nhiễm sắc thể i tương ứng là fi tổng cộng dồn thứ i là fti được xác định bởi:

$$\oint_{ti} = \sum_{j=1}^{i} \oint j$$

Gọi Fn là tổng độ thích nghi của toàn quần thể. Chọn một số ngẫu nhiên f trong khoảng từ 0 tới Fn. Chọn cá thể thứ k đầu tiên thoả mãn f ≥ ftk đưa vào quần thể mới.

+ Phép chọn: là quá trình loại bỏ các nhiễm sắc thể kém thích nghi trong quần thể. Quá trình này được mô tả như sau:

- Sắp xếp quần thể theo thứ tự mức độ thích nghi giảm dần.
- Loại bỏ các nhiễm sắc thể ở cuối dãy. Giữ lại n cá thể tốt nhất

Toán tử ghép chéo: Ghép chéo là quá trình tạo nhiễm sắc thể mới trên cơ sở các nhiễm sắc thể cha-mẹ bằng cách ghép một đoạn trên nhiễm sắc thể cha-mẹ với nhau. Toán tử ghép chéo được gán với một xác suất p c.

Quá trình được mô tả như sau:

Chọn ngẫu nhiên một cặp nhiễm sắc thể (cha-mẹ) trong quần thể. Giả sử, nhiễm sắc thể cha-mẹ có cùng độ dài m. Tạo một số ngẫu nhiên trong khoảng từ 1 tới m-1 (gọi là điểm ghép chéo).

Điểm ghép chéo chia nhiễm sắc thể cha-mẹ thành hai chuỗi con có độ dài m1, m2. Hai chuỗi con mới được tạo thành là: m11+ m22 và m21+m12.

Đưa hai nhiễm sắc thể mới vào quần thể.

Toán tử đột biến: Đột biến là hiện tượng nhiễm sắc thể con mang một số đặc tính không có trong mã di truyền của cha-mẹ.

• Chọn ngẫu nhiên một nhiễm sắc thể trong quần thể;

• Tạo một số ngẫu nhiên k trong khoảng từ 1 tới m,1 ≤ k ≤ m;

• Thay đổi bit thứ k. Đưa nhiễm sắc thể này vào quần thể để tham gia quá trình tiến hoá ở thế hệ tiếp theo.

1.11.3 Cơ sở toán học của giải thuật di truyền

Cơ sở lý thuyết của giải thuật di truyền dựa trên biểu diễn chuỗi nhị phân và lý thuyết sơ đồ. Một sơ đồ là một chuỗi, có chiều dài bằng chuỗi nhiễm sắc thể. Các thành phần của nó có thể nhận một trong các giá trị trong tập ký tự biểu diễn Gen hoặc một ký tự đại diện "*".

Sơ đồ biểu diễn không gian con trong không gian tìm kiếm. Không gian con này là tập tất cả các chuỗi trong không gian tìm kiếm mà với mọi vị trí

trong chuỗi, giá trị của Gen trùng với giá trị của sơ đồ; kí tự đại diện "*" có thể trùng khớp với bất kỳ ký tự biểu diễn nào.

Sơ đồ (* 1 0 1 0) sẽ khớp với 2 chuỗi: (1 1 0 1 0) và (0 1 0 1 0).

Như vậy, sơ đồ (1 1 0 1 0) và (0 1 0 1 0) chỉ khớp với chuỗi chính nó, còn sơ đồ (* * ** *) khớp với tất cả các sơ đồ có độ dài là 5.

Với sơ đồ cụ thể có tương ứng 2r chuỗi, r: là số ký tự đại diện "*" có trong sơ đồ; ngược lại, một chuỗi có chiều dài m sẽ khớp với 2m sơ đồ.

Một chuỗi có chiều dài m, sẽ có tối đa 3m sơ đồ. Trong một quần thể dân số kích thước n, có thể có tương ứng từ 2m đến nx2m sơ đồ khác nhau.

Thuộc tính của sơ đồ:

Các sơ đồ khác nhau có đặc trưng khác nhau. Các đặc trưng này thể hiện qua hai thuộc tính quan trọng: bậc và chiều dài xác định.

Bậc của sơ đồ S (ký hiệu o(S)) là tổng số vị trí 0, 1 có trong sơ đồ. Đây là các vị trí cố định (không phải vị trí của các ký tự đại diện) trong sơ đồ. Bậc có thể xác định bằng cách lấy chiều dài của chuỗi trừ đi số ký tự đại diện.

Trong sơ đồ S = (* * 1 0 * 1 *) có bậc o(S) = 7 - 4 = 3;

Chiều dài xác định của sơ đồ S (ký hiệu là δ(S)) là khoảng cách giữa 2 vị trí cố định ở đầu và cuối. Chiều dài của sơ đồ xác định độ nén thông tin chứa trong sơ đồ đó. Trong ví dụ trên δ(S)= 6-3 =3. Như vậy, nếu sơ đồ chỉ có một vị trí cố định thì chiều dài xác định của sơ đồ sẽ bằng 0.

Chiều dài của sơ đồ giúp ta tính xác suất tồn tại của sơ đồ do ảnh hưởng của ghép chéo.

Đặc điểm hội tụ của giải thuật di truyền khi áp dụng giải thuật GAs cho các vấn đề thực tế thường rất khó khăn.

Lý do:

• Cách biểu diễn nhiễm sắc thể có thể tạo ra không tìm kiếm khác với không gian thực của bài toán;

• Số bước lặp, khi cài đặt thường không xác định trước;

• Kích thước quần thể thường có giới hạn.

Trong một số trường hợp, GAs không thể tìm được lời giải tối ưu. Lý do, GAs hội tụ sớm về lời giải tối ưu cục bộ. Hội tụ sớm là vấn đề của giải

thuật di truyền cũng như các giải thuật tối ưu khác. Nếu hội tụ xảy ra quá nhanh thì các thông tin đáng tin cậy đang phát triển trong quần thể thường bị bỏ qua. Nguyên nhân của sự hội tụ sớm liên quan tới hai vấn đề:

• Quy mô và loại sai số do cơ chế tạo mẫu;

• Bản chất của hàm mục tiêu

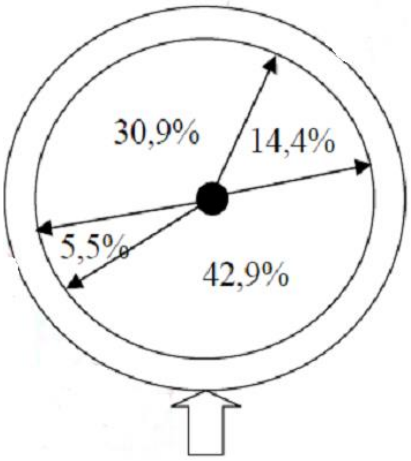
Cơ chế tạo mẫu: Có hai vấn đề quan trọng trong tiến trình tiến hoá của giải thuật di truyền là:

+ Tính đa dạng của quần thể và áp lực chọn lọc. Hai yếu tố này liên quan mật thiết với nhau: khi tăng áp lực chọn lọc thì tính đa dạng của quần thể sẽ giảm và ngược lại. Nói cách khác, áp lực hội tụ mạnh sẽ dẫn tới sự hội tụ sớm của giải thuật. Nhưng nếu áp lực chọn lọc yếu có thể làm cho tìm kiếm thành vô hiệu. Như vậy, cần thoả hiệp hai vấn đề. Hiện nay, các phương pháp đưa ra đều có khuynh hướng để đạt tới mục đích này.

Năm 1975 DeJong đã xem xét một số biến thể của chọn lọc đơn giản bằng cách đưa ra: mô hình phát triển ưu tú, mô hình giá trị mong đợi và mô hình nhân tố tập trung.

Năm 1981 Brindle xem xét một số biến thể khác như: tạo mẫu tất định, tạo mẫu hỗn loạn, tạo mẫu hỗn loạn phần dư không thay thế, đấu tranh hỗn loạn, tạo mẫu hỗn loạn phần dư có thay thế.

Năm 1987 Baker nghiên cứu phương pháp tạo mẫu không gian hỗn loạn. Phương pháp này dùng cách "quay" bánh xe định tỷ lệ trước để thực hiện chọn lọc. Bánh xe này được thiết kế theo chuẩn, quay với số khoảng chia đều theo kích thước quần thể.



Hình 1.13 Bánh xe Banker

Người ta thực hiện việc sinh sản bằng cách quay bánh xe Roulette với số lần bằng số nhiễm sắc thể trên bánh xe Roulette. Đối với bài toán này số lần quay bánh xe Roulette là 4. Nhiễm sắc thể 1 có giá trị thích nghi là 169, tương ứng 14,4 % tổng độ thích nghi. Như vậy, nhiễm sắc thể 1 chiếm 14.4% trên bánh xe Roulette. Mỗi lần quay nhiễm sắc thể 1 sẽ chiếm khe với giá trị 0,144.

Khi yêu cầu sinh ra 1 thế hệ mới, một vòng quay của bánh xe Roulette được đánh trọng số phù hợp sẽ chọn ra một cá thể để sinh sản. Bằng cách này, những nhiễm sắc thể có độ thích nghi cao sẽ có cơ hội được chọn lớn. Như vậy, sẽ có 1 số lượng con cháu lớn trong các thế hệ kế tiếp.

Hàm mục tiêu:

Cứ sau mỗi thế hệ được hình thành, chúng ta cần tính lại độ thích nghi cho từng cá thể để chuẩn bị cho một thế hệ mới. Do số lượng các cá thể tăng lên, độ thích nghi giữa các cá thể không có sự chêch lệch đáng kể.

Do đó, các cá thể có độ thích nghi cao chưa hẳn chiếm ưu thế trong thế hệ tiếp theo.

Vì vậy, cần ấn định tỷ lệ đối với hàm thích nghi nhằm tăng khả năng cho các nhiễm sắc thể đạt độ thích nghi cao. Có 2 cơ chế định tỷ lệ như sau:

1) Định tỷ lệ tuyến tính: Độ thích nghi được xác định theo công thức:

$$f_i' = \mathrm{a} * f_i \quad + b$$

Cần chọn các tham số a, b sao cho độ thích nghi trung bình được ánh xạ vào chính nó. Tăng độ thích nghi tốt nhất bằng cách nhân nó với độ thích nghi trung bình. Cơ chế này có thể tạo ra các giá trị âm cần xử lý riêng. Ngoài ra, các tham số a, b thường gắn với đời sống quần thể và không phụ thuộc vào bài toán.

2) Phép cắt Sigma:

Phương pháp này được thiết kế vừa để cải tiến phương pháp định tỷ lệ tuyến tính vừa để xử lý các giá trị âm, vừa kết hợp thông tin mà bài toán phụ thuộc. Ở đây, độ thích nghi mới được tính theo công thức:

$$f_i' = f_i + (\overline{f} - c * \sigma)$$

Trong đó c là một số nguyên nhỏ (thường lấy giá trị từ 1 tới 5); σ là độ lệch chuẩn của quần thể. Với giá trị âm thì f' được thiết lập bằng 0.

1.12 TÌM HIỂU VỀ GIẢI THUẬT DI TRUYỀN

Giải thuật di truyền (GAs) trong lĩnh vực tin học là một trong những giải thuật thú vị, bởi vì nó mô phỏng quy luật đấu tranh sinh tồn của tự nhiên và cũng là một giải thuật vô cùng hiệu quả đối với các bài toán tối ưu.

Giải thuật di truyền là một kỹ thuật của khoa học máy tính, nhằm tìm kiếm giải pháp thích hợp cho các bài toàn tối ưu tổ hợp. Giải thuật di truyền là một phân ngành của giải thuật tiến hóa vận dụng các nguyên lý của tiến hóa như di truyền, đột biến, chọn lọc tự nhiên và trao đổi chéo.

Giải thuật di truyền cũng như các thuật toán tiến hoá, đều được hình thành dựa trên một quan niệm được coi là một tiên đề phù hợp với thực tế khách quan. Đó là quan niệm "Quá trình tiến hoá tự nhiên là quá trình hoàn hảo nhất, hợp lý nhất và tự nó đã mang tính tối ưu". Quá trình tiến hoá thể hiện tính tối ưu ở chỗ thế hệ sau bao giờ cũng tốt hơn thế hệ trước. Ngày nay, giải thuật di truyền được dùng phổ biến trong một số ngành như tin sinh học, khoa học máy tính, trí tuệ nhân tạo, tài chính và một số ngành khác.

- *Đặc trưng của giải thuật di truyền*

Giải thuật di truyền là kỹ thuật chung, giúp giải quyết vấn đề bằng cách mô phỏng sự tiến hóa của con người hay của sinh vật nói chung (dựa trên thuyết tiến hóa muôn loài của Darwin), trong điều kiện quy định sẵn của môi trường. Mục tiêu của Giải thuật di truyền không nhằm đưa ra lời giải chính xác tối ưu mà là đưa ra lời giải tương đối tối ưu. Một cá thể trong Giải thuật di truyền sẽ biểu diễn một giải pháp của bài toán.

Tuy nhiên, không giống với trong tự nhiên là một cá thể có nhiều nhiễm sắc thể (NST) mà để giới hạn trong GAs, ta quan niệm một cá thể có một NST. Do đó, khái niệm cá thể và NST trong GAs coi như là tương đương. Một NST được tạo thành từ nhiều Gen, mỗi Gen có thể có các giá trị khác nhau để quy định một tình trạng nào đó. Trong GAs, một Gen được coi như một phần tử trong chuỗi NST. Một tập hợp các cá thể có cùng một số đặc điểm nào đấy được gọi là quần thể. Trong thuật giải di truyền, ta quan niệm quần thể là một tập các lời giải của một bài toán.

CHƯƠNG 2:ỨNG DỤNG MẠNG NƠRON TRONG BẢO MẬT

2.1 ĐỊNH NGHĨA VỀ NEURAL CRYPTOGRAPHY

Mạng nơron được biết đến với khả năng tìm kiếm những giải pháp giải quyết cho một vấn đề nhất định. Tính năng này được sử dụng rộng rãi trong các ứng dụng thuộc lĩnh vực mật mã học. Song song đó, mạng nơron cũng cung cấp một tính năng tiếp cận mới để nhằm tấn công các thuật toán mã hóa dựa trên nguyên tắc mọi chức năng đều có thể được tạo bởi một mạng nơron nhất định, đây là công cụ mạnh mẽ đã được chứng minh là có thể sử dụng để tìm hàm ngược của bất kỳ thuật toán mật mã học.

Những ý tưởng về việc hỗ trợ học luật, tự học và các hành vi ngẫu nhiên của mạng nơron hoặc các thuật toán tương tự có thể được sử dụng cho cách khía cạnh khác nhau của mật mã học, như mã hóa khóa công khai, giải quyết vấn đề phân phối khóa bằng cách sử dụng mạng nơron đồng bộ hóa lẫn nhau, băm hoặc hệ số giả ngẫu nhiên.

Hai cái tên được sử dụng để thiết kế trong lĩnh vực nghiên cứu này là : Neuro-Cryptography và Neural Cryptography.

Phương pháp này được biết đến lần đầu tiên là từ năm 1995.

2.2 CÁC NGHIÊN CỨU NEURAL CRYPTOGRAPHY

Năm 1995, Sebastien Dourlens áp dụng mạng nơron cryptanalyze DES bằng cách cho phép các mạng tự học để làm thế nào để có thể đảo ngược bảng S của DES. Thử nghiệm cho thấy khoảng 50% các bit quan trọng có thể được tìm thấy, cho phép hoàn thành việc tìm được khóa trong một thời gian ngắn. Ứng dụng phần cứng với nhiều bộ điều khiển đã được đề xuất để dễ dàng tạo ra mạng nơron đa lớp trong phần cứng.

Một ví dụ về một giao thức mã hóa công khai được đưa ra bởi Khalil Shihab. Ông mô tả các chương trình giải mã và tạo ra khóa công khai dựa trên một mạng nơron lan truyền ngược. Các chương trình mã hóa và quá trình tạo khóa riêng dựa trên đại số Boolean. Kỹ thuật này có ưu điểm là thời gian ngắn

và độ phức tạp nhỏ. Một bất lợi đặt trưng của các thuật toán lan truyền ngược: vì bộ đào tạo rất lớn, nên giai đoạn học tập của một mạng lưới nơron rất dài.[11]

2.3 MỘT SỐ ỨNG DỤNG CỦA NEURAL CRYPTOGRAPHY

2.3.1 Ứng dụng mạng nơron trong giám sát an toàn thông tin

Mạng nơron được ứng dụng nhiều trong giám sát an toàn thông tin bởi những ưu điểm của nó như khả năng cập nhật thường xuyên dấu hiệu của các cuộc tấn công mới hay chưa tồn tại trong hệ thống.

Phần lớn hoạt động của các hệ thống phát hiện tấn công trong giám sát an toàn thông tin chủ yếu dựa trên cơ sở dữ liệu (CSDL) các dấu hiệu và quy luật để phân tích các dữ liệu đầu vào sau đó đưa ra kết luận có hay không có tấn công. Để việc phát hiện tấn công đạt hiệu quả cao thì CSDL này cần phải thường xuyên được cập nhật (được thực hiện bằng phương pháp thủ công hoặc tự động trong khoảng thời gian nhất định).

Khi cuộc tấn công có dấu hiệu và quy luật khác với các dấu hiệu và quy luật trong CSDL thì tấn công đó sẽ không được phát hiện. Vì lúc này các CSDL chưa được cập nhật dấu hiệu của các kiểu tấn công này. Do hệ thống phát hiện tấn công thông thường không phải lúc nào cũng có khả năng nhận dạng được mọi cuộc tấn công nên cần một hệ thống có khả năng cập nhật thường xuyên dấu hiệu của các cuộc tấn công mới hay chưa có trong hệ thống. Mạng nơron hay mạng nơron nhân tạo (Artifical Neural network-ANN) là một giải pháp có thể đáp ứng được yêu cầu này.

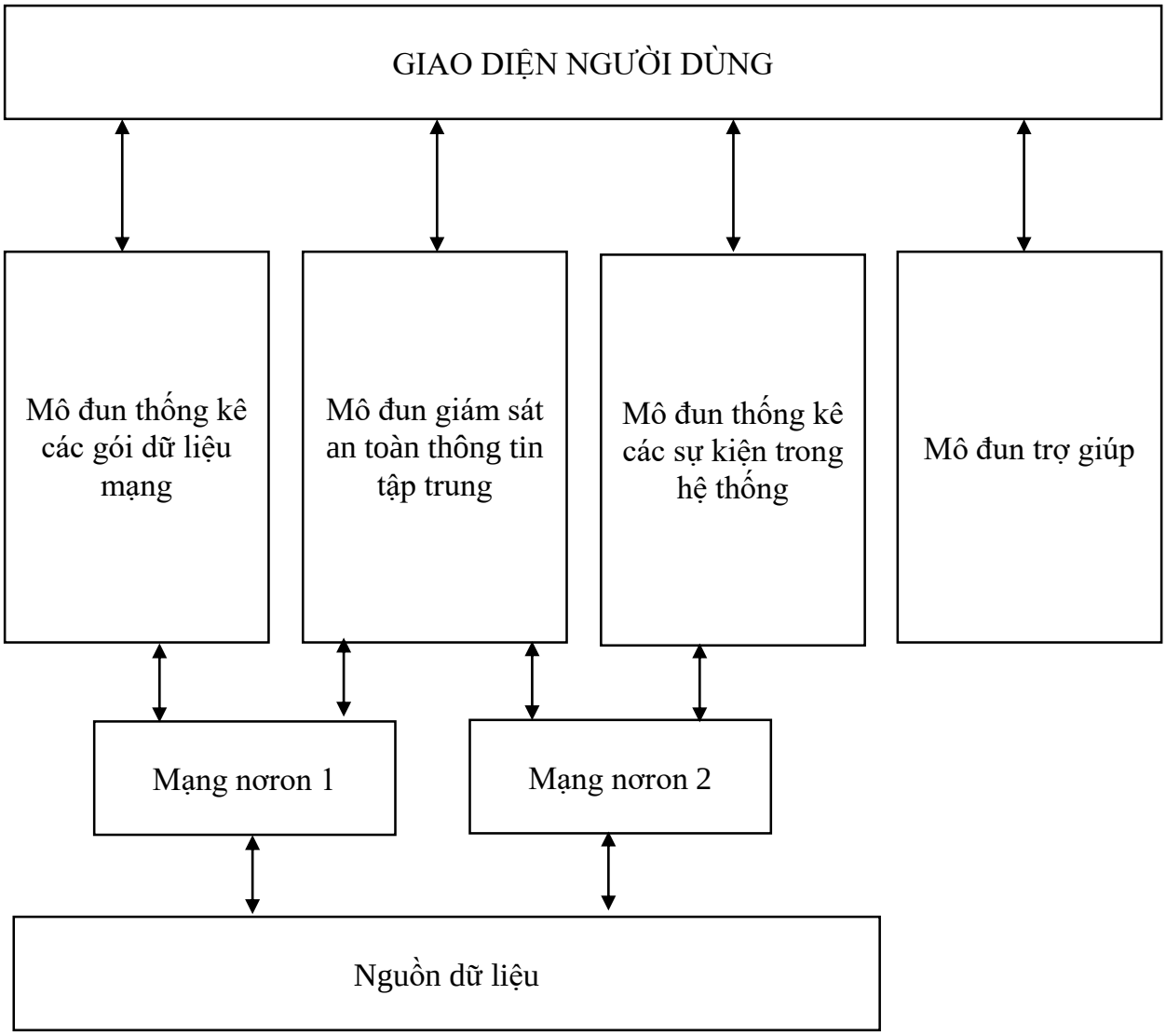
Mục tiêu chính của mạng nơron trong hệ thống phát hiện tấn công là chuyển đổi một tập cụ thể những dữ liệu đầu vào thành một tập cụ thể những dữ liệu đầu ra, có nghĩa là, dựa vào các dữ liệu đầu vào về các gói tin trong mạng hoặc các sự kiện trong hệ thống, mạng nơron sẽ phải đưa ra kết luận về một cuộc tấn công (để giải quyết bài toán phân loại). Hiệu quả giải quyết bài toán phụ thuộc vào sự lựa chọn kiến trúc mạng nơron và việc huấn luyện mạng nơron. Việc lựa chọn kiến trúc mạng nơron tối ưu là tìm ra được một mạng

nơron có khả năng giải quyết bài toán đặt ra với một mục tiêu có sai số tối thiểu.

Việc huấn luyện mạng nơron thủ công sẽ tốn thời gian và công sức, vì vậy hệ thống phát hiện tấn công này đã được tích hợp với phần mềm Statistica Neural Networks để huấn luyện mạng nơron (gọi là huấn luyện mạng nơron tự động).

Việc huấn luyện mạng nơron với phần mềm Statistica Neural Networks được dựa trên các mẫu đào tạo, trong đó mỗi bộ đầu dữ liệu đầu vào sẽ có một câu trả lời đúng (tương ứng một dữ liệu đầu ra xác định).

Cấu trúc tổng quát của hệ thống phát hiện tấn công được trình bày trong hình dưới đây:



Hình 2.1 Cấu trúc tổng quát của hệ thống phát hiện tấn công

Theo sơ đồ trên, môđun nguồn dữ liệu sẽ tạo vector dữ liệu đầu vào dựa trên phần mềm Snort và nhật ký an ninh của Windows. Dữ liệu đầu vào cho mạng nơron thứ nhất là thông tin về các gói tin trong mạng (thời gian, địa chỉ IP nguồn và đích, kiểu giao thức, thời gian sống của gói tin (time to live), độ dài tiêu đề, độ dài dữ liệu). Mạng nơron thứ nhất chịu trách nhiệm giám sát tấn công mạng. Dữ liệu đầu vào cho mạng neural thứ hai là các thông tin về sự kiện trong hệ thống (kiểu sự kiện, ID sự kiện, ngày, thời gian, kiểu sự kiện). Mạng nơron thứ 2 chịu trách nhiệm giám sát các sự kiện trong hệ thống.

Môđun thống kê các gói dữ liệu mạng được sử dụng để tạo mẫu huấn luyện. Các mẫu này sẽ được sử dụng để tạo ra một mạng nơron có khả năng phân tích dữ liệu đầu vào và thực hiện giám sát trong mạng. Môđun này cung cấp cho việc phân tích một số lượng tương đối của các cuộc tấn công mạng.

Môđun thống kê các sự kiện trong hệ thống cho phép phân tích theo biểu đồ động về sự xuất hiện của bất kỳ mối đe dọa nào trong bất kỳ khoảng thời gian nào, môđun này được sử dụng làm mẫu để huấn luyện mạng nơron thứ hai có khả năng giám sát các sự kiện trong hệ thống.

Môđun giám sát an toàn thông tin tập trung sẽ thu các gói tin mạng theo thời gian thực và môđun này đưa các thông tin đó đến đầu vào của mạng nơron thứ nhất. Mạng nơron thứ nhất này sẽ đưa ra kết luận về tấn công dựa trên các thông tin này. Tương tự như vậy, môđun này cũng sẽ thu các sự kiện trong hệ thống theo thời gian thực và đưa các thông tin này vào đầu vào của mạng nơron thứ hai. Mạng nơron thứ hai này sẽ xác định mức độ nguy hiểm của các sự kiện.

Thực tế cho thấy, việc ứng dụng mạng nơron vào trong hệ thống phát hiện tấn công cho phép giúp tăng hiệu quả giám sát, do khả năng tự học của mạng nơron giúp phát hiện các tấn công có ít dấu hiệu nhận biết giống với các dấu hiệu tấn công của CSDL trong hệ thống giám sát .

2.3.2 Phát hiện xâm nhập dựa trên mạng Nơron

Hệ thống phát hiện xâm nhập trái phép phát hiện sự truy cập và khai thác hệ thống máy tính bất hợp pháp thông qua việc giám sát các hoạt động bất thường của người sử dụng, dựa trên việc thiết lập các luật (rules) hoặc sử dụng các lệnh dự đoán trực tuyến.

Tuy nhiên, các biện pháp này tỏ ra không hiệu quả, khá tốn kém, độ tin cậy không cao và không có khả năng tự cập nhật để phát hiện xâm nhập mới. Việc ứng dụng mạng nơron, một kỹ thuật học máy trong các hệ thống phát hiện xâm nhập là hướng tiếp cận đã khắc phục được các hạn chế trên và đang được quan tâm nghiên cứu.

Những năm gần đây vấn đề an ninh mạng đã trở nên cấp thiết và tác động lớn tới hiệu quả hoạt động của các mạng máy tính hiện đại. Một trong những biện pháp bảo đảm an toàn cho các hệ thống mạng là Hệ thống phát hiện xâm nhập trái phép (Intrustion Detector System - IDS). Tuy nhiên, các biện pháp này tỏ ra không hiệu quả khá tốn kém, độ tin cậy không cao và không có khả năng tự cập nhật để phát hiện xâm nhập mới. Một hướng tiếp cận khác đã khắc phục được các hạn chế trên và ngày càng thể hiện tính ưu việt là ứng dụng kỹ thuật học máy (machine learning), với nhiều phương pháp khác nhau. Trong đó có ứng dụng mạng nơron, một kỹ thuật học máy trong các hệ thống phát hiện xâm nhập. Vấn đề này đã đã được nghiên cứu, đề xuất từ những năm 1990 và gần đây có nhiều kết quả nghiên cứu được công bố trên toàn thế giới.

- *Hệ thống NNID*

Từ năm 1998, ba nhà khoa học Jake Ryan, Meng-Jang Lin, Risto Miikkulainen đã đề xuất giải pháp xây dựng hệ thống phát hiện xâm nhập dựa trên mạng nơron (Neural Network Intrusion Detector - NNID). NNID sử dụng giải thuật học lan truyền ngược (backpropagation), hoạt động trên môi trường UNIX và là IDS không trực tuyến. Tại cuối mỗi ngày làm việc, người quản trị hệ thống sẽ chạy NNID để kiểm tra phiên đăng nhập của người dùng có phù hợp với mẫu hoạt động thông thường của họ hay không. Nếu hoạt động của người dùng không phù hợp với mẫu hoạt động thông thường thì sẽ đưa ra cảnh báo về một sự xâm nhập tới hệ thống.

Các mẫu hoạt động thông thường của người sử dụng hợp pháp được gọi là hồ sơ người dùng. Để tạo ra hồ sơ người dùng, hệ thống sẽ sử dụng phương pháp thống kê, nhằm thống kê tần suất sử dụng các câu lệnh trong hệ thống của mỗi người dùng, từ đó tạo nên các biểu đồ sử dụng lệnh của từng người dùng, việc học hồ sơ người dùng cũng được thực hiện thông qua các biểu đồ này. Dữ liệu để sử dụng cho việc thống kê được lấy từ các bản ghi nhật ký (log record) của hệ thống, với mục đích ghi lại toàn bộ hành vi của mỗi người dùng trong

phiên đăng nhập của họ. Các bản ghi này không làm ảnh hưởng tới quyền riêng tư của người dùng khi tham gia vào hệ thống. Tần suất sử dụng các câu lệnh trong hệ thống hay thói quen của mỗi người dùng khi sử dụng các ứng dụng trong hệ thống được gọi là dấu vết người dùng (a "print" of the user).

Hệ thống NNID gồm 3 tầng chuẩn (tầng đầu vào – input layer, tầng ẩn – hidden layer và tầng đầu ra – output layer). Tầng đầu vào của hệ thống NNID gồm 100 nơron, đại diện cho vector người dùng; tầng ẩn gồm 30 nơron và tầng đầu ra có 10 nơron tương ứng với 10 người dùng.

- *Triển khai hệ thống NNID*

NNID được triển khai theo 3 giai đoạn:

+ Thu thập dữ liệu huấn luyện (training data): thống kê nhật ký đăng nhập của mỗi người dùng trong nhiều ngày trước đó. Lập vector thể hiện tần suất sử dụng các lệnh của mỗi người dùng trong từng ngày.

+ Huấn luyện (training): Huấn luyện NNID để nhận dạng người dùng dựa trên các vector phân bố câu lệnh.

+ Thực hiện (performance): Xác định người dùng dựa trên mỗi vector phân bố lệnh mới. Nếu hệ thống xác định nó không thuộc các người dùng thường, hoặc không có xác định rõ ràng thì sẽ đưa ra cảnh báo về một sự bất thường.

- *Đánh giá về NNID*

Triển khai NNID cho hệ thống có nhiều người dùng thì tỷ lệ phát hiện bất thường vẫn không thay đổi. Hệ thống vẫn có thể học tốt các mẫu hồ sơ của người dùng và bất cứ một hành động nào khác với hành động thông thường của người dùng thì đều bị coi là bất thường.

Đối với các xâm nhập mới, do NNID luôn cập nhật hồ sơ và phân tích hoạt động hàng ngày của mỗi người dùng và NNID cũng được huấn luyện lại theo định kỳ nên các xâm nhập mới sẽ dễ dàng được phát hiện. Các hệ thống hiện nay chỉ cần 90 giây để thực hiện điều này.

NNID dễ dàng huấn luyện và không tốn kém bởi nó hoạt động không trực tuyến và dựa trên dữ liệu nhật ký đăng nhập hàng ngày. Với các hệ thống

phát hiện xâm nhập không yêu cầu thời gian thực thì NNID là một giải pháp khá tối ưu.

Các hệ thống phát hiện truy nhập trái phép truyền thống đang gặp khó khăn trước các cuộc tấn công ngày càng phức tạp và biến hóa lên các hệ thống máy tính. Việc ứng dụng mạng nơron trong phát hiện xâm nhập trái phép đã được nghiên cứu từ lâu và đã thể hiện nhiều ưu điểm so với các hệ thống dùng kỹ thuật truyền thống.

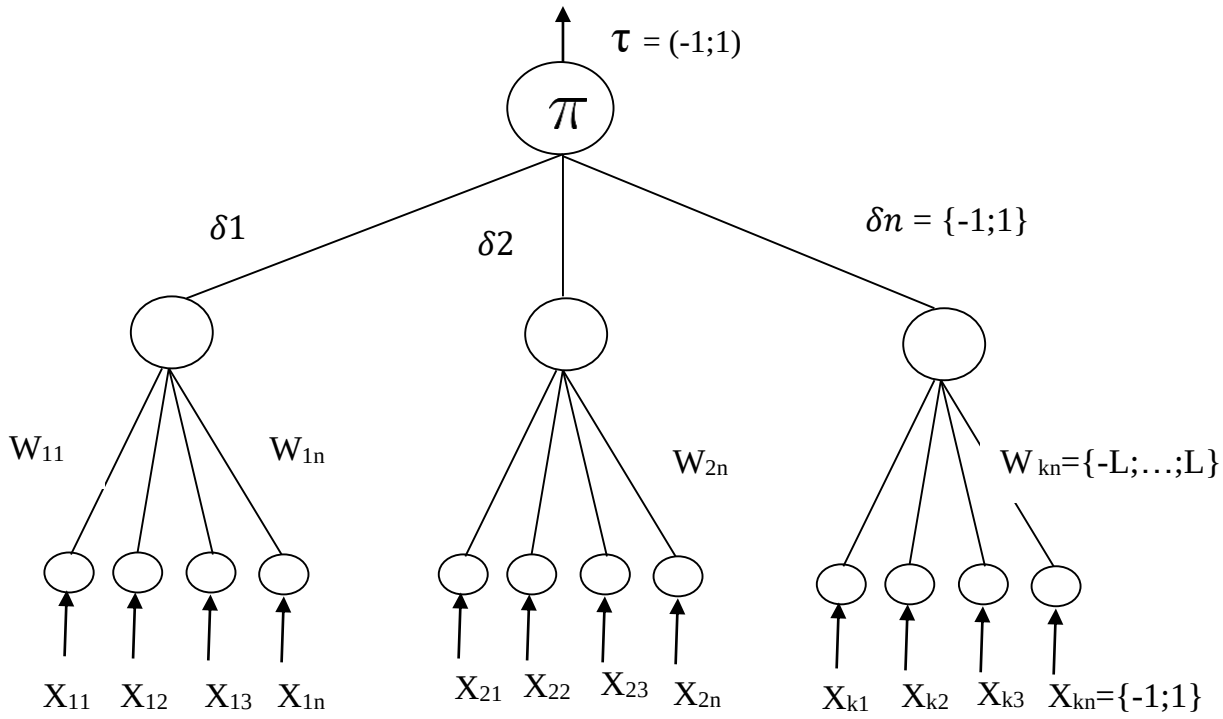
2.4 ỨNG DỤNG MẠNG NEURAL CRYPTOGRAPHY VÀO MÃ HÓA

2.4.1 Ý TƯỞNG

Để xây dựng một hệ thống bảo mật các văn bản quan trọng của công ty như các tài liệu mật, hợp đồng công ty… tôi đã ứng dụng mạng nơron vào mã hóa các tài liệu này, sau đó sẽ lưu trữ tài liệu được mã hóa vào một hệ cơ sở dữ liệu. Tài liệu chỉ được giải mã khi người dùng có được key do người upload cung cấp.

Xây dựng một mạng nơron Perceptron mà các phần tử trọng số liên kết được đồng bộ hóa vào trong lớp mạng này, mà trong đó các trọng số liên kết sẽ là các khóa bí mật trong mô hình Tree Parity Machines.

Mô hình TPM (Tree Parity Machines) bao gồm một vector đầu vào X, một lớp ẩn Sigma δ, một trọng số liên kết W giữa các vector đầu vào và lớp ẩn, và một bộ hàm kích hoạt mà đếm các giá trị kết quả là τ. Nó có thể được mô tả bởi ba thông số: K(số lượng tế bào thần kinh ẩn), N (số lượng các tế bào thần kinh kết nối với đầu vào mỗi tế bào thần kinh ẩn) và L (giới hạn giá trị cho trọng số ({-L ... + L}).



Hình 2.2 Mô hình Tree parity machine

Hai máy có cùng một cấu trúc mạng nơron theo mô hình TPM tương tự nhau. Để tính giá trị đầu ra, ta sử dụng một phương pháp đơn giản:

$$\tau = \prod_{i=1}^{K} \delta i$$

Với:

Nơron ẩn: K

Nơron đầu vào : $X_{ij} \in \{-1, 1\}$

Giá trị trọng số liên kết: $W_{ij} \in \{-l, \ldots . 0, \ldots . +l\}$

δi=Sgn($\sum_{i=1}^{w} W_{ij} X_{ij}$)

$$\text{Sgn}(x) = \begin{cases} -1 \text{ nếu } x < 0 \\ 1 \text{ nếu } x \geq 0 \end{cases}$$

Khi nào chúng ta cập nhật giá trị trọng số liên kết? Và bằng cách nào? Chúng ta chỉ cập nhật giá trị trọng số chỉ khi nào giá trị đầu ra bằng nhau. Ở đây có 3 qui tắc học tập khác nhau:

$$W^{+}_{i,j} = g(W_{i,j} + X_{i,j}.\tau\ \theta(\delta i\ \tau))$$ Hebbian learning rule (1)

$W^{+}_{i,j} = g(W_{i,j} - X_{i,j}.\tau\ \theta(\delta i\ \tau))$ Anti-Hebbian learning rule (2)

$W^{+}_{i,j} = g(W_{i,j} + X_{i,j}\ \theta(\delta i\ \tau))$ Random-walk learning rule (3)

$$\text{Với } \theta_N(x) = \begin{cases} 0\ if\ x\ \leq \frac{N}{2} \\ 1\ if\ x\ > \frac{N}{2} \end{cases} \quad (4)$$

Với:

Theta θ là một chức năng đặc biệt. Theta (a, b) = 0 nếu a ≠ b; ngược lại a=b thì Theta = 1.

g (...) có chức năng giữ trọng số trong phạm vi (-L ; + L)

x là vector đầu vào và w là vector trọng số.

Sau khi hai máy được đồng bộ hóa, thì ma trận trọng số liên kết của chúng là bằng nhau. Ta có thể sử dụng ma trận này để xây dựng một khóa chia sẻ giữa hai máy.

Trong [11], có rất nhiều thông tin về các cuộc tấn công trên thuật toán này. Trong một kênh công cộng chung thì những kẻ tấn công Eve có thể nghe trộm và bắt được giá trị thông tin giữa bên A và B, nhưng không có cơ hội để thay đổi chúng. Tôi chỉ muốn nói ở đây là kẻ tấn công Eve không thể hack được.

Đối với hệ thống mã hóa thông thường, chúng ta có thể cải thiện sự an toàn của các giao thức bằng cách tăng chiều dài của khóa. Trong trường hợp của mã hóa bằng nơron nhân tạo, chúng ta cải thiện bằng cách tăng giá trị L của mạng nơron. Thay đổi tham số này làm tăng chi phí của một cuộc tấn công thành công theo cấp số nhân. Do đó, phá vỡ sự an toàn của trao đổi khóa bằng mạng nơron thuộc độ phức tạp cao.

Ứng dụng giải thuật di truyền vào bước khởi tạo ma trận trọng số đầu vào để tạo ra 2 ma trận tương đối giống nhau thông qua sự so sánh các thông số của ma trận, quá trình này nhằm giảm thời gian đồng bộ giữa 2 cây TPM nên sẽ tăng được tốc độ xử lý của chương trình.

Chu trình hoạt động của Gas:

- Bước 1: Khởi tạo và đánh giá quần thể

  Kích thước quần thể được xác định và quần thể được khởi tạo ngẫu nhiên. Một hàm fitness sau đó được áp dụng sẽ đánh giá quần thể tức là nó sẽ quyết định sự tương thích của một cá thể so với phần còn lại của quần thể.

- Bước 2: Lựa chọn của nhiễm sắc thể

  Có rất nhiều phương pháp, trong đó sự chọn lọc cha mẹ phải được thực hiện. Trong bài báo này, chúng tôi tập trung vào roulette wheel và tournament selection.

- Bước 3: Lai chéo chọn lọc DNA

  Khi cá thể cha mẹ được lựa chọn, lai chéo hoặc trộn và kết hợp được sử dụng để tạo ra quần thể mới của cá thể con.

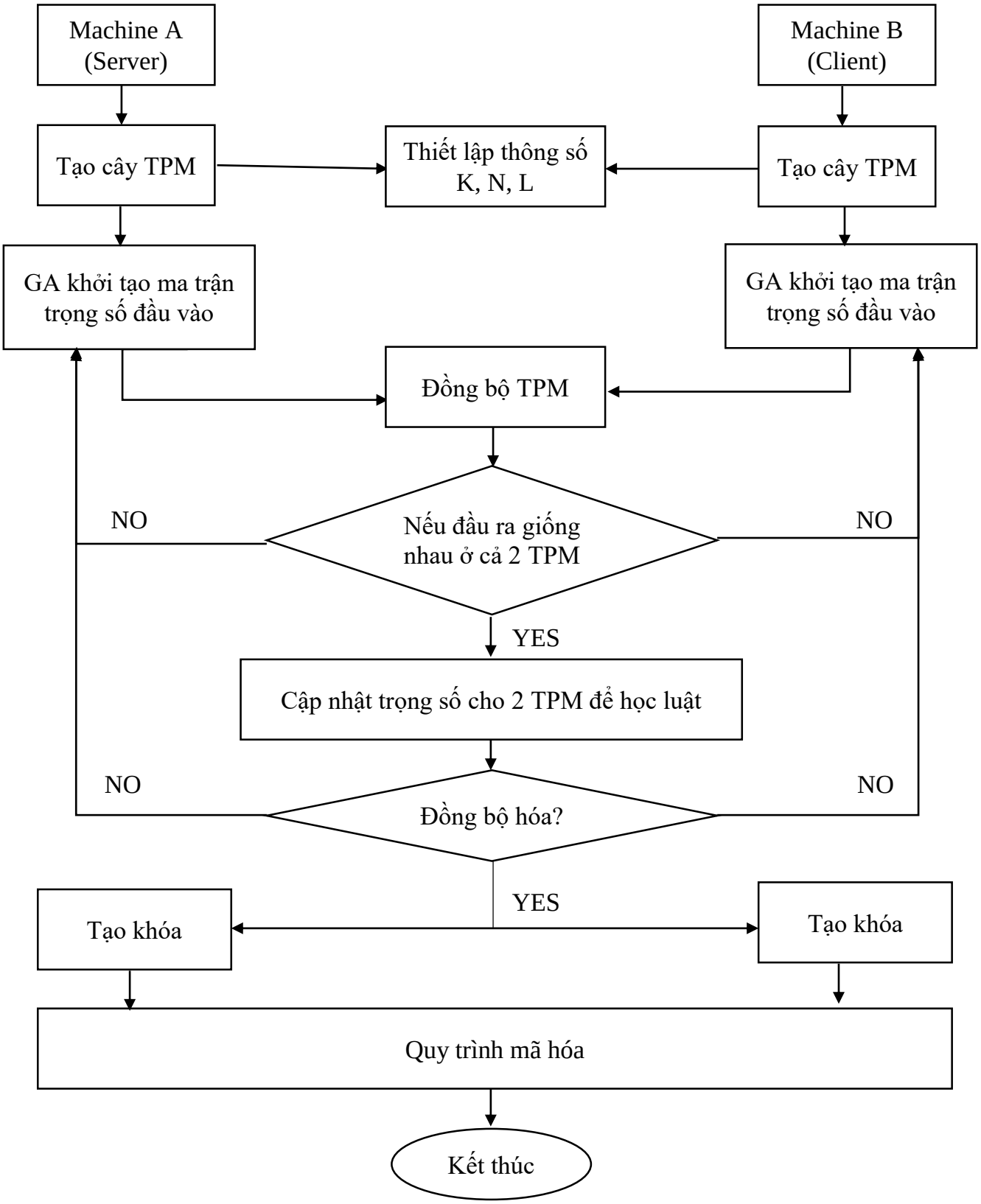
- Bước 4: Đột biến

  Đột biến trong các thuật toán di truyền đóng vai trò như một công cụ mà gây ra sự đa dạng trong dân số.

  Các bước trên được lặp đi lặp lại cho đến khi một điều kiện thích nghi được đáp ứng.

Bằng cách ứng dụng giải thuật di truyền , chúng tôi cố gắng tối ưu hóa các trọng số đầu vào để tạo ra khóa trong việc đồng bộ tạo khóa của cây TPM, để đạt được tốc độ xử lý nhanh hơn và ít lặp lại quá trình xử lý.[8]

2.4.2 QUY TRÌNH MÃ HÓA SỬ DỤNG THUẬT TOÁN NƠRON



Hình 2.3 Thuật toán mã hóa bằng mạng nơron nhân tạo

Thuật toán Algorithm được sử dụng trong khóa nơron dựa theo quy tắc sau:

1. Gán trọng số cho cây TPM ngẫu nhiên.
2. Lặp lại cho đến khi cả hai cây TPM được đồng bộ hóa

2.1 GA tạo ra ma trận trọng số đầu vào

2.2 Tính toán giá trị của các nơron ẩn sử dụng

2.3 Tính toán giá trị của các nơron đầu ra sử dụng

2.4 Dữ liệu đầu ra của cây TPM sẽ được đối chiếu.

Nếu đầu ra khác nhau , quay về 2.1

Nếu không áp dụng một học luật (Hebbian, Anti-Hebbian và Random Walk) cho trọng số sử dụng phương trình (1), (2), (3) và (4) ở trên.

+ *Đối với Geometric Attack*

1) Nếu Output A! = Output B, kẻ tấn công không cập nhật Output C

2) Nếu Output A = Output B = Output C, kẻ tấn công cập nhật bằng cách sử dụng quy tắc học tập.

3) Nếu Output A = Output B! = Output C; Những kẻ tấn công không thể cập nhật số trọng nhưng hai cây A và B cập nhật được trọng số của nó.

CHƯƠNG 3: CÀI ĐẶT CHƯƠNG TRÌNH THỬ NGHIỆM

3.1 MỤC ĐÍCH ỨNG DỤNG

Công ty cổ phần Kiên Nhẫn là một đơn vị chuyên cung cấp những ứng dụng, website theo yêu cầu của khác hàng. Với số lượng nhân viên hơn 30 người và một số cộng tác viên part-time, để quản lí công việc hằng ngày cũng như tiến độ thực hiện những dự án quy mô vừa và lớn công ty yêu cầu nhân viên gửi báo cáo bằng file văn bản.

Ngoài những văn bản công việc cơ bản, nhân viên cũng gửi những file mang tính chất bí mật của công ty nên phải đảm bảo không được để những công ty cạnh tranh hoặc những đối tượng xấu có được.

Ứng dụng này được tạo ra cũng bởi lý do đó. Các file văn bản sẽ được gửi đi dưới dạng đã được mã hóa và chỉ những người có quyền hạng mới có khả năng giải mã và xem file. Ứng dụng được xây dựng theo cơ chế client-server kèm theo quy trình mã hóa kết hợp giữa giải thuật di truyền và neural cryptography mang lại tính tuyệt mật và an toàn cao.

3.2 CÀI ĐẶT VÀ CHẠY THỬ NGHIỆM

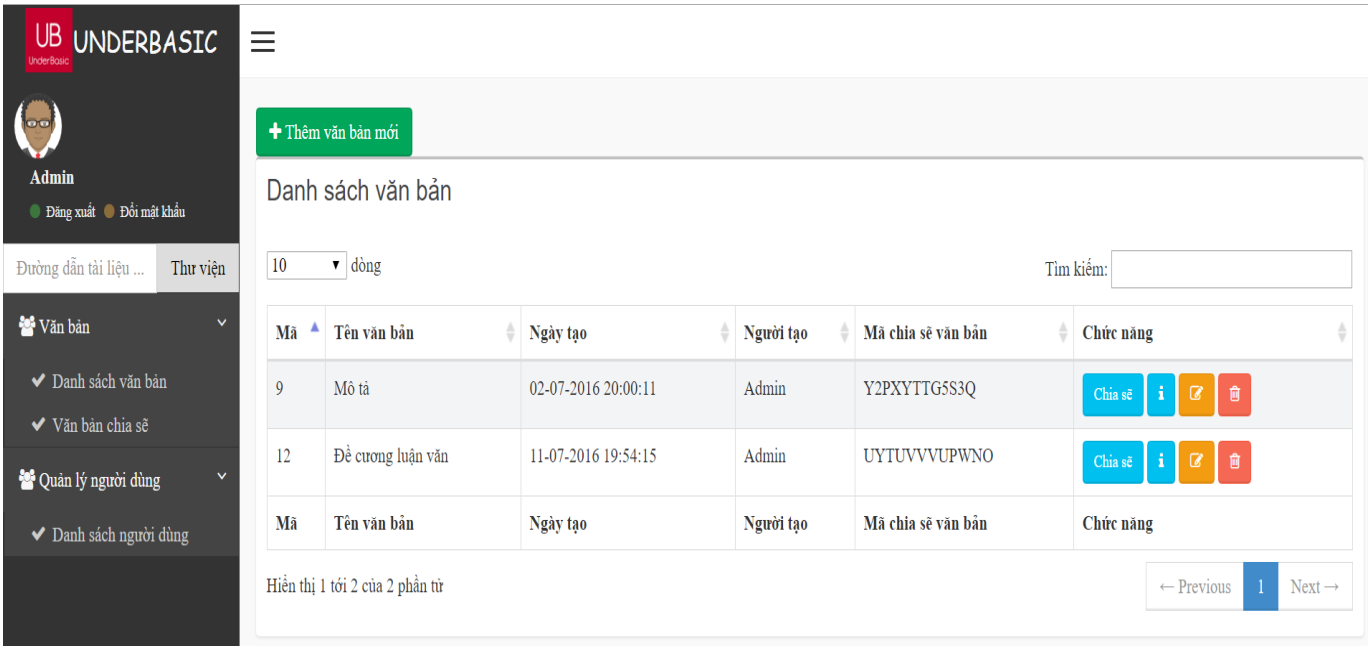
Chương trình được viết với ngôn ngữ C# trong bộ Visual Studio 2015 và SQL server 2010. Được chạy thử nghiệm trong nội bộ công ty .

Cài đặt chương trình kết nối với SQL server :

Tên database : UngDungMaHoa

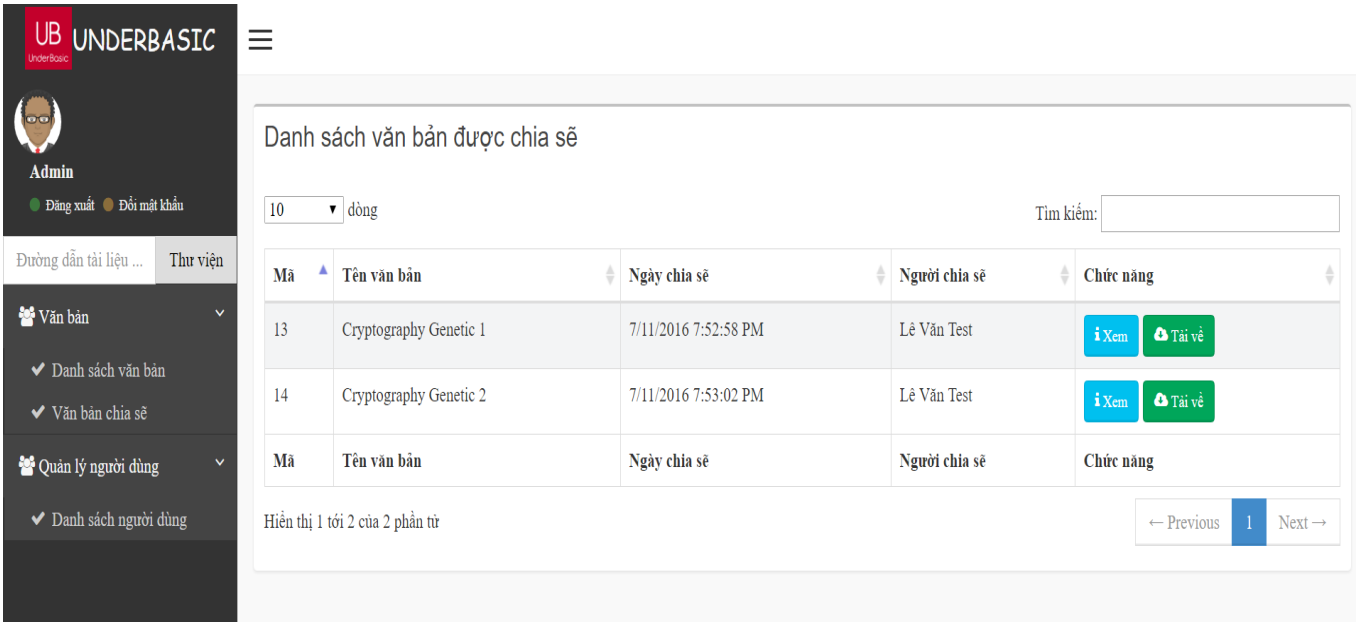
User : sa

Pass : 123123

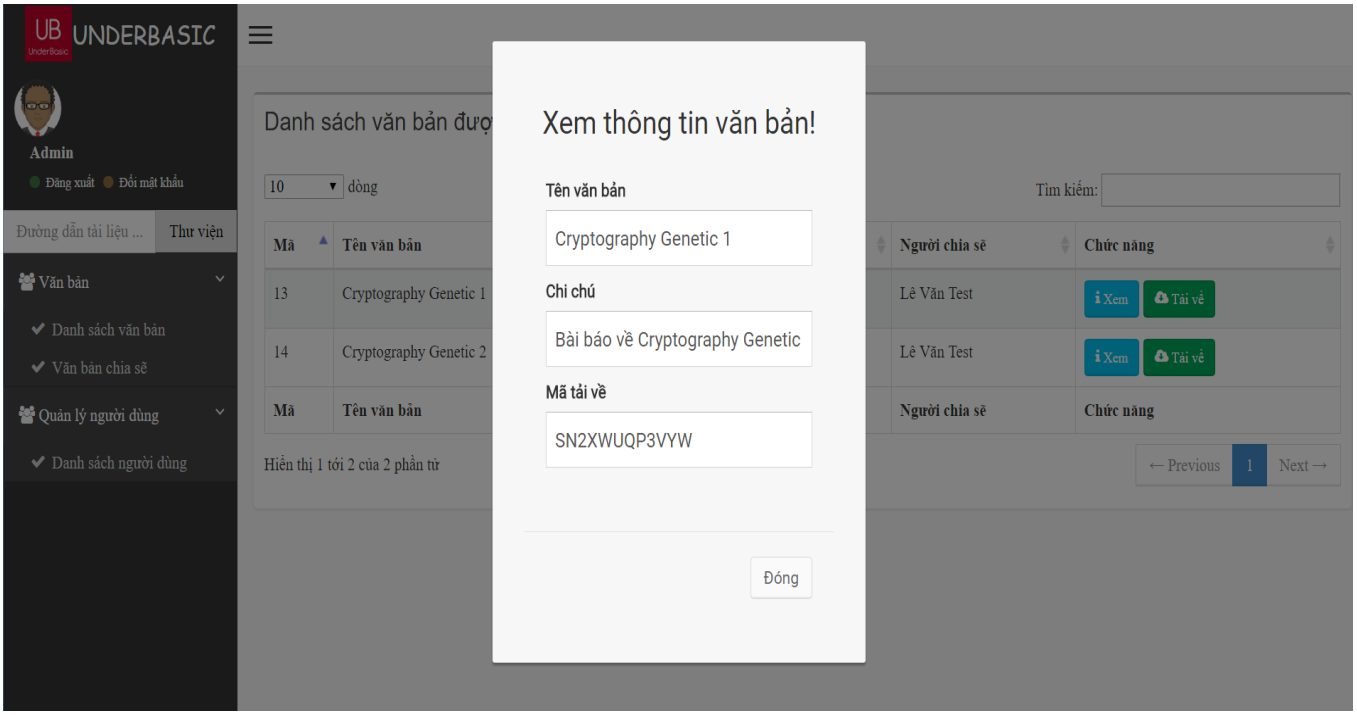


Hình 3.1 Giao diện chính của chương trình (Quyền admin)

Trong giao diện chính chúng ta có thể quản lý được cái mục văn bản, tài liệu của mình và có thể chia sẻ hoặc sửa đổi các mục này. Chỉ những người dùng được chia sẻ mới có được key và download dùng key để giải mã được tài liệu.

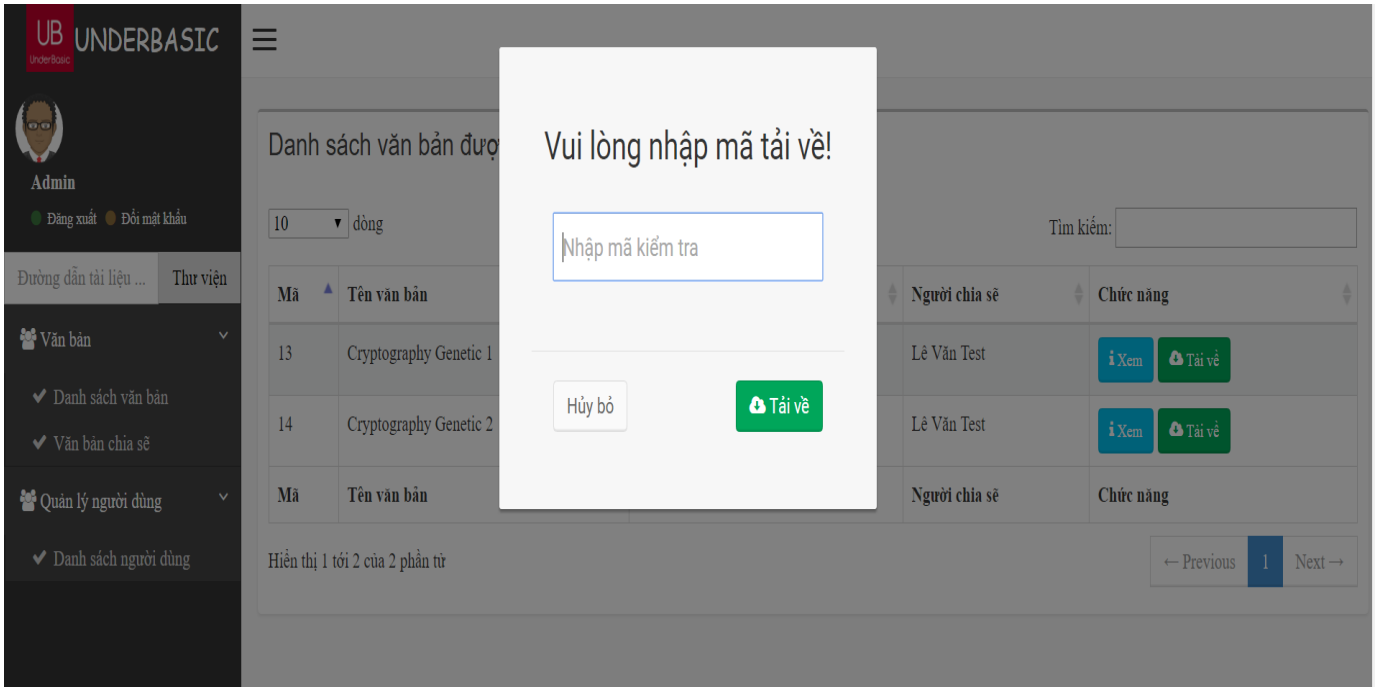


Hình 3.2 Mục văn bản được chia sẻ

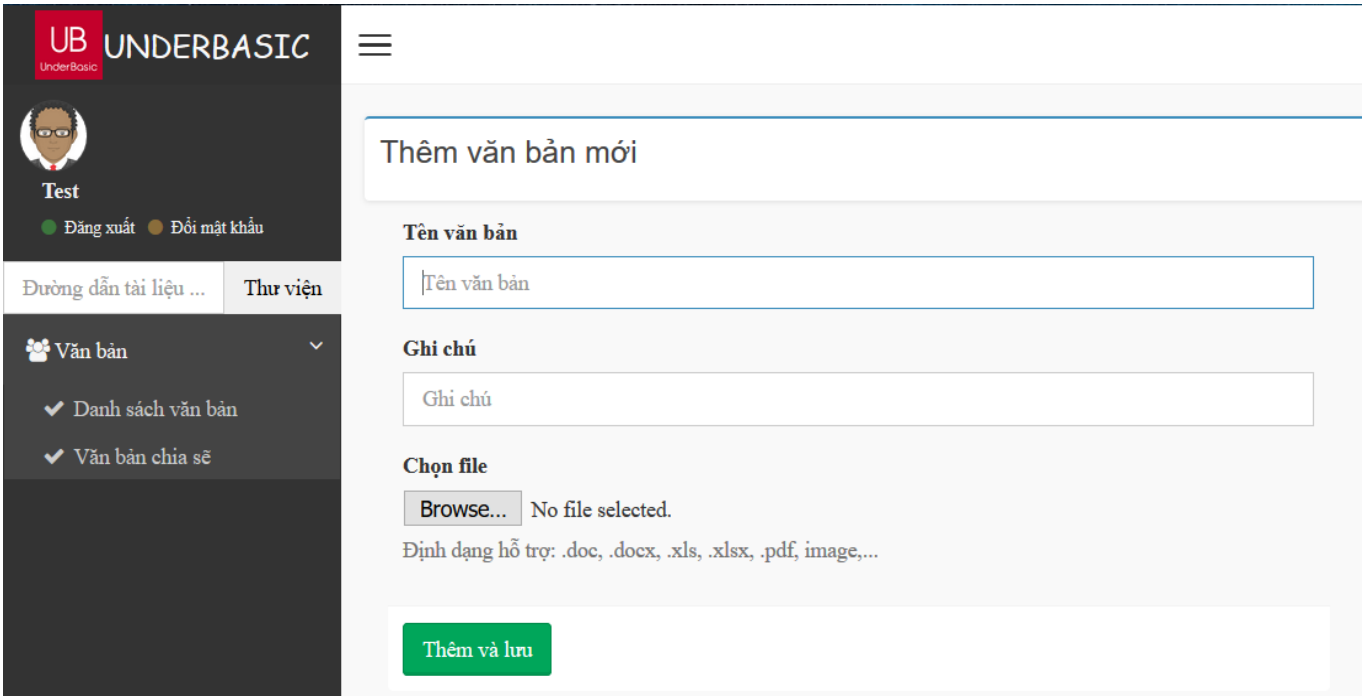


Hình 3.3 Mục thông tin của văn bản được chia sẻ

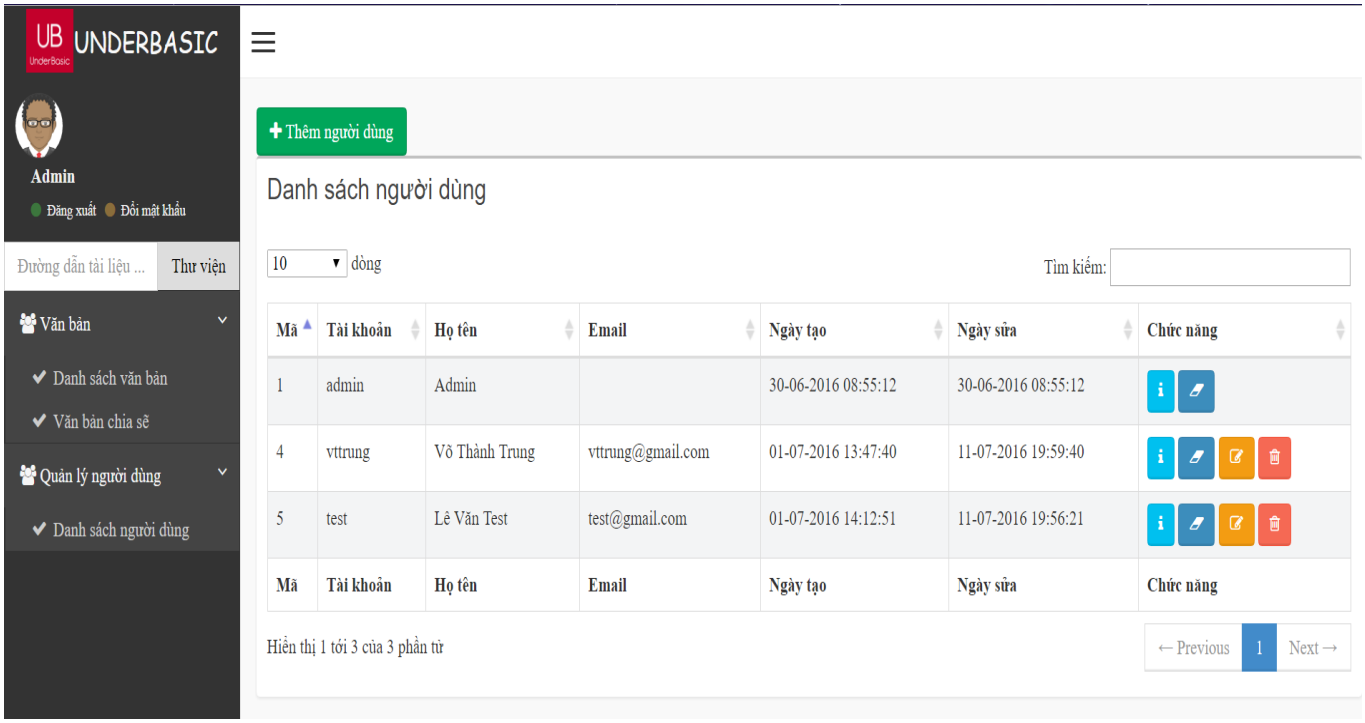
Văn bản được chia sẻ chỉ được xem những mục như tên văn bản, ghi chú, key mã hóa. Khi người dùng muốn xem tài liệu phải nhập đúng key mã hóa để chương trình giải mã và tải về.



Hình 3.4 Giao diện tải văn bản



Hình 3.5 Giao diện thêm văn bản



Hình 3.6 Giao diện quản lí người dùng (quyền admin)

3.3 KẾT QUẢ ĐẠT ĐƯỢC VÀ HƯỚNG PHÁT TRIỂN:

❖ ***Kết quả đạt được***

- Tìm hiểu chi tiết cơ sở lý thuyết liên quan đến mạng nơron, đặc trưng, cách xây dựng và huấn luyện mạng nơron.
- Tìm hiểu chi tiết cơ sở dữ liệu liên quan đến giải thuật di truyền, các cơ chế mã hóa ứng dụng Giải thuật di truyền. Các khái niệm về Giải thuật di truyền, nhiễm sắc thể, các toán tử lai, ghép chéo, đột biến.
- Tổng quan về Mật mã học, cơ chế mã hóa và giải mã.
- Nghiên cứu ứng dụng Giải thuật di truyền, mạng nơron nhân tạo vào xây dựng khóa bí mật.
- Xây dựng thành công thử nghiệm xây dựng khóa bí mật ứng dụng vào bảo mật thông tin tại công ty Kiên Nhẫn.

❖ ***Đánh giá thực tiễn ứng dụng***

- Tốc độ xử lý:

Dưới đây là bảng miêu tả tốc độ tạo key và mã hõa khi dùng đồng bộ TPM bình thường và đồng bộ khi có sử dụng giải thuật di truyền.

Kích thước Key	Không dùng GAs		Dùng GAs	
8 kí tự	2735 lần lặp	0.35 s	1352 lần lặp	0.29 s
12 kí tự	3251 lần lặp	0.39 s	2163 lần lặp	0.32 s
16 kí tự	3861 lần lặp	0.45 s	3187 lần lặp	0.37 s

- Các số liệu trên chỉ mang tính tham khảo do điều kiện thực hiện thí nghiệm còn tương đối.

- Hạn chế của ứng dụng:

Chưa thực hiện công việc truyền và kết nối với nhiều máy con cùng lúc được.
Công việc bảo mật các file dữ liệu và key mã hóa ở server còn tùy thuộc vào con người nên tính an toàn vẫn chưa cao.
Chưa đủ điều kiện và môi trường thí nghiệm ở quy mô lớn để có thể so sánh được với các phương thức mã hóa khác.

❖ ***Hướng phát triển***

- Neural cryptography vẫn còn khá mới, thông qua những nghiên cứu và ứng dụng của nó hiện tại cho thấy được tiềm năng phát triển rất lớn trong các lĩnh vực bảo mật, mã hóa.
- Một số lĩnh vực có thể ứng dụng thêm như nhận diện khuôn mặt, bóng mắt, vân tay, giọng nói… hoặc trong việc mã hóa, giải mã thông tin như email, tin nhắn, mạng xã hội..

TÀI LIỆU THAM KHẢO

[1] A.Singh and A. Nandal,“ *Neural Cryptography for Secret Key Exchange and Encryption with AES*”, Int. Journal of Advanced Research in CS and SE,Vol3(5) , pp376-381,May 2013.

[2] A.Forouzan, *“Cryptography and Network Security”* , First Edition. McGraw-Hill, USA, 2007.

[3] Sudip Kumar Sahana and Prabhat Kumar Mahanti, *“An Analysis of Email Encryption using NeuralCryptography”*, Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2 Issue 1, January – 2015.

[4] E. Volna, M. Kotyrba, and V. Kocian, “*Cryptography based onneural network*” , ECMS, pp. 386-391 (2012).

[5] A.M. Allam, H.M. Abbas, M.W. El-Kharashi, “*Authenticated key exchange protocol using neural cryptography with secret boundaries”* , In Proc. of the IEEE International Joint Conference on Neural Networks (IJCNN), pp. 1-8 (2013).

[6] http://voer.edu.vn/m/cac-ky-thuat-tri-tue-nhan-tao-hien-dai/00e47f55

[7] http://antoanthongtin.vn

[8] E.Klein, R Mislovathy, I Kanter, A.Ruttor ,W.Kinzel,“ *Synchronization of Neural Networks by Mutual Learning and its Application to Cryptography*”, Advances in N eural I nformation Processing Systems,Volume 1 7, M IT P ress, Cambridge, MA,2005. PP 689- 696.

[9] Phạm Công Thiện, “*Nghiên cứu mạng nơron nhân tạo và ứng dụng vào trao đổi khóa bí mật*”, 2015