A picture containing picture frame, rectangle, frame

Description automatically generated**TRƯỜNG ĐẠI HỌC LÂM NGHIỆP**

--🙢🕮🙠---



**AN TOÀN VÀ BẢO MẬT THÔNG TIN**

***Đề tài báo cáo****:*

**BẢO MẬT THÔNG TIN KHÁCH HÀNG CỦA MỘT CHI NHÁNH**

**NGÂN HÀNG**

|  |  |
| --- | --- |
| **Họ và tên sinh viên:**  **Giảng viên HD:** | **Đặng Phương Linh**  **Nguyễn Tiến Công**  **Mai Hà An**  **HÀ NỘI,2023** |

MỤC LỤC

[CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI 3](#_Toc137591634)

[CHƯƠNG 2: CÁC PHƯƠNG ÁN 13](#_Toc137591638)

[Phương án 1: Tường lửa 13](#_Toc137591639)

[Phương án 2: Mã hóa dữ liệu 17](#_Toc137591640)

[Phương án 3: Đăng ký và mật khẩu 19](#_Toc137591641)

[CHƯƠNG 3: KẾT QUẢ THỰC HIỆN 23](#_Toc137591642)

[CHƯƠNG 4: KẾT LUẬN, KIẾN NGHỊ 25](#_Toc137591643)

# **CHƯƠNG 1: TỔNG QUAN VỀ ĐỀ TÀI**

**Đề tài:** Bảo mật thông tin khách hàng của một chi nhánh ngân hành

1. **Những việc làm của thế giới trước vấn đề bảo mật thông tin ngân hàng hiện nay.**

**-** Hiện nay thế giới đã thường xuyên đưa ra những cảnh báo về lừa đảo cùng với đó là các giải pháp cho ngân hàng , khách hàng để bảo mật thông tin một cách an toàn nhất

- *Về ngân hàng*

+ Xây dựng hệ thống mạng nội bộ an toàn: Điều đầu tiên cần hướng tới trong việc bảo mật thông tin khách hàng là ngân hàng cần có cho mình một hệ thống mạng nội bộ an toàn bằng cách thiết lập các phần mềm có tính năng bảo mật hiệu quả để giảm thiểu nguy cơ xâm nhập của các hacker. Bởi vậy ngân hàng cần có nhân viên hỗ trợ về mảng trách nhiệm và kiến thức về an ninh mạng để từ đó có thể sớm khắc phục vấn đề này nhanh chóng.

+ Nâng cấp phần mềm liên tục: Mỗi ngân hàng cần có cho mình một phần mềm giúp bảo mật thông tin khách hàng. Vì thế, các ngân hàng cần đầu tư vào các biện pháp phần mềm bảo mật hiện đại và cập nhật nó liên tục điều đó sẽ dễ dàng trong việc bảo mật thông tin khách hàng trước các nguồn tin tặc và lừa đảo.

+ Kiểm tra các lỗ hổng bảo mật: Việc xảy ra các lỗ hổng nhỏ trong bảo mật thông tin khách hàng cũng khiến ngân hàng gặp tổn thất rất lớn. Vì thế các ngân hàng sở hữu trang web thương mại điện tử cần thường xuyên kiểm tra website để phát hiện những sai sót mà các công cụ bảo mật không phát hiện ra được. Do đó cần có giải pháp thuê chuyên gia và những người có kinh nghiệm để sửa chữa định kỳ các lỗ hổng có thể xảy ra tới khách hàng.

+ Công khai chính sách bảo mật: Khách hàng cần biết rằng ngân hàng có một chính sách bảo mật thông tin khách hàng hiệu quả và bạn có thể giữ thông tin đó một cách an toàn. Đảm bảo rằng ngân hàng luôn thành thật với khách hàng về dữ liệu thông tin cá nhân và những gì ngân hàng làm với nó. Thành thật với khách hàng sẽ khiến ngân hàng xây dựng được lòng tin của khách hàng và cho họ thấy phần mềm bảo mật thông tin khách hàng của ngân hàng cực kì đáng tin cậy.

+ Giáo dục nhân viên bảo mật: Nhân viên thường là người xử lý dữ liệu khách hàng và có trách nghiệm bảo mật thông tin khách hàng. Do đó họ cần đảm bảo kiến thức chuyên sâu và cập nhật kỹ năng thường xuyên trong quá trình làm việc

+ Sử dụng nhiều lớp bảo mật: Việc cập nhập nhiều lớp bảo mật sẽ giúp cho ngân hàng trong việc bảo mật thông tin khách hàng đối với những phần mềm độc hại dưới dạng thông tin rác. Có thể sử dụng tường lửa để ngăn chặn tội phạm mạng và dữ liệu xấu xâm nhập.

- *Về khách hàng*

+ Tuyệt đối không thuê, cho thuê, mượn, cho mượn tài khoản ngân hàng, tuyệt đối không mua, bán thông tin tài khoản ngân hàng. Đây là hành vi bất hợp pháp, sẽ bị xử phạt theo quy định của pháp luật.

+ Không sử dụng giấy tờ tùy thân của mình để mở hộ hoặc bán tài khoản thanh toán thẻ cho người khác. Việc cho mượn tên, giấy tờ để làm thẻ, mở tài khoản có thể là hình thức tiếp tay cho kẻ lừa đảo.

+ Trường hợp đã từng mở tài khoản ngân hàng sau đó chuyển cho người khác sử dụng, người dân cần mang giấy tờ cá nhân đến ngân hàng để làm thủ tục đóng tài khoản đó nhằm bảo vệ mình, đồng thời ngăn chặn các đối tượng sử dụng tài khoản làm công cụ phạm tội. Song song đó, người dân không cung cấp thông tin cá nhân, mật khẩu của các tài khoản mạng xã hội, ngân hàng, ví điện tử và mã OTP cho những người lạ hoặc chuyển tiền cho tổ chức, cá nhân mạo danh cán bộ, cơ quan nhà nước để giải quyết các thủ tục pháp lý, từ đó đối tượng dễ dàng chiếm đoạt tài sản...

+ Chủ động giữ kín các thông tin cá nhân/thông tin tài khoản, không tiết lộ cho bất kỳ ai để tránh các trường hợp chủ quan, bị lợi dụng gây mất tiền, tài sản.

+ Nếu phát hiện đối tượng có hành vi nhờ mở tài khoản ngân hàng, mở thẻ hoặc mua bán tài khoản ngân hàng với số lượng lớn thì cần kịp thời báo cơ quan Công an nơi gần nhất để xử lý.

+ Trong quá trình sử dụng dịch vụ, khách hàng cần tuân thủ theo các hướng dẫn của tổ chức cung ứng dịch vụ. Đặc biệt, khách hàng cần nâng cao cảnh giác với những thủ đoạn của tội phạm trên mạng. Ngoài ra, khách hàng cần bảo mật thông tin cá nhân, thông tin tài khoản... để tránh bị đánh cắp, lợi dụng (không cung cấp tài khoản đăng nhập, mật khẩu, mã OTP trong bất kỳ trường hợp nào yêu cầu để nhận/nạp tiền; không sử dụng mã PIN gắn liền với các thông tin cá nhân như số di động, số chứng minh nhân dân, căn cước công dân, ngày sinh, ghi số PIN bỏ vào ví; không nạp/chuyển tiền theo yêu cầu của người lạ khi nhận được các cuộc gọi lạ...). Khách hàng không mở hộ thẻ/tài khoản cho người khác, kể cả cho mượn hoặc bán.

+ Đối với mật khẩu truy cập dịch vụ giao dịch trực tuyến cần đặt mật khẩu khó đoán, thay đổi mật khẩu thường xuyên và không sử dụng các tính năng lưu mật khẩu để đăng nhập tự động. Không cung cấp tên, mật khẩu đăng nhập ngân hàng trực tuyến, mã xác thực một lần (OTP), cũng như số thẻ ngân hàng qua điện thoại, email, mạng xã hội, website.

+ Trong trường hợp bị lộ hoặc nghi ngờ bị lộ Tên đăng nhập/Mật khẩu, khách hàng cần nhanh chóng thông báo tới ngân hàng để được hỗ trợ kịp thời; trường hợp bị mất thẻ, cần khóa thẻ trên ứng dụng ngân hàng điện tử càng sớm càng tốt, tránh nguy cơ bị mất tiền trong tài khoản thẻ.

+ Hạn chế dùng máy tính công cộng, thiết bị di động kết nối với mạng không dây (Wifi) công cộng để truy cập vào hệ thống ngân hàng điện tử. Khách hàng nên gõ trực tiếp địa chỉ các trang web ngân hàng điện tử thay vì chọn đường link có sẵn, chỉ đăng nhập tại website chính thức của ngân hàng; luôn đăng xuất khỏi các website đã nhập thông tin cá nhân.

-Ngoài những giải pháp còn có thể nhắc tới những phương thức bảo mật: mã hóa và chữ ký số

### **A, Mã hóa:**

-Một quá trình làm cho các thông điệp không thể giải đoán được, ngoại trừ những người có khóa giải khóa được cho phép sử dụng. Dùng để che giấu nội dung của văn bảo rõ: để đảm bảo sao cjo chỉ người chủ hợp pháp của thông tin mới có quyền truy cập thông tin, hay nói cách khác là chống truy nhập không đúng quyền hạn

-Tạo các yếu tố xác thực thông tin: đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực Tổ chưc các sơ đồ chữ kí điện tử đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

* *CÁC LOẠI MÃ HÓA PHỔ BIẾN ĐƯỢC DÙNG HIỆN NAY:*

+ Mã hóa dữ liệu đối xứng

+ Mã hóa dữ liệu bất đối xứng

+ Mã hóa dữ liệu một chiều

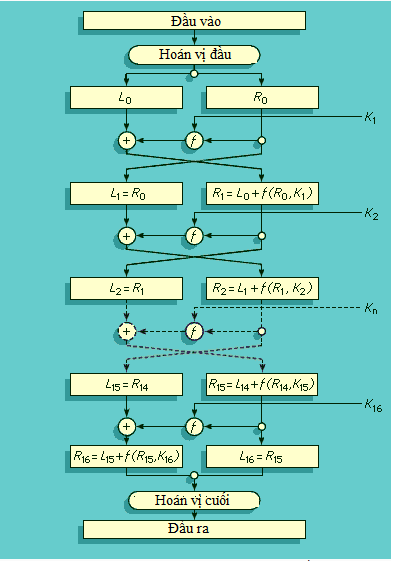
* Các thuật toán được khuyến khích dùng hiện nay : ( thuật toán DES và 3DES)

A1, Thuật toán DES

+ Thuật toán mã khối DES (Data Encryption Standard) là một thuật toán mã khối với kích thước khối 64 bít và kích thước khóa 56 bít, được công bố chính thức bởi Tổ chức Tiêu chuẩn xử lý thông tin liên bang Hoa Kỳ (FIPS) vào tháng 11/1976 và được xuất bản trong tài liệu FIPS PUB 46 (01/1977). Thuật toán DES đã trải quả nhiều lần cập nhật: năm 1988 (FIPS-46-1), 1993 (FIPS-46-2), 1998 (FIPS-46-3). Tiền thân của thuật toán DES là thuật toán Lucifer, một thuật toán do IBM phát triển. Cuối năm 1976, DES được chọn làm chuẩn mã hóa dữ liệu của Hoa Kỳ, sau đó được sử dụng rộng rãi trên toàn thế giới trong lĩnh vực an toàn, bảo mật thông tin trên môi trường số.

+ Đặc điểm kỹ thuật

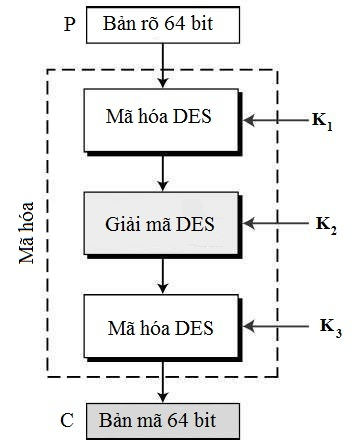
* DES: được thiết kế để mã hóa và giải mã các khối dữ liệu 64 bít với một khóa có độ dài 64 bít. Việc giải mã phải được thực hiện bởi một khóa tương ứng như trong quá trình mã hóa, mỗi khóa gồm 64 bít, trong đó 56 bít được sử dụng để thực hiện mã hóa/giải mã trong thuât toán. 8 bít còn lại được dùng để kiểm tra/phát hiện lỗi.
* Quy trình mã hóa



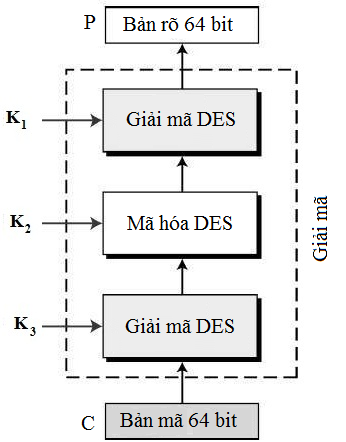
* Mã hóa DES được thực hiện qua 16 vòng. Thông tin đầu vào là 64 bít, sẽ được chia thành 2 khối (block) trái (L) và phải (R). Sau đó từ khóa (56 bít) người ta tạo ra các khóa con (subkey) 48 bít gọi là Ki. Hàm f ở trên thực chất là 1 hàm hoán vị.
* Trong quá trình mã hóa, dữ liệu đầu vào phải thực hiện quá trình hoán vị đầu (initial permutation) và hoán vị cuối (final permutation) sau vòng thứ 16. Việc thực hiện hoán vị phục vụ cho quá trình đưa thông tin vào và lấy thông tin ra từ các khối phần cứng, tạo điều kiện cho việc cài đặt phần cứng. Hàm cơ sở f cho phép đảm bảo tính bảo mật trong thuật toán DES này.
* Việc thực hiện nhiều lần các bước lặp với tác dụng của f là nhằm tăng cường tính phi tuyến và tính khuếch tán đã có trong hàm f.
* Cấu trúc của vòng lặp DES thực hiện theo công thức sau:
* (Li,Ri) = (Ri-1, Li-1 XOR f (Ri-1,Ki))
* Trong đó (Li,Ri) là nửa trái và nửa phải lấy được của phép biến đổi vòng lặp thứ i

A2,Thuật toán 3DES

* Thuật toán 3DES sử dụng một nhóm khóa bao gồm 03 khóa DES là K1, K2 và K3, mỗi khóa có giá trị 56 bít. Thuật toán mã hóa thực hiện như sau:



* Quá trình mã hóa
* Bản mã= EK3(DK2(EK1(Bản rõ)))
* Trước tiên, thực hiện mã hóa DES với khóa K1, tiếp tục giải mã DES với khóa K2 và cuối cùng mã hóa DES với khóa K3(E – Encryption: quá trình mã hóa; D - Decryption: quá trình giải mã; Bản rõ: Dữ liệu đầu vào của phép mã hóa hoặc dữ liệu đầu ra của phép giải mã; Bản mã: Dữ liệu đầu ra của phép mã hóa hoặc dữ liệu đầu vào của phép giải mã).
* Quá trình giải mã



* Bản rõ = DK1(EK2(DK3(Bản mã))
* Quá trình giải mã với việc  giải mã với khóa K3, sau đó mã hóa với khóa K2,và cuối cùng giải mã với khóa K1..
* 3DES mã hóa một khối dữ liệu có giá trị 64 bít (bản rõ) thành một khối dữ liệu mới có giá trị 64 bít (bản mã). Các tiêu chuẩn chỉ ra phương thức lựa chọn nhóm khóa (K1,K2, K3) như sau:

+Lựa chọn 1: K1,K2, K3 là các khóa độc lập

+Lựa chọn 2: K1,K2 là hai khóa độc lập và  K3 =K1

+Lựa chọn 3: K1=K2=K3

Lựa chọn 1 là phương thức mã hóa mạnh nhất với 168 bít khóa độc lập (168=3x56). Lựa chọn 2 ít bảo mật hơn với 112 bít khóa ( 2x56=112 bít) và lựa chọn 3 chỉ tương đương với việc mã hóa DES 1 lần với 56 bít khóa. Mỗi khóa DES thông thường được lưu trữ và truyền đi trong 8 byte, vì vậy một nhóm khóa yêu cầu 8 hoặc 16, 24 byte cho việc lưu trữ khóa.

1. **Chữ ký số:**

* Chữ kí số được sử dụng cho việc xác thực người gửi bằng việc áp dụng mã hóa khóa công khai lại Để tạo ra một chữ ký số, người gửi mã hóa một thông điệp với chìa khóa riêng của mình. Trong trường hợp này, bất cứ người nhận nào đó có chìa khóa công khai của họ đều có thể đọc nó, song người nhận có thể tin chắc rằng người gửi thực sự là tác giả của thông diệp. Một chữ ký số thường được gắn kèm với thông diệp được gửi , cũng giống như chữ ký viết tay. Tính chân thực và việc xác nhận được đảm bảo bằng việc sử dụng chữ ký số.
* Được coi là chữ ký điện tử an toàn khi đáp ứng các điều kiện sau:

+ Chữ ký số được tạo ra trong thời gian chứng thư số có hiệu lực và kiểm tra được bằng khóa công khai ghi trên khóa công khai ghi trên chứng thư số có hiệu lực đó.

+ Chữ ký số được tạo ra bằng việc sử dụng khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số do tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng được cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số hoặc tổ chức cung cấp dịch vụ chứng thực chữ ký số nước ngoài được công nhận tahi Việt Nam cấp.

+ Khóa bí mật chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.

+ Khóa bí mật và nội dung thông điệp dữ liệu chỉ gắn duy nhất với người ký khi người đó ký số thông điệp dữ liệu.

* Thế giới hiện đã và đang cố gắng làm tốt trong công cuộc bảo đảm an toàn thông tin cho khách hàng tuy nhiên vẫn còn rất nhiều lỗ hổng trong đó:

+ Hiện nay vẫn có rất nhiều lỗ hổng trong công tác bảo mật của hệ thống ngân hàng. Hacker có thể tấn công vào hệ thống dữ liệu ngân hàng qua các đối tác của ngân hàng, tiến công trực tiếp vào website thay đổi giao diện để tống tiền, lấy dữ liệu, thâm nhập hệ thống để thực hiện lệnh chuyển tièn nhằm chiếm đoạt thông tin, tài sản của ngân hàng và cả khách hàng.

+ Những vấn đề khó khăn trong bảo mật không thể không nhắc tới đối tác của ngân hàng, trong khi các ngân hàng đặc biệt chú trọng tới bảo đảm an ninh mạng và thế giới cũng tìm ra nhiều giải pháp để bảo mật thông tin, thì khách hàng lại không đặt nặng vấn đề này. Đã có rất nhiều trường hợp sinh ra lỗ hông do không đủ năng lực, hạ tầng về an toàn thông tin.

* Để có thể nhanh chống lấp những lỗ hổng phòng tránh rỏ rỉ thông tin khách hàng, có một vài biện pháp sau:

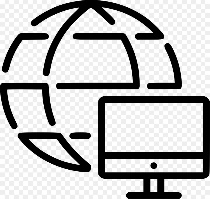
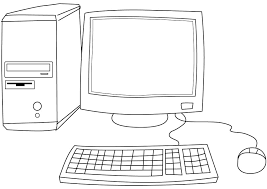
+ Để tăng cường đảm bảo an ninh bảo mật thông tin ngân hàng, các ngân hàng nhà nước nên đưa vào áp dụng khung đánh giá rủi ro công nghẹ thông tin theo thông lệ quốc tế để nâng cao chất lượng công tác kiểm tra tuân thủ các quy định về an toàn bảo mật tại các tổ chức ngân hàng

+ Sử dụng các phân mềm ngăn chặn hành vi xâm nhập hệ thống, các phần mềm này được tích hợp với hệ điều hành của máy chủ , chương trình theo dõi các hành vi trong thời gian thực, đối với các hành động có hại thì sẽ ngăn chặn, chấm dứt hoặc tìm kiếm

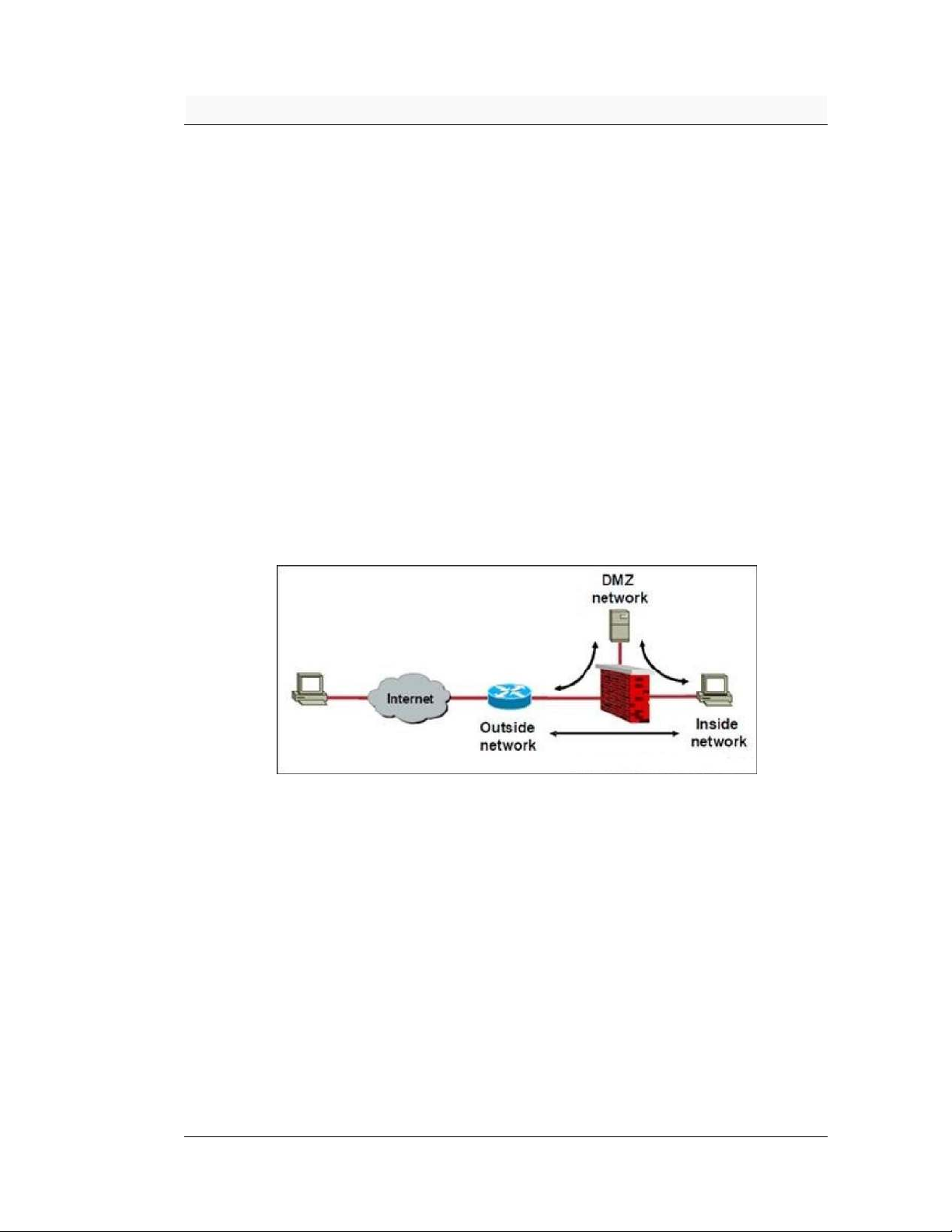
# **CHƯƠNG 2: CÁC PHƯƠNG ÁN**

## **Phương án 1: Tường lửa**

* Bức tường lửa phát triển mạnh mẽ, được ứng dụng trong các các hệ thống thông tin. Bây giờ mọi người đều muốn lên Internet và các mạng liên kết với nhau. Vì vậy cần quan tâm thường xuyên về an toàn. Không dễ dàng bảo vệ từng hệ thống trong tổ chức. Thông thường sử dụng bức tường lửa, cung cấp vòng bảo vệ như một phần của chiến lược an toàn toàn diện.
* Là điểm cổ chai để kiểm soát và theo dõi. Các mạng liên kết với độ tin cậy khác nhau, buộc có hạn chế trên các dịch vụ của mạng. Chẳng hạn, vận chuyển phải có giấy phép. Kiểm tra và kiểm soát truy cập, có thể cài đặt cảnh báo các hành vi bất thường. Cung cấp bảng NAT và sử dụng theo dõi giám sát. Cài đặt mạng riêng ảo (VPN) sử dụng cơ chế an toàn IPSec. Có thể miễn dịch trước
* Thực hiện thiết lập giả định một tường lửa ngăn cách giữ internet và pc của chi nhánh ngân hàng

* Mô hình một firewall cơ bản



* Nguyên lý hoạt động: Khi nói tới việc lưu thông dữ liệu giữa các mạng với nau thông qua firewall thì điều đó có nghĩa rằng firewall hoạt động chặt chẽ với giao thức TCP/IP. Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này dựa trên các thông tin ở đầu mỗi packet, dùng để cho phép truyền các packet đó ở trên mạng.
* Nếu luật lệ lọc packet được thỏa mãn thì packet được chuyển đi qua firewall. Nếu không packet sẽ bị bỏ đi. Nhờ vậy mà firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó mới được phép chạy trên hệ thống mạng cục bộ

*Ưu điểm của phương án tường lửa*

*Quản lý và điều khiển luồng dữ liệu trên mạng*

* Việc đầu tiên và cơ bản nhất mà tất cả các firewall đều có là quản lý và kiểm soát luồng dữ liệu trên mạng, firewall kiểm tra các gói tin và giám sát các kết nối đang thực hiện và sau đó lọc các kết nối dựa trên kết quả kiểm tra gói tin và các kết nối được giám sát

+ Packet inspection (kiểm tra gói tin)

+ Packet inspection (kiểm tra gói tin)

+ Connections và state ( kết nối và trạng thái)

+ Stateful Packet Inspection(giám sát gói tin theo trạng thái)

*Xác thực quyền truy cập*

* Firewall có thể xác thực quyền truy cập bằng nhiều cơ chế xác thực khác nhau.
* Thứ nhất, firewall có thể yêu cầu username và password của người dùng khi người dùng truy cập (thường được biết đến như là extended authentication hoặc xauth). Sau khi firewall xác thực xong người dùng, firewall cho phép người dùng thiết lập kết nối và sau đó không hỏi username và password lại cho các lần truy cập sau (thời gian firewall hỏi lại username và password phụ thuộc vào cách cấu hình của người quản trị)
* Thứ hai, firewall có thể xác thực người dùng bằng certificates và public key. Thứ ba, firewall có thể dùng pre-shared keys (PSKs) để xác thực người dùng.

*Hoạt động như một thiết bị trung gian*

* Khi user thực hiện kết nối trực tiếp ra bên ngoài sẽ đối mặt với vô số nguy cơ về bảo mật như bị virus tấn công, nhiễm mã độc hại… do đó việc có một thiết bị trung gian đứng ra thay mặt user bên trong để thực hiện kết nối ra bên ngoài là cần thiết để đảm bảo an toàn. Firewall được cấu hình để thực hiện chức năng này và firewall được ví như một proxy trung gian.

*Bảo vệ tài nguyên*

* Nhiệm vụ quan trọng nhất của một firewall là bảo vệ tài nguyên khỏi các mối đe dọa bảo mật. Việc bảo vệ này được thực hiện bằng cách sử dụng các quy tắc kiểm soát truy cập, kiểm tra trạng thái gói tin, dùng application proxy hoặc kết hợp tất cả để bảo vệ tài nguyên khỏi bị truy cập bất hợp pháp hay bị lạm dụng. Tuy nhiên, firewall không phải là một giải pháp toàn diện để bảo vệ tài nguyên của chúng ta

*Ghi nhận và báo cáo các sự kiện*

* Ta có thể ghi nhận các sự kiện của firewall bằng nhiều cách nhưng hầu hết các firewall sử dụng hai phương pháp chính là syslog và proprietaty logging format. Bằng cách sử dụng một trong hai phương pháp này, chúng ta có thể dễ dàng báo cáo các sự kiện xảy ra trong hệ thống mạng

*Hạn chế của phương án tường lửa*

* Không bảo vệ được các tấn công đi vòng qua nó, chẳng hạn mạng lén lút, thiết bị modems. Nó ngăn cản cả các tổ chức tin cậy và dịch vụ tin cậy (SSL/SSH).
* Không bảo vệ chống các mối đe dọa từ bên trong, chẳng hạn như những nhân viên bực tức hoặc thông đồng với kẻ xấu.
* Không thể bảo vệ chống việc truyền các chương trình hoặc file nhiễm virus, vì có phạm vi rất rộng các dạng file và các hệ điều hành

## ***Phương án 2: Mã hóa dữ liệu***

* Phương thức mã hóa hiện nay đang là phương thức bảo mật thông tin một cách tối ưu nhất. Mã hóa làm xáo trộn dữ liệu chỉ để hai bên trao đổi thông tin có thể hiểu được. Về mặt kỹ thuật đó là quá trình chuyển đổi văn bản gốc sang mã hóa. Mã hóa yêu cầu sử dụng khóa mã hóa( đây là một tập hợp các giá trị toán học mà cả người gửi và người nhận tin nhắn được mã hóa đều biết)
* Hiện nay thuật toán AES được sử dụng nhiều trong việc bảo mật thông tin bằng cách mã hóa. Đây là một thuật toán mã hóa khối đối xứng được chính phủ Hoa Kì áp dụng làm tiêu chuẩn mã hóa, được chấp thuận làm tiêu chuẩn liên bang bởi Viện công nghệ và tiêu chuẩn quốc gia Hoa Kỳ(NIST) sau một quá trình tiêu chuẩn hóa kéo dài 5 năm
* AES sử dụng mạng thay thế- hóa vị, có thể dễ dàng thữ hiện với tốc độ cao bằng phần mềm hoặc phần cứng cà không đòi hỏi quá nhiều bộ nhớ.
* Đặc tả thuật toán AES

+ Đối với thuật toán AES, độ dài của khối đầu vào, khối đầu ra và trạng thái là 128 bít, số các cột (các từ có độ dài 32 bít) tạo nên trạng thái là Nb = 4.

* Trong thuật toán AES, độ dài khóa mã K có thể là 128, 192 hay 256 bít. Độ dài khóa được biểu diễn bằng Nk = 4, 6 hoặc 8 thể hiện số lượng các từ 32 bít (số cột) của khóa mã.
* Đối với thuật toán AES, số vòng được thay đổi trong quá trình thực hiện thuật toán phụ thuộc vào kích cỡ khóa. Số vòng này được ký hiệu là Nr. Nr = 10 khi Nk = 4, Nr = 12 khi Nk = 6 và Nr = 14 khi Nk = 8.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Độ dài khóa | Kích thước khối | Số lần lặp |
| AES 128 | 4 | 4 | 10 |
| AES 196 | 6 | 4 | 12 |
| AES 256 | 8 | 4 | 14 |

* Mô hình mã hóa đối xứng



*Ưu điểm của phương án mã hóa:*

* Có thể che đậy nội dung của văn bản rõ: để đảm bảo sao cho chỉ người chủ hợp pháp của thông tin mới có quyền truy cập thông tin, hay nói cách khách là chống truy nhập không đúng quyền hạn
* Tạo các yếu tố xác thực thông tin: đảm bảo thông tin lưu hành trong hệ thống đền người nhận hợp pháp là xác thực. Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để rò rỉ thông tin
* Có thể đánh giá được độ phức tạp tín toán phải giải quyết bài toán để lấy được thông của dữ liệu đã được mã hóa
* Cực kì an toàn: Khi sử dụng một thuật toán an toàn, mã hóa có thể được bảo mật tuyệt đối
* . Việc mã hóa và giải mã dữ liệu khóa đối xứng tương đối dễ thực hiện, mang lại cho người dùng hiệu suất đọc và ghi rất tốt.

*Nhược điểm của phương án mã hóa:*

* Cần phải có cách lấy khóa cho bên mà mình đang chia sẻ dữ liệu. Khóa mã hóa không phải là một chuỗi văn bản đơn giải như mật khâir. Về cơ bản chúng là những khối vô nghĩa, do đó cần phải có một cách an toàn để lấy chìa khóa cho bên kia
* Nếu như ai đó chạm tay vào một khóa, họ có thể giải mã mọi thứ được mã hóa bằng khóa đó. Khi người dùng sử dụng mã hóa đối xứng để liên lạc hai chiều, điều này có nghĩa cả hai bên của cuộc trò chuyện đều bị xâm phạm

## **Phương án 3: Đăng ký và mật khẩu**

* Mật khẩu là một trong những phương pháp bảo mật được sử dụng phổ biến nhất trên thế giới. Tài khoản đăng nhập và mật khẩu được sử dụng trên các hệ thống máy tính, tài khoản ngân hàng, ATM và rất nhiều ứng dụng khác
* Mật khẩu thường không được lưu trữ trong hệ thống dưới dạng cleartext. Theo nguyên tắc, mật khẩu sẽ được lữu trữ dưới dạng mã băm (Hash). Mã băm là mã hóa một chiều duy nhất cho một đầu vào nhất định. Các hệ thống thường sử dụng mã hóa MD5 hoặc SHA1 để mã hóa mật khẩu lưu trữ.
* Ta có thể thấy, Trong hệ điều hành Windows, mật khẩu trong hệ thống được lưu trữ trong file SAM. Còn hệ điều hành Linux thì lưu trữ chúng trong file /etc/shadow. Các file này chỉ có thể truy cập bởi quyền root hoặc Administrator

Cơ chế hoạt động:

Liên kết

Bảng lưu trữ thông tin đăng nhập

Form đăng nhập

Xác nhận

+ Tại form đăng nhập người dùng nhập vào các thông tin như sau: tên người dùng và mật khẩu.

+ Tên người dùng và mật khẩu đã đăng ký với ngân hàng trong quá trình tạo lập tài khoản và được bên ngân hàng lưu trữ trong bộ nhớ của công ty. Ở đây bảng lưu trữ thông tin đăng nhập đại diện cho bộ nhỡ của ngân hàng.

+ Trong trường hợp người dùng nhập mật khẩu và tên tài khoản không đúng với tên tài khoản và mật khấu đã đăng ký và được lưu trữ trong bộ nhớ thì ngân hàng trả về thông báo cho người dùng

+ Trường hợp người dùng nhập đúng tên tài khoản và mật khẩu ở tại form đăng nhập thì ngân hàng cấp phép cho người dùng vào được hệ thống.

* *Những phương pháp để mật khẩu trở nên an toàn hơn:*

+ Sử dụng trình quản lý mật khẩu chuyên nghiệp: Các mật khẩu thường dài, có nhiều kí tự và khó nhớ, đặc biệt là khi sử dụng từng mật khẩu riêng cho từng tài khoản. Vì vậy cần phải sử dụng một ứng dụng quản lý mật khẩu chuyên nghiệp. Nó giúp người dùng có thể truy cập và quản lý các mật khẩu khác mà nó lưu trữ.

+ Tránh sử dụng các từ, dãy số hoặc cách kết hợp dễ đoán trong mật khẩu. Không nên dùng các biệt danh, ngày sinh, địa chỉ hay bất cứ thông tin công khai nào liên quan đến người dùng để làm mật khẩu. Vì chúng dễ bị lộ trên mạng xã hội

+ Không nên dùng một mật khẩu cho nhiều tài khoản : Nếu ai đó biết được mật khẩu đó, họ gần như có thể xâm nhập vào những tài khoản khác dùng chung mật khẩu đó của người dùng

*Ưu điểm của phương án tài khoản và đăng nhập:*

+ Tài khoản và mật khẩu được sử dụng rộng rãi trên mọi nền tảng của mạng xã hội , điều này giúp phương án dễ dàng tiếp cận với người dùng hơn.

+ Cách hoạt động đơn giản nhưng hiệu quả cao, ngân hàng dễ dàng quản lý các hoạt động ra vào hệ thống của người dùng

*Nhược điểm của phương án tài khoản và mật khẩu*

+ Tài khoản và mật khẩu dễ dàng bị phá giải bởi các chiêu trò lừa đảo, mật khẩu yếu cũng là một yếu tố khiến tài khoản của người dùng bị mất.

+ Mật khẩu không được mã hóa nên dễ dàng bị nhìn lén từ trên không gian mạng, thậm chí là ở ngoài đời.

+ Mật khẩu và tài khoản khi đăng nhập được truyền trực tiếp tới máy chủ đang đăng nhập, điều này tạo cho hacker cơ hội để hack thông tin ngươid dùng

+ Nếu người dùng đăng nhầm vào máy chủ hoặc website lạ và sau đó máy chủ và website có mật khẩu của người dùng. Tạo cơ hội để tin tặc tạo các bản sao web nổi tiếp đánh cắp thông tin đăng nhập.

***Sau thử qua ba phương án trên, nhóm em quyết định chọn phương án ba: Tài khoản và mật khẩu:***

+ Phương án tường lửa là một phương án bảo mật tốt dành cho hệ thống ngân hàng, tuy nhiên nhóm em gặp khó khăn khi xây dựng mô phỏng bảo mật bằng tưởng lửa. Mô phỏng trên phần mềm cisco packet tracer chưa đủ để làm rõ vấn đề bảo mật và đối tượng cụ thể

+ Phương án mã hóa được đề cao ngay từ đầu nhưng việc thiết lập thuật toán mã hóa gặp khó khăn với lượng kiến thực hiện tại mà nhóm em đang có. Thuật toán mã hóa AES được lập trình chủ yếu bằng ngôn ngữ html ( ngôn ngữ mà nhóm em chưa ai nắm rõ) không chỉ vậy việc liên kết thuật toán mã hóa với bảng danh sách thông tin của khách hàng được thiết lập trong SQL Server gặp rất nhiều khó khăn.

+ Phương án 3: Thiết lập tài khoản và mật khẩu

* Ngôn ngữ chủ yếu được dùng trong tạo lập form đăng nhập là C#, ngôn ngữ lập trình mà nhóm em đã được tiếp xúc qua. Việc thiết lập một form đăng nhập đơn giản hơn so với hai phương án trên và đăng nhập cùng mật khẩu là một cách bảo mật được sử dụng một cách phố biến trong không gian mạng.
* Mô phỏng của phương án này dễ dàng truyền đặt thông tin tới mọi người hơn là những phương án khác
* Phương án cũng phù hợp hơn với lượng kiến thức về bảo mật thông tin mà nhóm em đã trang bị

# **CHƯƠNG 3: KẾT QUẢ THỰC HIỆN**

*Các vấn đề cần giải quyết:*

*Lựa chọn phương án để bảo mật thông tin khách hàng:*

* Phương án 1: Thất bại

+ Mô phỏng tường lửa chưa làm nổi bật được đối tượng cần bảo mật cụ thể. - Phương án còn vấp phải những khó khăn về mặt kiến thức chưa đủ, khó khăn trong việc tìm kiếm từ khóa về tường lửa trên mạng.

* Phương án 2: Thất bại

+ Thuật toán được lựa chọn khó khăn trong việc giải thích và hiểu. Kiến thức chuyên sâu về thuật toán khó tìm kiếm tren mạng và lượng kiến thức của các thành viên nhóm không đủ để lập trình phương án

* Phương án 3: Thành công

+ Phương án dễ hiểu và dễ tìm thông tin trên mạng. Được phổ biến, sử dụng rộng rãi trên các nền tàng xã hội nên việc tiếp cận kiến thức về phương án dễ dàng hơn.

*Cách bảo mật an toàn nhất hiện nay*

Mã hóa thông tin hiện đang là cách bảo mật an toàn nhất. Vận dụng những thuật toán rắc rối và khóa mà chỉ riêng người dùng biết được gần như là cách bảo mật an toàn, khó xâm nhập nhất.

* Có thể che đậy nội dung của văn bản rõ để đảm bảo sao cho nguwoif chủ hợp pháp của thông tin mới có quyền truy cập thông tin, chống truy nhập không đúng quyền hạn
* Mã hóa dữ liệu hương tới bỏa vệ dữ liệu số được lưu trên hệ thống, truyền qua internet, các mạng máy tính khác. Các ngân hàng ứng dụng công nghệ mã hóa sẽ tránh được thiệt hại khi thông tin bị lộ ra bên ngoài. Nếu kẻ có ý đồ xấu muốn đọc thông tin cũng sẽ khó lòng giải mã ngay lập tức
* Mã hóa thông tin vừa mã hòa vừa giúp nâng cao tính toàn vẹn, tính không thu hồi, xác thực thông tin.....

+ Tính toàn vẹn: sẽ đảm bảo nội dung gửi đi không bị thay đổi

+ Tính xác thực: được đảm bảo cho phép người dùng truy xuất được nguồn gốc phát của thông tin

+ Tính không thu hồi: ngăn người gửi hủy thao tác dữ liệu

*Hậu quả khi thất thoát tệp dữ liệu khách hàng*

- Việc làm thất thoát thông tin khách hàng là điều cực kỳ đáng lo ngại. Nó không chỉ gây tổn thất cho khách hàng mà còn mất đi sự uy tín cho ngân hàng trong việc bảo mật thông tin khách hàng:

+ Mất sự uy tín vốn có của ngân hàng: Trong thời đại Internet tin tức luôn được cập nhật liên tục. Nếu ngân hàng không có khả năng bảo mật thông tin khách hàng hiệu quả làm thất thoát dữ liệu khách hàng thì chắc chắn những công khai tiêu cực sẽ có thể làm hỏng danh tiếng ngân hàng vĩnh viễn. Chính vì vậy chỉ một sai lầm nhỏ cũng khiến khách hàng quay lưng với ngân hàng.

+ Doanh thu giảm trầm trọng: Khi ngân hàng có lỗ hổng trong bảo mật thông tin khách hàng cho dù đó có là sự cố mất mạng lỗi ổ cứng hay phần mềm hoặc có cuộc tấn công mạng bất ngờ. Thì các dữ liệu bị mất có thể tốn đến hàng giờ hoặc có khi là mất nhiều ngày để khôi phục điều đó sẽ khiến ngân hàng sụt giảm về doanh số cũng như bị ngưng hoạt động nguồn lực để tập trung khắc phục.

+ Vướng vào rắc rối pháp lý: Việc thất thoát dữ liệu sẽ khiến ngân hàng phải đối mặt với nhiều vấn đề về pháp lý và kiện tụng. Nếu là dữ liệu khách hàng ngân hàng có thể đối mặt với tiền phạt vì không tuân thủ luật cũng như quy định liên quan đến bảo mật thông tin khách hàng. Bị cuốn vào những cuộc chiến pháp lý này sẽ khiến ngân hàng trở nên tồi tệ và giảm uy tín với khách hàng.

+ Ngân hàng đi tới thất bại: Việc không bảo mật thông tin khách hàng tốt sẽ tác động đến kinh tế và tài chính đối với ngân hàng. Hậu quả lớn nhất ngân hàng gặp phải là dừng toàn bộ hoạt động của ngân hàng.

# **CHƯƠNG 4: KẾT LUẬN, KIẾN NGHỊ**

* Trong khoảng thời gian thực hiện đề tài, chúng em đã thực hiện thử nghiểm thiết lập mô hình tường lửa giả định trên cisco packet và mang lại kết quả không được như mong đợi. Thử nghiệm không làm nổi bật được rõ tính bảo mật đối với đối tượng cụ thể ở đây là thông tin của khách hàng
* Bảo mật luôn là một đề tài nóng đối với thời đại công nghiệp hóa hiện đại hóa như ngày nay, thời đại mà con người ta phần lớn thời gian được dùng vào các thiết bị điện tử. Công nghệ ngày càng được áp dụng vào ngân hàng để thuận tiện, tiện lợi hơn trong việc quản lý thông tin của ngân hàng và nắm bắt tài khoản của bản thân dối với đối tác ngân hàng. Nhận thức được điều đó chúng em đã thực hiện bảo mật bằng phương pháp đăng ký và mật khẩu, đây không phải là một phương pháp mới mẻ và tân tiến nhất nhưng nó lại phù hợp nhất với kiến thức hạn hẹp mà chúng em có. Không chỉ vậy, phương pháp này cũng là một phương pháp bảo mật tốt và được áp dụng rộng rãi hầu hết trên các trang web, app,phần mềm v...v... độ bao phủ của nó rộng khắp trên không gian mạng.
* Sau những lần thử nghiệm thất bại có, thành công có, các thành viên trong nhóm đã trau dồi nhiều hơn kiến thức về bảo mật thông tin trên thế giới hiện nay, các biện pháp bảo mật có thể áp dụng trong thực tế cuộc sống.
* Hiện nay, công nghệ thông tin ngày càng phát triển mạnh mẽ. Việc áp dụng tốt các hình thức phát triển thông qua công nghệ số sẽ giúp ngân hàng phát triển mạnh mẽ hơn. Cũng như là một điều không thể thiếu trong hoạt động của ngân hàng hiện nay. Vì vậy việc bảo mật thông tin khách hàng của một chi nhánh ngân hàng hay là của toàn bộ ngân hàng đều quan trọng và thực sự cần thiết. Bảo mật thông tin khách hàng càng an toàn thì khách hàng càng an tâm khi sử dụng ngân hàng và đồng thời càng thu hút nhiều khách hàng sử dụng các dịch vụ của ngân hàng hơn. An toàn khi bảo mật thông tin khách hàng sẽ làm tăng sự uy tín của ngân hàng đối với người sử dụng dịch vụ ngân hàng. Ngoài ra, khách hàng phải giữ bảo mật thông tin tài khoản ngân hàng và các giấy tờ liên quan.

***Tài liệu tham khảo***

Đề tài: Giải pháp bảo mật thông tin khách hàng trong thanh toán trực tuyến tại ngân hàng nông nghiệp và phát triển nông thôn Việt Nam( Luận văn tốt nghiệp -*Đại học Thương Mại-2009)* –Nguyễn Thị Hồng Lam

Bảo mật và an toàn thông tin trong hệ thống mạng cục bộ của cơ quan nhà nước( Luận văn thạc sĩ khoa học – *Trường Đại học khoa học tự nhiên -2011) –* Phùng Thị Thanh Mai

Giáo trình an toàn và bảo mật thông tin (*Trường Đại học giao thông)*

Đề tài: Nghiên cứu triển khai hệ thống firewall ASA( Đồ án tốt nghiệp -*Đại học Văn Lang- 2017*) –Trần Văn Hiếu

Tìm hiểu về hệ mã hóa AES(*Đại học công nghiệp Hà Nội-2013*)-Phạm Đăng Hảo,Trần Văn Minh