

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM



CAO TRẦN THÁI ANH

**BẢO MẬT DỮ LIỆU TRÊN THẺ RFID
ỨNG DỤNG ĐIỂM DANH VÀ THANH TOÁN**

LUẬN VĂN THẠC SĨ

Chuyên ngành: Công nghệ thông tin

Mã số ngành: 60480201

TP. HỒ CHÍ MINH, tháng 08 năm 2015

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM**



CAO TRẦN THÁI ANH

**BẢO MẬT DỮ LIỆU TRÊN THẺ RFID
ỨNG DỤNG ĐIỂM DANH VÀ THANH TOÁN**

LUẬN VĂN THẠC SĨ

Chuyên ngành: Công nghệ thông tin

Mã số ngành: 60480201

CÁN BỘ HƯỚNG DẪN KHOA HỌC: TS. LƯU THANH TRÀ

TP. HỒ CHÍ MINH, tháng 08 năm 2015

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

Cán bộ hướng dẫn khoa học : Tiến sĩ Lưu Thanh Trà

Luận văn Thạc sĩ được bảo vệ tại Trường Đại học Công nghệ TP. HCM
ngày 15 tháng 08 năm 2015

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

TT	Họ và tên	Chức danh Hội đồng
1	PGS.TSKH. Nguyễn Xuân Huy	Chủ tịch
2	PGS.TS. Lê Hoài Bắc	Phản biện 1
3	TS. Võ Đình Bảy	Phản biện 2
4	TS. Trần Đức Khánh	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 20.....

NHIỆM VỤ LUẬN VĂN THẠC SĨ

Họ tên học viên: Cao Trần Thái Anh

Giới tính: Nam

Ngày, tháng, năm sinh: 16/01/1985

Nơi sinh: TP.HCM

Chuyên ngành: Công nghệ thông tin

MSHV: 1341860001

I- Tên đề tài:

Bảo mật dữ liệu trên thẻ RFID - Ứng dụng điểm danh và thanh toán.

II- Nhiệm vụ và nội dung:

- Tìm hiểu công nghệ RFID.
- Nghiên cứu phương pháp bảo mật dữ liệu trên thẻ RFID.
- Ứng dụng công nghệ RFID và kết quả nghiên cứu để xây dựng ứng dụng về điểm danh sinh viên và thanh toán bằng thẻ hỗ trợ offline.
- Tiến hành thực nghiệm và đánh giá.

III- Ngày giao nhiệm vụ: 18/08/2014

IV- Ngày hoàn thành nhiệm vụ: 31/05/2015

V- Cán bộ hướng dẫn: TS. Lưu Thanh Trà

CÁN BỘ HƯỚNG DẪN

KHOA QUẢN LÝ CHUYÊN NGÀNH

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

Cao Trần Thái Anh

LỜI CẢM ƠN

Tôi xin bày tỏ lời cảm ơn chân thành và sâu sắc nhất tới Tiến Sĩ Lưu Thanh Trà đã tận tâm, nhiệt tình chỉ bảo, hướng dẫn tôi trong suốt quá trình thực hiện luận văn thạc sĩ này.

Tôi xin chân thành cảm ơn Ban Giám hiệu, Phòng Sau đại học, các thầy cô khoa Công nghệ thông tin trường Đại học Công nghệ TP.HCM đã quan tâm và tạo điều kiện thuận lợi cho tôi hoàn thành khóa học.

Xin cảm ơn các bạn, anh chị đồng nghiệp đã tạo điều kiện về tư liệu để tôi thực hiện luận văn này.

Xin gửi lời tri ân đến gia đình, bạn bè và tất cả những người thân yêu đã luôn động viên, khích lệ, giúp đỡ tôi trong quá trình học tập và nghiên cứu.

Tác giả Luận văn

Cao Trần Thái Anh

TÓM TẮT

Công nghệ nhận dạng đối tượng bằng sóng vô tuyến RFID (Radio Frequency Identification) [1,2,3,4,5,6,7] là một kỹ thuật nhận dạng tự động cho phép một thiết bị đọc thông tin chứa trong chip ở khoảng cách xa, không cần tiếp xúc trực tiếp, dựa trên khả năng lưu trữ và nhận tín hiệu từ xa bằng hệ thống thẻ thông minh.

Với sự phát triển rất mạnh mẽ của khoa học kỹ thuật, ngày càng nhiều các công nghệ ứng dụng vào việc quản lý nhằm giảm nhẹ và tối ưu hóa công việc. Công nghệ RFID và những ứng dụng của nó là một ví dụ điển hình mang lại nhiều lợi ích cho con người.

Công nghệ RFID đang ngày càng được sử dụng nhiều trong những ứng dụng yêu cầu bảo mật cao như hệ thống kiểm soát truy cập (access system), những hệ thống thanh toán (payment system), hệ thống vé (ticket system) [8] và các ứng dụng trong môi trường nhỏ như: ứng dụng quản lý sinh viên bằng công nghệ RFID để kiểm soát an ninh, ra vào ký túc xá [15], quản lý thư viện [17].

Việc sử dụng hệ thống RFID trong các ứng dụng trên đòi hỏi phải sử dụng các phương pháp mã hóa dữ liệu trên thẻ để bảo vệ hệ thống và chống lại các cuộc tấn công của hacker với mục đích truy cập trái phép để bẻ khóa mật khẩu của tổ chức và cá nhân sử dụng hệ thống RFID. Ngoài phương pháp mã hóa, hệ thống RFID còn đòi hỏi thêm việc chèn 1 password ngay trong thẻ để trong trường hợp bị mất thẻ thì hệ thống không thực hiện được giao dịch.

Luận văn tập trung nghiên cứu các thuật toán mã hóa, chọn một thuật toán phù hợp để bảo mật dữ liệu trên thẻ RFID. Xây dựng 2 ứng dụng cụ thể là điểm danh sinh viên thay cho việc điểm danh theo phương pháp truyền thống và thanh toán với giá trị nhỏ tại căn tin.

ABSTRACT

Nowadays, Information Technology has become a main key to support the development of our society in many facts, especially in business. It helps human to have a more comfortable and secured life. As same as other technologies, Radio-frequency identification (RFID) is the one of most efficient technologies in information management today.

RFID technology is used frequently in those applications which require high security (access system, payment system, ticket system, etc...) and also in some small applications such as: library management system, student management system, university access system.

Due to the wide deployment of RFID over the world, there emerges need to protect RFID card's information safety from hackers.

This project focus on researching security algorithms. Base on the characteristic of those security algorithms, the research will choose an appropriate algorithm to apply it into RFID card. The results of this work are to create two applications - checking student's attendance application and payment system by using RFID technology.

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
TÓM TẮT	iii
MỤC LỤC.....	v
DANH MỤC CÁC TỪ VIẾT TẮT	ix
DANH MỤC CÁC BẢNG.....	x
DANH MỤC CÁC HÌNH ẢNH	xi
CHƯƠNG 1: TỔNG QUAN.....	1
1.1. Lý do chọn đề tài	1
1.2. Yêu cầu, nội dung và phương pháp nghiên cứu	3
1.2.1. Yêu cầu của đề tài.....	3
1.2.2. Nội dung và phương pháp nghiên cứu.....	4
1.3. Ý nghĩa khoa học và thực tiễn	5
1.3.1. Điểm mới của đề tài.....	5
1.3.2. Dự kiến kết quả đạt được.....	5
1.4. Tổng quan về lĩnh vực nghiên cứu	6
1.4.1. Tình hình nghiên cứu trên thế giới	6
1.4.2. Tình hình nghiên cứu trong nước	6
1.5. Cấu trúc của luận văn	7
CHƯƠNG 2: CÔNG NGHỆ RFID	8
2.1. Giới thiệu về công nghệ RFID	8
2.2. Các thành phần của hệ thống RFID.....	8
2.3. Phương thức hoạt động.....	10
2.4. Ưu điểm và hạn chế của hệ thống RFID	12
2.5. Thẻ RFID	13
2.5.1. Khái niệm.....	13
2.5.2. Các thông số của thẻ	14
2.5.2.1. Dung lượng	14

2.5.2.2.	Tần số hoạt động	14
2.5.3.	Các thuộc tính của thẻ RFID	16
2.5.4.	Giao thức thẻ.....	16
2.5.5.	Phân loại thẻ.....	17
2.5.5.1.	Phân loại theo vai trò	18
2.5.5.2.	Phân loại thẻ dựa vào khả năng ghi dữ liệu trên thẻ	19
2.5.6.	Cách lựa chọn thẻ	20
2.6.	Các thiết bị Mifare RFID của Soyal	21
2.6.1.	Thẻ thụ động Mifare	21
2.6.1.1.	Giới thiệu	21
2.6.1.2.	Đặc điểm các loại thẻ Mifare	21
2.6.1.3.	Tính năng	23
2.6.2.	Đầu đọc Mifare Soyal AR-721H	24
2.6.2.1.	Khái niệm.....	24
2.6.2.2.	Đặc điểm và phương thức hoạt động	24
2.6.2.3.	Thông số kỹ thuật.....	25
2.6.3.	Đầu ghi Mifare Soyal AR-737P	25
2.6.3.1.	Giới thiệu	25
2.6.3.2.	Đặc điểm	25
2.6.3.3.	Thông số kỹ thuật.....	26
2.6.4.	Ứng dụng	26
2.6.5.	Lý do chọn thiết bị Mifare của Soyal	26
2.7.	Chuẩn truyền thông giữa thẻ và đầu đọc	27
CHƯƠNG 3: MÃ HÓA DỮ LIỆU		29
3.1.	Tổng quan về mã hóa.....	29
3.1.1.	Khái niệm về mã hóa	29
3.1.2.	Độ an toàn của thuật toán	30
3.1.3.	Ba mục tiêu chính của an toàn thông tin.....	30
3.1.4.	Phân loại các thuật toán mã hóa	31
3.2.	Phương pháp mã hóa dữ liệu trên thẻ RFID.....	32
3.2.1.	Hashing – Hàm băm	32
3.2.2.	Hàm băm MD5	33

3.2.2.1. Giới thiệu	33
3.2.2.2. Giải thuật.....	33
3.2.2.3. Ứng dụng.....	36
3.2.3. Hàm băm SHA-1	36
3.2.3.1. Giới thiệu	36
3.2.3.2. Giải thuật.....	36
3.2.3.3. Ứng dụng.....	39
3.2.4. So sánh 2 phương pháp mã hóa	39
3.2.5. Khả năng chống tấn công.....	40
3.2.6. Phương pháp mã hóa	42
3.2.6.1. Hệ thống thẻ Mifare	42
3.2.6.2. Phương pháp mã hóa.....	44
CHƯƠNG 4: XÂY DỰNG HỆ THỐNG	49
4.1. Yêu cầu hệ thống	49
4.1.1. Mô hình hệ thống.....	49
4.1.2. Yêu cầu chức năng.....	49
4.1.2.1. Chức năng cho sinh viên.....	49
4.1.2.2. Chức năng cho Quản trị	50
4.1.2.3. Chức năng cho kế toán.....	50
4.1.3. Yêu cầu phi chức năng.....	50
4.2. Thiết kế dữ liệu.....	51
4.2.1. Sơ đồ dữ liệu	51
4.2.2. Mô tả dữ liệu	51
4.3. Mô hình thực hiện.....	53
4.3.1. Ghi thông tin vào thẻ	53
4.3.2. Ghi thông tin nạp tiền	54
4.3.3. Điểm danh sinh viên	55
4.3.4. Thanh toán	56
4.4. Môi trường cài đặt và các công nghệ sử dụng.....	57
CHƯƠNG 5: KẾT QUẢ ĐẠT ĐƯỢC	58
5.1. Giao diện thiết kế.....	58
5.1.1. Giao diện quản trị thẻ.....	58

5.1.2.	Giao diện điểm danh sinh viên	63
5.1.3.	Giao diện thanh toán bằng thẻ tại căn tin	64
5.2.	Triển khai.....	71
5.3.	Thử nghiệm hệ thống.....	72
5.4.	Kết quả đạt được và hướng phát triển	72
5.4.1.	Kết quả đạt được	72
5.4.2.	Hướng phát triển	73
5.5.	Kết luận.....	73

DANH MỤC CÁC TỪ VIẾT TẮT

RFID (Radio Frequency Identification): nhận dạng đối tượng bằng sóng vô tuyến

RF (Radio frequency): tần số sóng vô tuyến

LF (Low-frequency): tần số thấp

HF (High-frequanecy): tần số cao

UHF (Ultrahigh-frequency): siêu cao tần

DANH MỤC CÁC BẢNG

Bảng 2.1 – So sánh hệ thống RFID với các hệ thống khác [26]	13
Bảng 2.2 – Tần số hoạt động cho các thẻ Passive.....	15
Bảng 2.3 – Các thông số của thẻ thủ động Mifare	23
Bảng 3.1 - So sánh các thông số của các thuật toán hàm băm an toàn [24]	40
Bảng 3.2 – Luồng dữ liệu bên trong hệ thống thẻ Soyal RFID	46

DANH MỤC CÁC HÌNH ẢNH

Hình 1.1 – Mô hình điểm danh sinh viên.....	1
Hình 1.2 – Mô hình thanh toán tại căn tin	2
Hình 2.1 - Cấu trúc thẻ.....	8
Hình 2.2 - Một số mẫu thẻ thông dụng	9
Hình 2.3 - Reader	9
Hình 2.4 - Mô hình hệ thống RFID.....	10
Hình 2.5 - Hoạt động của thẻ và đầu đọc RFID.....	12
Hình 2.6 - Thủ tục master-slaver giữa Application, đầu đọc và thẻ	24
Hình 2.7 – Thông số kỹ thuật đầu đọc Mifare Soyal AR-721H [21].....	25
Hình 2.8 – Thông số kỹ thuật đầu đọc Mifare Soyal AR-737P [22]	26
Hình 3.1 – Quy trình mã hóa dữ liệu [27].....	29
Hình 3.2 - Hệ thống mã hóa thông tin [27]	29
Hình 3.3 - Tam giác bảo mật C-I-A	30
Hình 3.4 – Hệ thống thẻ RFID [19]	43
Hình 3.5 – Cấu trúc thẻ RFID [19]	43
Hình 3.6 – Mô hình mã hóa dữ liệu chung	45
Hình 3.7 – Sơ đồ mã hóa dữ liệu [32].....	47
Hình 4.1 – Mô hình hệ thống	49
Hình 4.2 – Sơ đồ dữ liệu	51
Hình 4.3 – Mô hình ghi thông tin vào thẻ.....	53
Hình 4.5 – Mô hình ghi thông tin nạp tiền.....	54
Hình 4.4 – Mô hình điểm danh sinh viên.....	55
Hình 4.6 – Mô hình thanh toán	56

Hình 5.1 – Giao diện đăng nhập.....	58
Hình 5.2 – Giao diện quản trị thẻ.....	58
Hình 5.3 – Giao diện phát hành thẻ.....	59
Hình 5.4 – Giao diện cập nhật thông tin thẻ	60
Hình 5.5 – Giao diện hủy thẻ	61
Hình 5.6 – Giao diện nạp tiền	63
Hình 5.7 – Giao diện điểm danh	64
Hình 5.8 – Giao diện thanh toán	66

CHƯƠNG 1: TỔNG QUAN

1.1. Lý do chọn đề tài

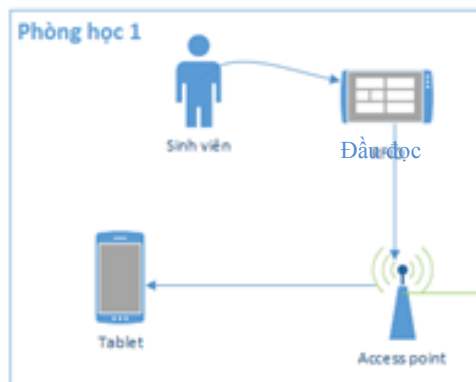
Công nghệ RFID đang ngày càng được sử dụng nhiều trong những ứng dụng yêu cầu bảo mật cao như hệ thống kiểm soát truy cập (access system), những hệ thống thanh toán (payment system), hệ thống vé (ticket system). Các ứng dụng của RFID ngày càng được mở rộng trong mọi lĩnh vực, trong đó môi trường giáo dục là một điển hình.

Quản lý điểm danh sinh viên theo phương pháp truyền thống là một phương pháp mất rất nhiều thời gian của giảng viên và sinh viên (nếu dạy tập trung ở hội trường, có cả hàng trăm SV); Dữ liệu không tập trung do nhiều lớp học tại nhiều thời điểm khác nhau, khó khăn trong việc tổng kết dữ liệu (ghi nhiều lần).

Sinh viên phải đứng xếp hàng dài để chờ mua thức ăn, trả tiền mặt và chờ hoàn lại tiền dư tại căn tin trong giờ giải lao (30 phút), mất nhiều thời gian và tạo ra cảm giác mệt mỏi cho sinh viên.

Luận văn nhằm tiến đến việc:

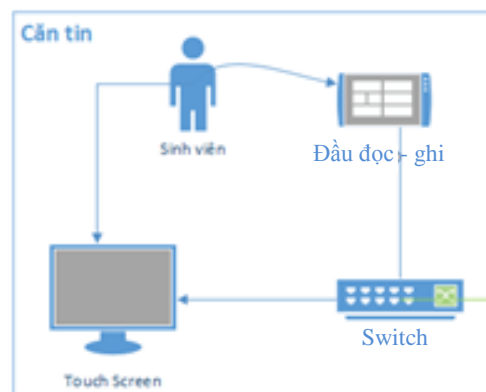
- Xây dựng mô hình quản lý điểm danh sinh viên, sử dụng hệ thống RFID gồm các thiết bị như hình 1.1 với mục đích quản lý các thông tin cá nhân của sinh viên một cách nhanh chóng, chính xác; Dữ liệu tập trung, tiết kiệm thời gian và công sức cho tính nhất quán của dữ liệu (chỉ ghi 1 lần).



Hình 1.1 – Mô hình điểm danh sinh viên

Với mô hình điểm danh, sinh viên thực hiện việc tấp thẻ RFID vào đầu đọc được đặt tại các phòng học. Đầu đọc đọc dữ liệu ghi thông tin của sinh viên trong thẻ và truyền thông tin đến các thiết bị hiển thị (lưu ý vẫn chọn sử dụng thiết bị tablet) thông qua 1 access point (làm nhiệm vụ giao tiếp giữa đầu đọc và tablet, sau đó thông tin của sinh viên được hiển thị trên màn hình tablet. Hệ thống có thể hoạt động được offline (hệ thống vẫn thực hiện điểm danh mà không cần kết nối với máy chủ. Dữ liệu sẽ được lưu tạm thời tại tablet).

- Xây dựng mô hình thanh toán tại căn tin, sử dụng hệ thống RFID gồm các thiết bị như hình 1.2 để quản lý quá trình thực hiện giao dịch (chọn món ăn và thanh toán) của sinh viên nhằm tiết kiệm thời gian.



Hình 1.2 – Mô hình thanh toán tại căn tin

Với mô hình thanh toán tại căn tin, thông tin về món ăn và nước uống được hiển thị trên màn hình touch screen. Sinh viên thực hiện việc chọn món và nước uống trên màn hình và tấp thẻ RFID vào đầu đọc-ghi được đặt tại căn tin để xác nhận thanh toán. Đầu đọc-ghi đọc dữ liệu giao dịch trên thẻ và lưu thông tin giao dịch vào máy tính điều khiển màn hình touch screen. Đầu đọc-ghi và máy tính giao tiếp với nhau thông qua thiết bị giao tiếp switch. Hệ thống có thể hoạt động được offline (hệ thống vẫn thực hiện điểm danh mà không cần kết nối với máy chủ. Dữ liệu sẽ được lưu tạm thời tại máy tính).

- Ngoài ra, để dữ liệu trên thẻ được bảo mật, chống mất thẻ, chống sao chép thẻ thì hệ thống phải sử dụng các phương pháp mã hóa và kết hợp chèn 1 password ngay trong thẻ.

Vấn đề này đã và đang được nhiều tổ chức, trường học cũng như cá nhân quan tâm và tham gia nghiên cứu. Nắm bắt được xu thế và sự quan tâm đó, cộng với niềm đam mê trong lĩnh vực tìm hiểu bảo mật hệ thống, tôi đã chọn đề tài: **“BẢO MẬT DỮ LIỆU TRÊN THẺ RFID - ỨNG DỤNG ĐIỂM DANH VÀ THANH TOÁN”**

1.2. Yêu cầu, nội dung và phương pháp nghiên cứu

1.2.1. Yêu cầu của đề tài

Với hai mô hình trên thì hệ thống RFID cần thực hiện và đảm bảo các yêu cầu dự kiến sau:

- Xây dựng hệ thống RFID gồm 2 ứng dụng mẫu là điểm danh và thanh toán nhằm hỗ trợ cho sinh viên thực hiện điểm danh và thanh toán với số tiền nhỏ tại căn tin.
- Hệ thống phải được bảo mật: dữ liệu ghi trên thẻ RFID của người dùng phải được đảm bảo trong quá trình sử dụng. Trong trường hợp thẻ bị sao chép hoặc bị mất thẻ thì đảm bảo hệ thống không thực hiện được giao dịch.
- Hệ thống có thể hoạt động được offline: trong một số trường hợp tín hiệu giữa đầu đọc hoặc đầu ghi và máy chủ lưu trữ dữ liệu bị mất liên lạc thì đảm bảo vẫn thực hiện được giao dịch.

Để có thể đáp ứng được các yêu cầu trên thì hệ thống RFID dự kiến ứng dụng các công nghệ và phương pháp sau:

- Hệ thống RFID gồm: đầu đọc, đầu ghi và thẻ.
- Tần số hoạt động của đầu đọc: 13.56MHz.
- Khoảng cách đọc: 2-5cm

- Thời gian đáp ứng: là thời gian đọc dữ liệu trên thẻ của đầu đọc, thời gian thực hiện càng nhanh càng tốt để tránh tình trạng phải chờ đợi. Dự kiến thời gian điểm danh là 1 giây, thời gian thanh toán 3 giây.
- Bảo mật: sử dụng các phương pháp mã hóa có độ dài dữ liệu xử lý nằm trong khoảng từ 128 bit đến 160 bit và kết hợp chèn 1 password ngay trong thẻ RFID để trong trường hợp mất thẻ hoặc thẻ bị copy, thì không thực hiện được giao dịch.
- Hệ thống offline: Dữ liệu được lưu trữ tạm thời tại các thiết bị đặt tại phòng học và đặt tại căn tin, khi hệ thống online dữ liệu sẽ tự động đồng bộ.

1.2.2. Nội dung và phương pháp nghiên cứu

- Tìm hiểu chung về công nghệ RFID và công nghệ RFID của Soyal [19].
- Tìm hiểu về tần số hoạt động của thẻ, chuẩn truyền thông giữa đầu đọc và thẻ, khảo sát thực tế môi trường lắp đặt để chọn thiết bị phù hợp.
- Tìm hiểu các thuật toán mã hóa để mã hóa dữ liệu trên thẻ RFID nhằm bảo vệ những thông tin cá nhân của người dùng lưu trên thẻ được an toàn và bảo mật.
- Nghiên cứu về vấn đề bảo mật thông tin trên thẻ và phương pháp xác thực đối xứng (Mutual Symmetrical Authentication) giữa đầu đọc (reader) và thẻ RFID (transponder) để chống lại việc lấy cắp thẻ bằng cách chèn 1 password vào ngay trong thẻ. Để thông tin được bảo mật phải đảm bảo ba mục tiêu bảo mật C-I-A: Đảm bảo tính bí mật của thông tin (Confidentiality); Đảm bảo tính toàn vẹn của thông tin (Integrity); Đảm bảo độ sẵn sàng của thông tin (Availability).
- Tìm hiểu ngôn ngữ lập trình trên nền .Net, Java và các phương pháp kết nối CSDL nhằm xây dựng một CSDL hoàn chỉnh chứa các thông tin cơ bản về sinh viên và các món ăn tại căn tin.

- Xây dựng một phần mềm cho người dùng có thể truy xuất các thông tin liên quan đến điểm danh sinh viên và cách thức chọn món tại căn tin.
- Cập nhật lại các thông tin về sinh viên và thông tin về các món ăn tại căn tin để đáp ứng nhu cầu sử dụng.

1.3. Ý nghĩa khoa học và thực tiễn

1.3.1. Điểm mới của đề tài

- Hai ứng dụng trên giúp cho con người có thể giám sát, quản lý dễ dàng hơn, ít mắc lỗi, tốn ít thời gian và giảm thiểu nhân lực quản lý. Đặc biệt là hệ thống sử dụng được offline. Ứng dụng có khả năng xử lý tự động việc điểm danh sinh viên và tạo sự tiện lợi trong việc thanh toán của người dùng khi sử dụng các dịch vụ tại căn tin.
- Mã hóa được dữ liệu trên thẻ và chèn 1 password ngay trên thẻ nhằm bảo vệ người dùng trong việc bảo mật thông tin và chống mất thẻ, chống lại việc thay đổi, sao chép dữ liệu trên thẻ.

1.3.2. Dự kiến kết quả đạt được

- Xây dựng và chạy thành công hai ứng dụng quản lý sinh viên và thanh toán tại căn tin.
- Bảo mật (Security): Dữ liệu trên thẻ được hash đảm bảo tính toàn vẹn của dữ liệu, chống thay đổi dữ liệu trên thẻ.
- Hiệu suất (Performance): Thời gian thực hiện điểm danh 1 giây, thanh toán khoảng 3 giây.
- Tính sẵn sàng (Availability): Hoạt động 24/ 24, hệ thống sử dụng offline.
- Tiện dụng (Usability): Dễ sử dụng, số lượng thao tác ít.
- Triển khai ứng dụng thực tế cho cơ quan/doanh nghiệp.

1.4. Tổng quan về lĩnh vực nghiên cứu

1.4.1. Tình hình nghiên cứu trên thế giới

Công nghệ RFID đã được các quốc gia trên thế giới ứng dụng rộng rãi trong các lĩnh vực an ninh, kinh doanh, ngân hàng, y học, ..., điển hình tại một nước như:

Tại Mỹ: Các nhà khoa học Mỹ vừa tìm ra cách gắn chip nhận dạng tần số vô tuyến (RFID) vào giấy dùng để in tiền, tài liệu pháp lý, vé và nhãn dán thông minh khác với mục tiêu tránh giả mạo [9]. Ngoài ra, công nghệ RFID còn được tích hợp trên thẻ tín dụng, thẻ visa, nhà ga, tàu điện ngầm, sân bay, gắn chip RFID trên học sinh,... [10]

Tại Hàn Quốc: công nghệ RFID đang được vào cuộc sống trong các dịch vụ: S-Oil, Bưu chính, theo dõi hải sản, ... [11]

Malaysia: ứng dụng công nghệ RFID vào hệ thống tàu điện [12] và rất nhiều quốc gia khác trên thế giới đã và đang sử dụng công nghệ RFID

1.4.2. Tình hình nghiên cứu trong nước

Việt Nam đã từng bước ứng dụng các tiện ích của công nghệ RFID. Điển hình như công ty TECHPRO Việt Nam, hợp tác cùng Hãng IDTECK – Korea ứng dụng RFID trong chấm công điện tử, kiểm soát thang máy.[13]

Viện Công nghệ Thông tin đã giới thiệu chào bán các hệ thống ứng dụng RFID như: hệ thống kiểm soát xâm thực AC200 sử dụng thẻ RFID; khóa thẻ điện tử RFID K400R; hệ thống kiểm soát vô tuyến. [13]

Tại TP. HCM, công nghệ RFID cũng đang được triển khai ứng dụng trong trạm thu phí Xa lộ Hà Nội và hệ thống kiểm soát bãi đỗ xe tự động tại hầm đậu xe tòa nhà The Manor... Bãi giữ xe thông minh tại các trung tâm thương mại, bệnh viện, siêu thị Coopmark... [14]

Các ứng dụng của công nghệ RFID trong giáo dục như: Đại học Bách khoa Hà Nội với ứng dụng quản lý thư viện [17], Đại học Khoa học tự nhiên – Tp.HCM với ứng dụng quản lý sinh viên bằng công nghệ RFID để kiểm soát an ninh, ra vào

ký túc xá, thanh toán các loại phí cũng như khám chữa bệnh cho sinh viên, sửa chữa, lưu trữ hồ sơ, làm kênh thông tin liên lạc với nhà trường, gia đình,...[15]

Ngoài ra, còn có các đề tài đang nghiên cứu như “Nghiên cứu xây dựng hệ thống quản lý, điều hành kho thông minh Smart Warehouse dựa trên công nghệ RFID và hệ thống nhúng” (Đại học Khoa học Tự nhiên) và “Nghiên cứu công nghệ xác định, nhận dạng sử dụng RFID trên mạng Internet” (Trung tâm Internet Việt Nam). [16]

1.5. Cấu trúc của luận văn

Cấu trúc của luận văn gồm các chương chính như sau

Chương 1: Tổng quan

Nội dung của chương này Trình bày lý do chọn đề tài, mục đích, đối tượng và phạm vi nghiên cứu, ý nghĩa khoa học và thực tiễn của đề tài nghiên cứu.

Chương 2: Công nghệ RFID

Nội dung của chương này giới thiệu về công nghệ RFID nói chung và các thiết bị Mifare RFID của Soyal được sử dụng để nghiên cứu trong luận văn.

Chương 3: Mã hóa dữ liệu

Nội dung của chương này là trình bày các thuật toán mã hóa dữ liệu trên thẻ RFID; Nghiên cứu phương pháp mã hóa và chọn ra một phương pháp phù hợp để mã hóa dữ liệu trên thẻ RFID.

Chương 4: Xây dựng hệ thống

Nội dung của chương này mô tả, thiết kế, xây dựng mô hình, chức năng của hệ thống. Xây dựng môi trường cài đặt và ứng dụng các công nghệ sử dụng cho 2 ứng dụng điểm danh và thanh toán.

Chương 5: Kết quả đạt được

Nội dung của chương này là kết quả thiết kế thành công giao diện 2 ứng dụng điểm danh và thanh toán tại căn tin dựa trên quy trình xây dựng các chức năng trong chương 4. Triển khai thử 2 ứng dụng trên tại một số cơ quan/doanh nghiệp. Đánh giá kết quả đạt được so với yêu cầu ban đầu và đưa ra hướng phát triển cho hệ thống.

CHƯƠNG 2: CÔNG NGHỆ RFID

2.1. Giới thiệu về công nghệ RFID

Công nghệ RFID (Radio Frequency Identification) là công nghệ nhận dạng đối tượng bằng sóng vô tuyến, cho phép một thiết bị đọc thông tin chứa trong chip ở khoảng cách xa, không cần tiếp xúc trực tiếp, không thực hiện bất kì giao tiếp vật lý nào giữa hai vật không nhìn thấy. Công nghệ này cho ta phương pháp truyền, nhận dữ liệu từ một điểm đến một điểm khác. Ba thành phần thẻ (tag), đầu đọc (reader) và ăngten là những khối chính của một hệ thống RFID.

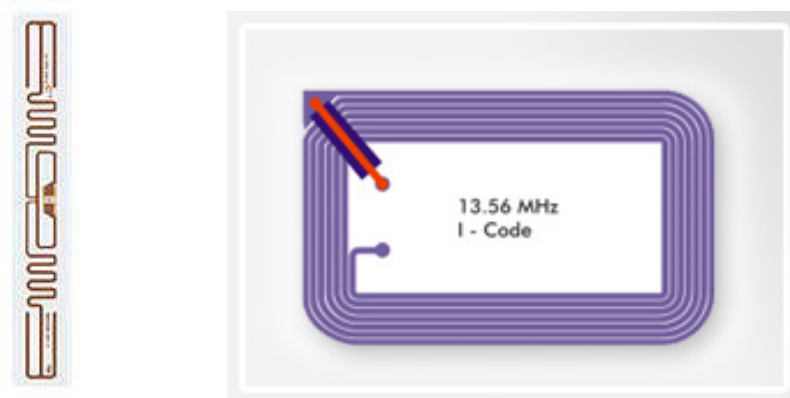
Kỹ thuật RFID sử dụng truyền thông không dây trong dải tần sóng vô tuyến để truyền dữ liệu từ các thẻ đến các đầu đọc. Tag có thể được đính kèm hoặc gắn vào đối tượng được nhận dạng chẳng hạn sản phẩm, hộp hoặc giá kê (pallet). Reader quét dữ liệu của tag và gửi thông tin đến cơ sở dữ liệu có lưu trữ dữ liệu của tag.

Sự ra đời công nghệ nhận dạng tần số vô tuyến thật sự là cuộc cách mạng trong quản lý tài sản nói chung và công nghệ đeo bám phục vụ mục đích quản lý trở thành mối quan tâm của thế giới thương mại.

2.2. Các thành phần của hệ thống RFID

Một hệ thống RFID bao gồm các thành phần sau :

Thẻ (Tag): gồm chip bán dẫn và ăngten nhỏ trong các hình thức đóng gói.



Hình 2.1 - Cấu trúc thẻ

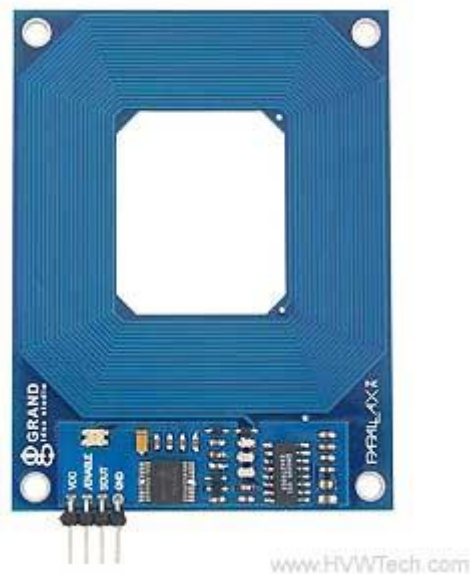
(Nguồn: Sưu tầm hình ảnh Internet)



Hình 2.2 - Một số mẫu thẻ thông dụng

(Nguồn: Sưu tầm hình ảnh Internet)

Đầu đọc (Reader): thực hiện việc ghi đọc trên thẻ và giao tiếp với máy chủ.



Hình 2.3 - Reader

(Nguồn: Sưu tầm hình ảnh Internet)

Ăngten của đầu đọc: làm nhiệm vụ bức xạ, thu sóng điện từ và gia công tín hiệu. Một vài đầu đọc hiện nay cũng đã có sẵn ăngten.

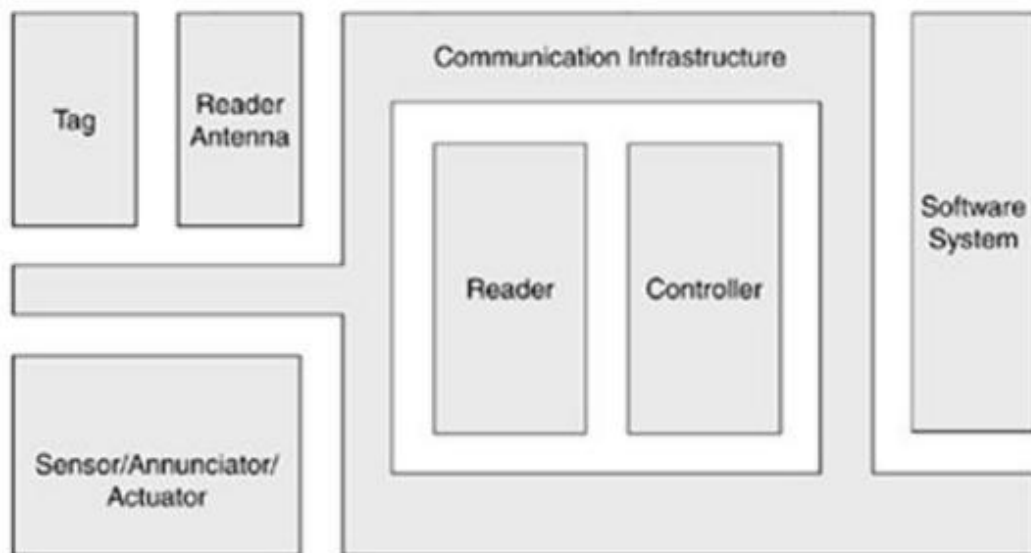
Mạch điều khiển (Controller): cho phép các thành phần bên ngoài giao tiếp điều khiển chức năng của đầu đọc và các thành phần khác như annunciation,

actuator,... Ngày nay mạch điều khiển thường được tích hợp sẵn trong đầu đọc .

Cảm biến (sensor), cơ cấu chấp hành (actuator) và bảng tín hiệu điện báo (annunciator): những thành phần này hỗ trợ nhập và xuất của hệ thống.

Máy chủ (host) và hệ thống phần mềm (software system) : về mặt lý thuyết, một hệ thống RFID có thể hoạt động độc lập không có thành phần này. Thực tế, một hệ thống RFID gần như không có ý nghĩa nếu không có thành phần này.

Cơ sở hạ tầng truyền thông (communication infrastructure) : là thành phần bắt buộc, gồm cả hai mạng có dây và không dây và các bộ phận kết nối tuần tự để kết nối các thành phần đã liệt kê ở trên với nhau để chúng truyền với nhau hiệu quả.



Hình 2.4 - Mô hình hệ thống RFID.

(Nguồn: Sưu tầm hình ảnh Internet)

2.3. Phương thức hoạt động

Một hệ thống RFID có ba thành phần cơ bản: thẻ, đầu đọc, và một máy chủ. Thẻ RFID gồm chip bán dẫn nhỏ và ăngten được thu nhỏ trong một vỏ hình thức đóng gói. Mỗi thẻ được lập trình với một nhận dạng duy nhất cho phép theo dõi không dây đối tượng hoặc con người đang gắn thẻ đó vì các chip được sử dụng trong thẻ RFID có thể giữ một số lượng lớn dữ liệu, chúng có thể chứa thông tin về đối tượng được gắn

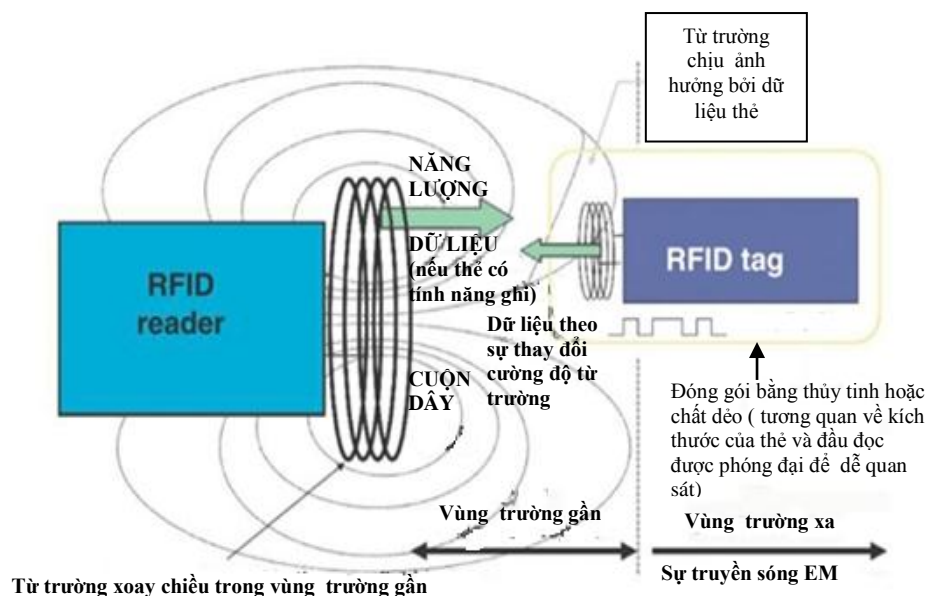
thẻ.

Hệ thống RFID sử dụng bốn băng thông tần số chính : tần số thấp (LF), tần số cao (HF), siêu cao tần (UHF) hoặc sóng cực ngắn (viba). Các hệ thống trong siêu thị ngày nay hoạt động ở băng thông UHF, trong khi các hệ thống RFID cũ sử dụng băng thông LF và HF. Băng thông viba đang được để dành cho các ứng dụng trong tương lai.

Các thẻ có thể được cấp nguồn bởi một bộ pin thu nhỏ trong thẻ (các thẻ tích cực) hoặc bởi đầu đọc, nó “wake up” (đánh thức) thẻ để yêu cầu trả lời khi thẻ đang trong phạm vi vùng đọc (thẻ thụ động).

Đầu đọc gồm một ăngten liên lạc với thẻ và một đơn vị đo điện tử học đã được nối mạng với máy chủ. Đơn vị đo tiếp sóng giữa máy chủ và tất cả các thẻ trong phạm vi đọc của ăngten, cho phép một đầu đọc liên lạc đồng thời với hàng trăm thẻ. Nó cũng thực thi các chức năng bảo mật như mã hóa/ giải mã và xác thực người dùng. Đầu đọc có thể phát hiện thẻ ngay cả khi không nhìn thấy chúng.

Khi thẻ đi vào vùng sóng điện từ nó sẽ phát hiện tín hiệu kích hoạt từ đầu đọc và nó sẽ phát thông tin nhận dạng đến đầu đọc. Đầu đọc giải mã dữ liệu được mã hóa trong chip (sóng vô tuyến phản xạ từ thẻ) và đưa vào máy chủ để xử lý.



Hình 2.5 - Hoạt động của thẻ và đầu đọc RFID

(Nguồn: Sưu tầm hình ảnh Internet)

2.4. Ưu điểm và hạn chế của hệ thống RFID

*** Ưu điểm**

Khả năng xử lý đồng thời: RFID có khả năng xử lý đồng thời nhiều đối tượng cùng một lúc. Điều này làm tăng đáng kể tốc độ kiểm tra và tiết kiệm thời gian xử lý.

Khả năng xử lý tự động: hệ thống RFID tự động nhận dạng mà không cần đến hỗ trợ của con người nên sẽ giảm được chi phí nhân công.

Hệ thống RFID có khả năng đọc/ghi thông tin trên thẻ một cách dễ dàng.

Hoạt động tốt trong môi trường không thuận lợi (ví dụ nóng, ẩm, bụi, bẩn, môi trường ăn mòn hay có sự va chạm...)

Mỗi đối tượng cần nhận dạng trong hệ thống RFID chỉ có một số nhận dạng duy nhất cho một đối tượng và khả năng mã hóa dữ liệu.

Lưu trữ được nhiều dữ liệu hơn, có thể chứa từ 64 đến 512 bit thông tin.

Thu thập dữ liệu nhanh và không cần tiếp xúc.

Tuổi thọ và độ bền lâu hơn đối với những thẻ thụ động không cần pin.

*** Hạn chế**

Bên cạnh nhiều ưu điểm của hệ thống ứng dụng RFID, một vài nhược điểm của công nghệ này vẫn chưa được khắc phục như:

- Dung độ đầu đọc: Các đầu đọc có thể đọc chồng lấn lên nhau.
- Chi phí cho thẻ và đầu đọc RFID vẫn là khá lớn.
- Chưa có được một chuẩn thống nhất giữa các quốc gia, các nhà sản xuất thiết bị.

Với những nhược điểm còn tồn tại này, mặc dù đã được biết đến từ rất sớm trong khoảng thập niên 50 nhưng RFID vẫn chưa được ứng dụng rộng rãi và phổ biến.

Cần khắc phục những nhược điểm trong tương lai, đặc biệt là chi phí giảm xuống thì công nghệ này mới có thể ứng dụng trong cuộc sống hàng ngày của con người và trong nhiều lĩnh vực kinh doanh, dịch vụ.

*** So sánh hệ thống RFID với các hệ thống khác**

Tham số hệ thống	Mã vạch	Nhận dạng tiếng nói	Nhận dạng bằng đặc điểm sinh học	Hệ thống RFID
Lượng dữ liệu đặc trưng (byte)	1-100	—	—	16-64K
Ảnh hưởng của bụi và độ ẩm	Cao	—	—	Không ảnh hưởng
Ảnh hưởng của hướng và vị trí	Bị giới hạn	—	—	Không ảnh hưởng
Giảm chất lượng, hao mòn	Bị giới hạn	—	—	Không ảnh hưởng
Chi phí mua sắm	Rất thấp	Rất cao	Rất cao	Trung bình
Tốc độ đọc	Thấp (~4s)	Rất thấp (>5s)	Rất thấp (> 5-10s)	Cực nhanh (~0.5s)
Khoảng cách tối đa giữa đầu đọc và thiết bị mang dữ liệu	0-50 cm	0-50 cm	Tiếp xúc trực tiếp	0-5m, vi sóng

Bảng 2.1 – So sánh hệ thống RFID với các hệ thống khác [26]

2.5. Thẻ RFID

2.5.1. Khái niệm

Thẻ RFID là một thiết bị có thể lưu trữ và truyền dữ liệu đến một đầu đọc trong

một môi trường không tiếp xúc bằng sóng vô tuyến. Thẻ RFID mang dữ liệu về một vật, một sản phẩm (item) nào đó và gắn lên sản phẩm đó.

Thẻ RFID gồm chip bán dẫn nhỏ (bộ nhớ của chip có thể chứa tới 96 bit đến 512 bit dữ liệu nhiều gấp 64 lần so với mã vạch) và ăngten được thu nhỏ trong một số hình thức đóng gói.

Thông thường mỗi thẻ RFID có một cuộn dây hoặc ăngten nhưng không phải tất cả RFID đều có vi chip và nguồn năng lượng riêng.

2.5.2. Các thông số của thẻ

2.5.2.1. Dung lượng

Thẻ RFID có thể lưu trữ được phụ thuộc nhà cung cấp và loại ứng dụng, thông thường nó có thể mang lượng thông tin không lớn hơn 2 Kb - đủ để lưu trữ dữ liệu về sản phẩm đang nằm trong diện cần quản lý.

2.5.2.2. Tần số hoạt động

Tần số làm việc là tần số điện từ thẻ để truyền thông hay thu được năng lượng. Tần số xác định tốc độ truyền thông và khoảng cách đọc thẻ. Tần số cao (High-frequency) có phạm vi đọc dài hơn, có tốc độ đọc nhanh. Tần số thấp (Low-frequency) có thể xuyên qua tường tốt hơn. RFID sử dụng sóng từ 30KHz đến 5,8GHZ.

Có 4 tần số chính mà RFID hoạt động:

- Low-frequency (LF): băng tần từ 125 KHz - 134 KHz. Băng tần này phù hợp với phạm vi ngắn như hệ thống chống trộm, nhận dạng động vật và hệ thống khóa tự động.
- High-frequency (HF): băng tần 13,56 MHz. Tần số cao cho phép độ chính xác cao hơn với phạm vi 3 feet ($3 \times 0,3048\text{m} \approx 1\text{m}$). Các thẻ thụ động 13,56 MHz được đọc ở tốc độ 10 đến 100 thẻ trên giây và ở phạm vi 3 feet. Các thẻ thụ động được dùng trong việc theo dõi vật liệu trong các thư viện, kiểm soát hiệu sách, theo dõi pallet, truy cập, theo dõi hành lý vận chuyển bằng máy bay và theo dõi item đồ trang sức.

- Ultrahigh-frequency (UHF): các thẻ hoạt động ở 900 MHz và có thể được đọc ở khoảng cách dài hơn các thẻ high-frequency, phạm vi từ 3 đến 15 feet. Tuy nhiên các thẻ này dễ bị ảnh hưởng bởi các nhân tố môi trường hơn các thẻ hoạt động ở các tần số khác. Băng tần 900 MHz thực sự phù hợp cho các ứng dụng dây chuyền cung cấp vì tốc độ và phạm vi của nó. Các thẻ thụ động ultrahigh - frequency có thể được đọc ở tốc độ 100 đến 1000 thẻ trên giây. Các thẻ này thường được sử dụng trong việc kiểm tra pallet và container, xe chở hàng và toa trong vận chuyển tàu biển.
- Microwave frequency: băng tần 2.45 và 5.8 GHz, có nhiều sóng radio bức xạ từ các vật thể ở gần nên có thể cản trở khả năng truyền thông giữa bộ đọc và thẻ. Các thẻ microwave RFID thường được dùng trong quản lý dây chuyền cung cấp.

Tên tần số	Khoảng tần số	Phạm vi, tốc độ
Low frequency	125 KHz - 134 KHz	~ 1,5 feet, tốc độ đọc thấp
High frequency	13,56 MHz	~ 3 feet, tốc độ đọc trung bình
Ultrahigh frequency	860-930 MHz	15 feet, tốc độ đọc cao
Microwave frequency	2.45/5.8 GHz	~ 3 feet, tốc độ đọc cao

Bảng 2.2 – Tần số hoạt động cho các thẻ Passive

Hiện nay, chưa có thống nhất được chuẩn chung cho tần số RFID. Phần lớn các nước ấn định vùng tần số vô tuyến 125 kHz hoặc 134Khz cho các hệ thống RFID ở tần số thấp, 13.56 MHz cho tần số cao. Châu Âu thì sử dụng tần số 868 MHz trong khi Mỹ thì sử dụng 915 MHz, còn Nhật đang tìm kiếm để mở băng tần 960 MHz,...

2.5.3. Các thuộc tính của thẻ RFID

Mục đích của một thẻ RFID về mặt vật lý gắn dữ liệu về một đối tượng lên sản phẩm đó. Mỗi thẻ có một vài cơ chế bên trong nào đó để chứa dữ liệu và một cách truyền thông của dữ liệu đó

Mỗi thẻ có 2 hoạt động cơ bản là:

- Gắn thẻ: bất kì thẻ nào cũng được gắn lên sản phẩm theo nhiều cách.
- Đọc thẻ: thẻ RFID phải có khả năng giao tiếp thông tin qua sóng radio theo nhiều tần số khác nhau.

Ngoài ra, thẻ còn có một hoặc nhiều thuộc tính hoặc đặc điểm sau:

- Làm chết/vô hiệu hóa (Kill/disable): Nhiều thẻ cho phép bộ đọc ra lệnh cho nó ngưng các chức năng. Sau khi thẻ nhận chính xác “kill code”, thẻ sẽ không đáp ứng lại bộ đọc.
- Ghi một lần (write once): Với thẻ được sản xuất có dữ liệu cố định thì các dữ liệu này được thiết lập tại nhà máy, nhưng với thẻ ghi một lần dữ liệu của thẻ có thể được thiết lập một lần bởi người dùng sau đó dữ liệu này không thể thay đổi.
- Ghi nhiều lần (write many): nhiều kiểu thẻ có thể được ghi dữ liệu nhiều lần.
- Chống xung đột (Anti-collision): Khi nhiều thẻ đặt cạnh nhau, bộ đọc sẽ gặp khó khăn để nhận biết khi nào đáp ứng của một thẻ kết thúc và khi nào bắt đầu một đáp ứng khác. Với thẻ anticollision sẽ nhận biết được thời gian đáp ứng đến bộ đọc.
- Mã hóa và bảo mật (Security and encryption): Nhiều thẻ có thể tham gia vào các giao tiếp có mật mã, khi đó thẻ chỉ đáp ứng lại bộ đọc chỉ khi cung cấp đúng password.

2.5.4. Giao thức thẻ

Giao thức thẻ là một tập các quy tắc chính thức mô tả cách truyền dữ liệu,

đặc biệt là qua một mạng. Các giao thức cấp thấp xác định các tiêu chuẩn về điện, về vật lý được tiến hành theo kiểu bit và kiểu byte, việc truyền, việc phát hiện lỗi và hiệu chỉnh chuỗi bit. Các giao thức cấp cao đề cập đến định dạng dữ liệu bao gồm cú pháp của thông điệp, đoạn đối thoại giữa đầu cuối tới máy tính, các bộ ký tự, sự sắp xếp thứ tự của thông điệp, v.v...

Với định nghĩa này, các giao diện không gian sẽ là các giao thức cấp thấp, còn các giao thức được mô tả dưới đây là các giao thức cấp cao. Nó xác định cú pháp của thông điệp và cấu trúc của đoạn đối thoại giữa đầu đọc và thẻ.

Sau đây là một số thuật ngữ thường được sử dụng:

- Singulation : Thuật ngữ này mô tả một thủ tục giảm một nhóm (group) thành một luồng (stream) để quản lý kế tiếp nhau được. Singulation cũng có hàm ý rằng đầu đọc đọc các ID của mỗi thẻ để nó kiểm kê.
- Anti-collision: Thuật ngữ này mô tả một tập thủ tục ngăn chặn các thẻ khác và không cho phép có thay đổi. Singulation nhận dạng các thẻ riêng biệt, ngược lại anti-collision điều chỉnh thời gian đáp ứng và tìm các phương thức sắp xếp ngẫu nhiên những đáp ứng này để đầu đọc có thể hiểu từng thẻ trong tình trạng quá tải này.
- Identity: Identity là một cái tên, một số hoặc địa chỉ mà nó chỉ duy nhất một vật hoặc một nơi nào đó.

2.5.5. Phân loại thẻ

Có nhiều cách phân loại thẻ : dựa trên nguồn cung cấp, các đặc điểm vật lý, các giao diện không khí “air interface” (cách mà chúng giao tiếp được với bộ đọc), khả năng lưu trữ và xử lý thông tin,...

Sau đây là phương pháp phân loại thẻ thường được sử dụng đó là dựa theo vai trò của thẻ :

- Thụ động (Passive)

- Tích cực (chủ động)(Active)
- Bán tích cực (Semi-active, cũng như bán thụ động semi-passive)

2.5.5.1. Phân loại theo vai trò

*** Thẻ thụ động (Passive tag)**

Đây là loại tag được sử dụng rộng rãi hiện nay, giá thành rẻ.

- Phương thức hoạt động: Bộ phận đọc thẻ sẽ truyền sóng radio đến thẻ thụ động và kích hoạt thẻ. Sau đó thẻ sẽ tự động truyền thông tin được mã hóa của nó đến bộ phận đọc.
- Hạn chế: tầm hoạt động hạn chế, thường chỉ xấp xỉ 3-2m.
- Ưu điểm: thẻ thụ động không đòi hỏi phải có pin để hoạt động, có vòng đời sử dụng rất lâu, kích thước nhỏ và rẻ, có thể tái sử dụng

*** Thẻ tích cực (Active tag)**

Là loại tag có gắn pin (một loại gắn pin cố định, một loại có thể thay thế)

- Phương thức hoạt động: thẻ tích cực sẽ tự động phát ra tín hiệu trong một bán kính khoảng 100m đến các bộ phận đọc và truyền thông tin được mã hóa.
- Hạn chế: thẻ không thể hoạt động nếu không có pin, đắt và có kích thước tương đối lớn
- Ưu điểm: tầm phủ sóng lớn (hơn 100m), có thể sử dụng các nguồn điện để hoạt động. Trong tương lai gần, các active tag có thể sẽ mang nhưng chức năng sau:
 - Khả năng tự kiểm soát và theo dõi sản phẩm nó gắn vào.
 - Có dung lượng thông tin lớn nhất.
 - Có thể được gắn với bộ phận tìm kiếm mạng lưới tự động, cho phép nó lựa chọn kênh truyền thông tốt nhất.

Ngoài ra còn có loại thẻ bán thụ động là sự kết hợp giữa thẻ thụ động và chủ động. Thẻ bán thụ động có sử dụng nguồn pin, khoảng cách đọc thẻ ngắn hơn thẻ chủ động nhưng xa hơn so với thẻ thụ động.

2.5.5.2. Phân loại thẻ dựa vào khả năng ghi dữ liệu trên thẻ

Ngoài cách phân loại cơ bản trên thì có thể dùng cách phân loại khác đó là dựa vào khả năng hỗ trợ việc ghi dữ liệu trên thẻ, khi đó thẻ được chia làm ba loại:

- Thẻ chỉ đọc RO (Read Only).
- Thẻ ghi một lần - đọc nhiều lần WORM (Write Once Read Manly).
- Thẻ đọc – ghi RW (Read Write).

*** Thẻ RO:**

Thẻ Read Only (RO) có thể được lập trình (tức là ghi dữ liệu lên thẻ RO) chỉ một lần.

Dữ liệu có thể được lưu vào thẻ tại trong lúc sản xuất. Nhà sản xuất loại thẻ này sẽ đưa dữ liệu lên thẻ và người sử dụng thẻ không thể điều chỉnh được. Loại thẻ này chỉ tốt đối với những ứng dụng nhỏ mà không thực tế đối với quy mô sản xuất lớn hoặc khi dữ liệu của thẻ cần được làm theo yêu cầu của khách hàng dựa trên ứng dụng. Loại thẻ này được sử dụng trong các ứng dụng kinh doanh và hàng không nhỏ.

*** Thẻ WORM :**

Thẻ Write Once, Read Many (WORM) có thể được ghi dữ liệu một lần, mà thường thì không phải được ghi bởi nhà sản xuất mà bởi người sử dụng thẻ ngay lúc thẻ cần được ghi. Tuy nhiên trong thực tế thì có thể ghi được vài lần (khoảng 100 lần). Nếu ghi quá số lần cho phép, thẻ có thể bị phá hỏng vĩnh viễn. Thẻ WORM được gọi là field programmable (lập trình theo trường).

Loại thẻ này có giá cả và hiệu suất tốt, có an toàn dữ liệu và là loại thẻ phổ biến nhất trong lĩnh vực kinh doanh ngày nay.

***Thẻ RW :**

Thẻ RW có thể ghi dữ liệu được nhiều lần, khoảng từ 10.000 đến 100.000 lần hoặc có thể hơn nữa. Việc này đem lại lợi ích rất lớn vì dữ liệu có thể được ghi bởi đầu đọc hoặc bởi thẻ (nếu là thẻ tích cực). Thẻ RW thường rất đắt nên không được sử dụng rộng rãi trong các ứng dụng ngày nay, trong tương lai có thể công nghệ thẻ phát triển thì chi phí thẻ giảm xuống.

2.5.6. Cách lựa chọn thẻ

Lựa chọn thẻ phụ thuộc vào yêu cầu sau:

- Dải đọc yêu cầu: Các thẻ active thường cho có dải đọc rộng hơn thẻ passive. Đối với các ứng dụng bán hàng, người ta thường sử dụng thẻ passive vì dải đọc của những thẻ này cũng đủ đáp ứng yêu cầu.
- Chất liệu và đóng gói: Mỗi một chất liệu khác nhau sẽ tạo ra các thẻ RFID có đặc điểm khác nhau. Ví dụ, chất lỏng có thể ngăn cả luồng sóng radio. Các hộp chứa bằng kim loại cũng tạo ra nhiễu tới đầu đọc.
- Hệ số kích thước: Thẻ RFID có các kích thước khác nhau. Hệ số kích thước cho các loại thẻ RFID dùng cho các mỗi loại sản phẩm sẽ phụ thuộc vào cách đóng gói sản phẩm đó.
- Chấp nhận các chuẩn: Việc tính toán xem liệu có phải hầu hết các đầu đọc hiện có sẽ hiểu được các thẻ RF bạn đã chọn hay không cũng là một điều quan trọng. EPCglobal và International Standards Organization (ISO) đã cung cấp các chuẩn cho giao tiếp giữa thẻ RFID và đầu đọc.
- Chi phí: Chi phí của một thẻ RFID giữ vai trò quan trọng trong việc có chọn loại thẻ đó hay không bởi vì hầu hết các ứng dụng đều sử dụng rất nhiều thẻ RFID. Vì vậy, cần phải chọn loại thẻ RFID đáp ứng vừa đủ nhu cầu và có chi phí chấp nhận được.

2.6. Các thiết bị Mifare RFID của Soyal

2.6.1. Thẻ thụ động Mifare

2.6.1.1. Giới thiệu

Mifare [18] là nhãn hiệu nổi tiếng sở hữu bởi NXP Semiconductors (công ty con được hình thành từ Philips Semiconductors) phân phối các sản phẩm thẻ thông minh không tiếp xúc được sử dụng rộng rãi trên thế giới: thẻ cảm ứng, công nghệ cảm ứng,...

Công nghệ độc quyền Mifare được công nhận tiêu chuẩn ISO 14443 (RFID) loại 13,56 MHz, là thẻ thông minh không tiếp xúc tiêu chuẩn. Công nghệ này được dùng để chế tạo thẻ và đầu đọc (còn được gọi là thiết bị ghép cảm ứng).

2.6.1.2. Đặc điểm các loại thẻ Mifare

*** MIFARE tiêu chuẩn**

- Thẻ Mifare tiêu chuẩn là thẻ thông minh không tiếp xúc thông dụng nhất phù hợp cho các ứng dụng như: kiểm soát ra vào, thanh toán bằng thẻ, các ứng dụng thanh toán trong công ty hoặc trường học, vé xe công cộng, thẻ khách hàng thân thiết... Với kích thước bằng thẻ tín dụng thông thường;
- Tương thích với chuẩn ISO 14443A;
- Mifare tiêu chuẩn gồm hai loại bộ nhớ 1K và 4K;
- Dữ liệu được bảo vệ bởi Key A và B;
- Tính năng đọc/ghi thông tin lên thẻ, tốc độ dưới 10% giây;
- Tuổi thọ của chip lên tới 100.000 lần đọc/ghi;
- Công nghệ ổn định đã được sử dụng rộng rãi – biên độ đọc ổn định;
- Kích thước bằng thẻ tín dụng tiêu chuẩn (85.6mm x 56mm x 0.78mm);
- Có thể in hình ảnh trực tiếp lên thẻ.

*** Thẻ Mifare siêu nhẹ**

- Mifare siêu nhẹ là thẻ thông minh không tiếp xúc 13.56 MHz, dung lượng bộ

nhớ 512 bits với chi phí thấp nhất;

- Tương thích với chuẩn ISO 14443A;
- Hỗ trợ Triple DES;
- Tính năng đọc/ghi thông tin lên thẻ, tốc độ dưới 10% giây;
- Tuổi thọ của chip lên tới 100.000 lần đọc/ghi;
- Công nghệ ổn định đã được sử dụng rộng rãi – biên độ đọc ổn định;
- Ứng dụng kiểm soát ra vào, vé thu phí, thẻ tích điểm, ghi thông tin;
- Kích thước bằng thẻ tín dụng tiêu chuẩn (85.6mm x 56mm x 0.78mm);
- Có thể in hình ảnh trực tiếp lên thẻ.

*** Mifare DESFire**

- Mifare DESFire là thẻ thông minh không tiếp xúc 13.56Mhz, độ bảo mật cao phù hợp với các ứng dụng ví điện tử;
- Tương thích với chuẩn ISO 14443A (từ 1-4);
- Hỗ trợ các thuật toán bảo mật 2KTDES, 3KTDES;
- Dung lượng 2K, 4K và 8K.

*** Mifare DESFire EV1 (còn gọi là DESFire8)**

- Phát triển mới của thẻ Mifare DESFire có sẵn dung lượng 2 KB, 4 KB và 8 KB;
- Hỗ trợ cho các ID ngẫu nhiên;
- Hỗ trợ mã hóa 128-bit AES.

*** MIFARE Plus**

- Mifare Plus là một thẻ thay thế cho Mifare cổ điển;
- Bộ nhớ: 2 Kbytes hoặc 4 Kbytes;
- Hỗ trợ 128-bit AES;

- Ít linh hoạt hơn MIFARE DESFire EV1;
- Mifare Plus khi được sử dụng trong hệ thống giao thông cũ mà chưa hỗ trợ AES từ phía đầu đọc vẫn có thể bị tấn công.

Các loại thẻ	Bộ nhớ	Bảo mật
Thẻ Mifare tiêu chuẩn	1k/4k	Bảo vệ phím A/B
Thẻ Mifare siêu nhẹ	512 bit	3-DES
Thẻ Mifare DESFire	2k/4k/8k	DES, 3-DES, AES
Thẻ Mifare Plus	2k/4k	AES

Bảng 2.3 – Các thông số của thẻ thủ động Mifare

2.6.1.3. Tính năng

- Truyền dữ liệu bằng cách không tiếp xúc và cung cấp năng lượng (không cần pin)
- Phạm vi hoạt động: trên 100mm (phụ thuộc vào hình dạng của ăngten)
- Tần số hoạt động: 13.56MHz
- Truyền dữ liệu: 106kbit/s
- Tính toán vẹn dữ liệu: 16 Bit CRC, tính chẵn lẻ, bit mã hóa, bit đếm
- Chống va chạm
- EEPROM
 - o 1 Kbyte, chia thành 16 khu vực với 4 khối, mỗi khối gồm 16 byte
 - o Người dùng truy cập các điều kiện đối với mỗi khối bộ nhớ
 - o Lưu trữ dữ liệu trong 10 năm
 - o Độ bền 100.000 chu kỳ ghi
- Bảo mật

2.6.2. Đầu đọc Mifare Soyal AR-721H

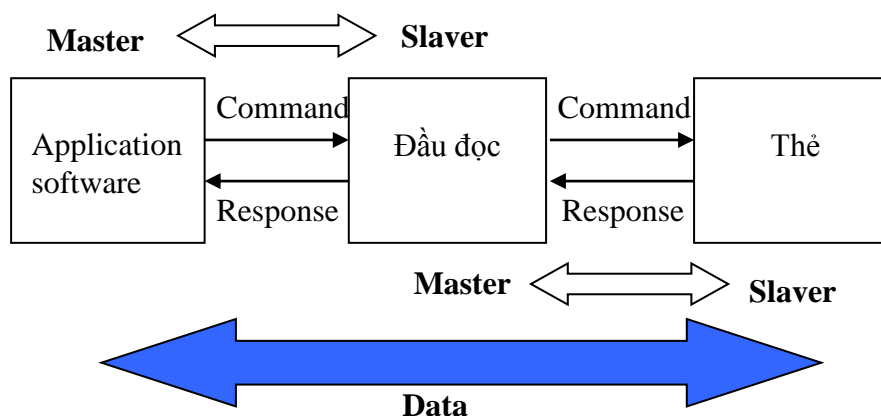
2.6.2.1. Khái niệm

Đầu đọc RFID là thiết bị kết nối không dây với thẻ để nhận dạng đối tượng được gắn thẻ. Nó là một thiết bị đọc và ghi dữ liệu lên thẻ RFID tương thích. Thời gian mà đầu đọc có thể phát năng lượng sóng vô tuyến để đọc thẻ được gọi là chu kỳ làm việc của đầu đọc.

2.6.2.2. Đặc điểm và phương thức hoạt động

Đầu đọc có nhiệm vụ kích hoạt thẻ, truyền nhận dữ liệu bằng sóng vô tuyến với thẻ, thực hiện giải mã tín hiệu nhận được từ thẻ ra dạng tín hiệu cần thiết để truyền về máy chủ, đồng thời cũng nhận lệnh từ máy chủ để thực hiện các yêu cầu truy vấn hay đọc/ghi thẻ.

Đầu đọc có thể thực hiện những hoạt động nói trên là nhờ vào phần mềm ứng dụng (Application Software) nằm trên máy chủ, nó chỉ huy các lệnh đến đầu đọc theo thủ tục master-slaver, điều này có nghĩa là trong cấu trúc phân cấp của hệ thống thì phần mềm ứng dụng đóng vai trò master, còn đầu đọc đóng vai trò slaver (chỉ hoạt động khi có lệnh từ master). Để thực hiện lệnh từ phần mềm ứng dụng thì trước tiên đầu đọc phải kết nối với thẻ, lúc này đối với thẻ thì đầu đọc đóng vai trò là master, thẻ có nhiệm vụ đáp ứng các yêu cầu của đầu đọc.



Hình 2.6 - Thủ tục master-slaver giữa Application, đầu đọc và thẻ

(Nguồn: Sưu tầm hình ảnh Internet)

2.6.2.3. Thông số kỹ thuật

Tần số	125kHz	13,56MHz
Tiêu chuẩn	EM Standard	ISO 14443A/B ISO15693 DESFire PSAM
Khoảng cách đọc	10-18cm	2-8cm
Nguồn hoạt động	9-16VDC	
Công suất tiêu thụ	<3W	
Kết nối máy tính	RS-485	
Date Transfer Rate	9600 bps (N,8,1)	
Nhiệt độ hoạt động	-20°C đến 60°C	
Digital Input	Egress(R.T.E)/ Door contact	
Relay Output	Lock Relay	
Lock relay time	Toggle 0.1~600 Sec	
Alarm time	Toggle, 1~600 Sec	
Tamper Switch	Limit Switch (Form C)	
Bộ nhớ	M4/M8 M6	1.024 65.000
Lưu trữ	M4/M8	1.200
External Reader	WG26/34	
Anti-pass-back	Yes(M4/M8 Only)	
Kiểm soát thang máy	32 tầng, 1.024 use	
Serial Port	TTL(4800bps, N,8,1)	
Real Time Clock	Yes	
LCD Panel	No	
Nút chuông cửa	No	
Transistor Output	Arming LED/ Alarm/ Duress /Security trigger signal	
Tiêu chuẩn bảo vệ	No	
Indicator	1 Bi-color LED & 1 Beeper	
Chất liệu bàn phím	Cao Su	
Vật liệu vỏ	ABS	
Time Zone	11/63(Connect to Multi-Door Networking Controller)	
Chế độ hoạt động	Stand-Alone/ Networking	



Hình 2.7 – Thông số kỹ thuật đầu đọc Mifare Soyol AR-721H [21]

2.6.3. Đầu ghi Mifare Soyol AR-737P

2.6.3.1. Giới thiệu

Mifare AR-737P [19,20] ra đời năm 2005, AR-737P là một lập trình thông minh nhất của hệ thống thẻ thông minh có thể đọc từ xa Mifare®. Nó được thiết kế để cải thiện tính năng đọc/ghi của ứng dụng Mifare® đọc từ xa.

2.6.3.2. Đặc điểm

Hỗ trợ kiểm tra CRC8 tự động lệnh đơn, chức năng lưu trữ/sao lưu tự động.

Hỗ trợ giao diện RS-232 và USB 2.0 (Trình điều khiển USB nên được cài đặt trước)

Kiểm soát thông qua phần mềm (Giải pháp Mifare và công cụ SOR)

Các tầng đệm phím A/B mặc định và phím A/B nhiệt tích hợp.

Sử dụng giao thức SORMifare với độ an ninh cao và giao diện thân thiện.

2.6.3.3. Thông số kỹ thuật

Tần số	13.56MHz
Tiêu chuẩn	ISO14443A / B + 15693 ISO15693 DESFire PSAM
Nguồn cung cấp	5VDC
Công suất tiêu thụ	<1.5W
Giao diện truyền thông	USB 2.0 cổng COM ảo
Chuyển dữ liệu Rate	9600bps (N, 8,1)
Nhiệt độ hoạt động	-20 °C đến + 60 °C
Hỗ trợ Tag	Mifare 1
Chỉ số	2 LED & 1 Beeper
Vật liệu vỏ	ABS
Màu	Màu xám
Kích thước (mm)	113 (L) X71 (W) X36 (H)
Trọng lượng (g)	150 ± 10



Hình 2.8 – Thông số kỹ thuật đầu đọc Mifare Soyal AR-737P [22]

2.6.4. Ứng dụng

Khách sạn, nhà nghỉ mát và các nền công nghiệp bán lẻ.

Bãi đậu xe, thanh toán phí trước, soát vé.

Hệ thống điều khiển ra vào.

Ví điện tử.

Kiểm soát giấy phép khách hàng.

2.6.5. Lý do chọn thiết bị Mifare của Soyal

- Mifare là tiêu chuẩn công nghiệp hàng đầu cho giao dịch thẻ thông minh

không tiếp xúc.

- Được sử dụng rộng rãi trên toàn thế giới
- Phù hợp với tiêu chuẩn ISO14443A
- Lộ trình và con đường phát triển trong tương lai: Giao diện tiêu chuẩn đảm bảo rằng cơ sở hạ tầng ngày nay có thể dễ dàng được nâng cấp cho thẻ IC trong tương lai
- Danh mục sản phẩm phù hợp và nhiều nguồn cung ứng ở tất cả các cấp trong chuỗi giá trị
- Bộ nhớ đa dạng và hỗ trợ nhiều chuẩn bảo mật.

2.7. Chuẩn truyền thông giữa thẻ và đầu đọc

Quá trình ghi dữ liệu lên thẻ, giao tiếp và trao đổi dữ liệu giữa đầu đọc và thẻ RFID là một quá trình phức tạp. Để thực hiện được một hệ thống RFID hoàn chỉnh, phục vụ cho việc đọc và ghi dữ liệu lên thẻ cũng như lên cơ sở dữ liệu. Có nhiều tổ chức đã có nhiều sáng kiến liên quan đến tiêu chuẩn RFID. Đáng chú ý nhất đó là tổ chức tiêu chuẩn hóa quốc tế (International Organization for Standardization - ISO) và EPC toàn cầu (EPCglobal)

Các chuẩn ISO phổ biến:

ISO 11784 và 11785 là hai tiêu chuẩn đáng chú ý trong công nghệ tần số thấp mà đã đang sử dụng trong sự theo dõi động vật.

ISO 18000 -2 được hoàn thành và xuất bản vào năm 2004. Đây là tiêu chuẩn định nghĩa những tham số cho giao diện truyền thông dưới 135KHz đó là dãy tần số thấp.

ISO 15693 và 14443 là tiêu chuẩn tần số cao 13.56MHz sử dụng rộng rãi cho đến nay.

ISO 15693 thì được xuất bản vào năm 2000 định nghĩa những tham số cho thẻ RFID, sử dụng trong những phạm vi yêu cầu đọc hơn 10cm.

ISO 14443 là tiêu chuẩn cho thẻ RFID với phạm vi đọc giới hạn ít hơn 10cm. Sự khác nhau chính giữa hai tiêu chuẩn này là ứng dụng của chúng. ISO 14443 vì

khoảng cách đọc ngắn và khả năng mã hóa nên thích hợp hơn với những ứng dụng an toàn như là thanh toán điện tử, ngân hàng và giao dịch tài chính.

ISO 18000 -3 được xuất bản vào năm 2004, là tiêu chuẩn mới cho RFID 13.56MHz. ISO 18000- 3 là một tiêu chuẩn toàn diện được xây dựng dựa trên ISO 15693. Nó có hai phiên bản, phiên bản 1 giống như ISO 15693.

Với tần số UHF (860MHz-956MHz) thì hiện nay không có tần số toàn cầu được công nhận do sự hạn chế của những vùng khác nhau trên thế giới. Ở Bắc Mỹ, UHF RFID sử dụng 915MHz, 869MHz -868MHz và 950MHz-956MHz tương ứng được sử dụng ở Châu Âu và Nhật Bản

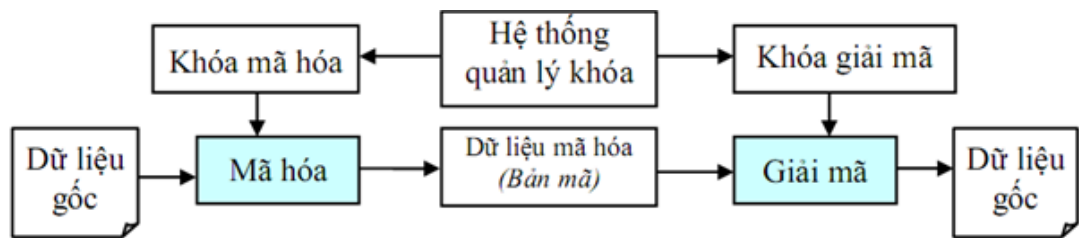
ISO 18000-6 (trong tần số UHF 860-956MHz) được xuất bản vào năm 2004. Tiêu chuẩn này định nghĩa những tham số cho Air Interface và Communication.

CHƯƠNG 3: MÃ HÓA DỮ LIỆU

3.1. Tổng quan về mã hóa

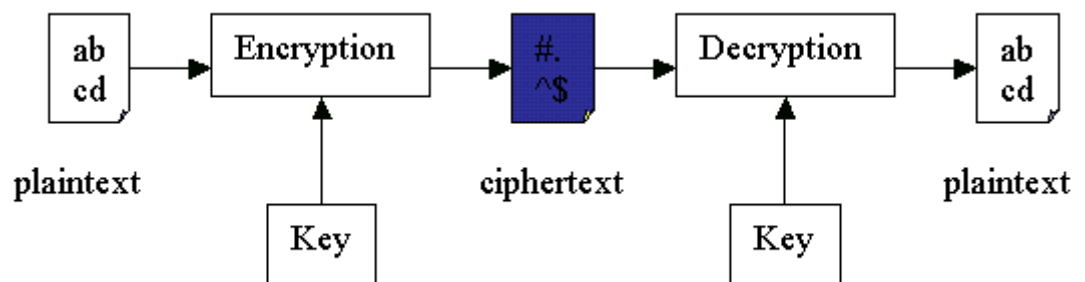
3.1.1. Khái niệm về mã hóa

Mã hóa (Encrypt) là phương pháp để biến thông tin (phím, ảnh, văn bản, hình ảnh...) từ định dạng bình thường sang dạng thông tin không thể hiểu được (với mục đích giữ bí mật thông tin đó) nếu không có phương tiện giải mã.



Hình 3.1 – Quy trình mã hóa dữ liệu [27]

Thuật toán Cryptography đề cập tới ngành khoa học nghiên cứu về mã hoá và giải mã thông tin. Cụ thể hơn là nghiên cứu các cách thức chuyển đổi thông tin từ dạng rõ (clear text) sang dạng mờ (cipher text) và ngược lại. Đây là một phương pháp hỗ trợ rất tốt cho trong việc chống lại những truy cập bất hợp pháp tới dữ liệu được truyền đi trên mạng, áp dụng mã hóa sẽ khiến cho nội dung thông tin được truyền đi dưới dạng mờ và không thể đọc được đối với bất kỳ ai cố tình muốn lấy thông tin đó.



Hình 3.2 - Hệ thống mã hóa thông tin [27]

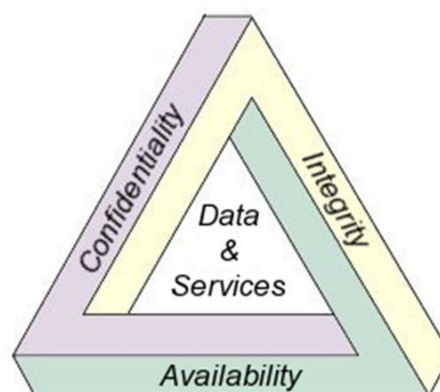
3.1.2. Độ an toàn của thuật toán

Nguyên tắc đầu tiên trong mã hoá là “Thuật toán nào cũng có thể bị phá vỡ”. Các thuật toán khác nhau cung cấp mức độ an toàn khác nhau, phụ thuộc vào độ phức tạp để phá vỡ chúng. Tại một thời điểm, độ an toàn của một thuật toán phụ thuộc:

- Nếu chi phí hay phí tổn cần thiết để phá vỡ một thuật toán lớn hơn giá trị của thông tin đã mã hóa thuật toán thì thuật toán đó tạm thời được coi là an toàn.
- Nếu thời gian cần thiết dùng để phá vỡ một thuật toán là quá lâu thì thuật toán đó tạm thời được coi là an toàn.
- Nếu lượng dữ liệu cần thiết để phá vỡ một thuật toán quá lớn so với lượng dữ liệu đã được mã hoá thì thuật toán đó tạm thời được coi là an toàn.

3.1.3. Ba mục tiêu chính của an toàn thông tin

Vấn đề bảo mật thông tin không chỉ đơn thuần là việc chống lại các cuộc tấn công từ hacker, ngăn chặn malware để đảm bảo thông tin không bị phá hủy hoặc bị tiết lộ ra ngoài... Hiểu rõ 3 mục tiêu của bảo mật là bước căn bản đầu tiên trong quá trình xây dựng một hệ thống thông tin an toàn nhất có thể. Ba mục tiêu này còn được gọi là tam giác bảo mật C-I-A.



Hình 3.3 - Tam giác bảo mật C-I-A

(Nguồn: Sưu tầm hình ảnh Internet)

*** Confidentiality**

Đảm bảo tính bí mật của thông tin, tức là thông tin chỉ được phép truy cập (đọc) bởi những đối tượng (người, chương trình máy tính...) được cấp phép.

Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng.

*** Integrity**

Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi. Về điểm này, nhiều người thường hay nghĩ tính “integrity” đơn giản chỉ là đảm bảo thông tin không bị thay đổi (modify) là chưa đầy đủ.

Ngoài ra, một giải pháp “data integrity” có thể bao gồm thêm việc xác thực nguồn gốc của thông tin này (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy và ta gọi đó là tính “authenticity” của thông tin.

*** Availability**

Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn. Ví dụ, nếu một server chỉ bị ngưng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng của nó là 99,999%.

3.1.4. Phân loại các thuật toán mã hóa

Có rất nhiều các thuật toán mã hóa khác nhau. Từ những thuật toán được công khai để mọi người cùng sử dụng và áp dụng như là một chuẩn chung cho việc mã hóa dữ liệu; đến những thuật toán mã hóa không được công bố. Có thể phân loại các thuật toán mã hoá như sau:

Phân loại theo các phương pháp:

Mã hóa cổ điển (Classical cryptography)

Mã hóa đối xứng (Symetric cryptography)

Mã hóa bất đối xứng (Asymetric cryptography)

Hàm băm (Hash function)

Phân loại theo số lượng khóa:

Mã hóa khóa bí mật (Private-key Cryptography)

Mã hóa khóa công khai (Public-key Cryptography)

Luận văn tập trung nghiên cứu phương pháp mã hóa Hàm băm (Hashing) vì hàm băm làm thay đổi dữ liệu thành một dạng mật mã, quá trình hashing sử dụng một thông số hash value và không thay đổi dữ liệu ban đầu. Hashing có thể sử dụng để bảo vệ và kiểm tra tính toàn vẹn của dữ liệu. Nó cũng có khả năng sử dụng để kiểm tra khi có một tiến trình copy được thực hiện và đảm bảo tính chính xác của dữ liệu khi chúng được copy. Hashing là hàm 1 chiều nên có tốc độ xử lý nhanh phù hợp với yêu cầu điểm danh.

3.2. Phương pháp mã hóa dữ liệu trên thẻ RFID

3.2.1. Hashing – Hàm băm

Hashing là một phương thức mật mã nhưng nó không phải là một thuật toán mã hoá. Hashing chỉ sử dụng một chứng chỉ số duy nhất được biết đến với tên như "hash value – giá trị hash", "hash – băm", Message Authentication Code (MAC), fingerprint – vân tay, hay một đoạn message. Dữ liệu đầu vào của bạn có thể là một file, một ổ đĩa, một quá trình truyền thông tin trên mạng, hay một bức thư điện tử. Thông số hash value được sử dụng để phát hiện khi có sự thay đổi của tài nguyên. Nói cách khác, hashing sử dụng nó để phát hiện ra dữ liệu có toàn vẹn trong quá trình lưu trữ hay trong khi truyền hay không.

Hàm băm có chức năng mật mã “một chiều”, và có một kích thước cố định cho bất kỳ một văn bản gốc nào.

Thuật toán hashing thường được sử dụng: MD4, MD5, SHA-1

*** Đặc tính của hàm băm**

Với hàm băm là hàm 1 chiều có các đặc tính sau:

- Với dữ liệu đầu vào (bản tin gốc) M , chỉ thu được giá trị băm duy nhất $h = H(M)$.
- Nếu dữ liệu trong bản tin M bị thay đổi hay bị xoá để thành bản tin M' , thì giá trị băm $h(M')$ khác $h(M)$.
- Nội dung của bản tin gốc “khó” thể suy ra từ giá trị hàm băm của nó. Nghĩa là, với thông điệp M thì “dễ” tính được $h = H(M)$, nhưng lại “khó” tính ngược lại được nếu chỉ biết giá trị băm $h(M)$.

3.2.2. Hàm băm MD5

3.2.2.1. Giới thiệu

MD5 [23] (viết tắt của tiếng Anh Message-Digest algorithm 5, giải thuật Tiêu hóa tin 5) là một hàm băm mật mã học được sử dụng phổ biến với giá trị Hash dài 128-bit. MD5 được thiết kế bởi Ronald Rivest vào năm 1991 để thay thế cho hàm băm trước đó, MD4.

Là một chuẩn Internet (RFC 1321), MD5 đã được dùng trong nhiều ứng dụng bảo mật, và cũng được dùng phổ biến để kiểm tra tính toàn vẹn của tập tin. Một bảng băm MD5 thường được diễn tả bằng một số hệ thập lục phân 32 ký tự.

3.2.2.2. Giải thuật

Gồm 5 bước

Đầu vào: chuỗi có độ dài bất kì.

Đầu ra: giá trị băm có độ dài 128 bits.

Bước 1: nhồi dữ liệu

- Nhồi thêm các bits sao cho dữ liệu có độ dài $l \equiv 448 \pmod{512}$ hay $l = n * 512 + 448$ (n, l nguyên).
- Luôn thực hiện nhồi dữ liệu ngay cả khi dữ liệu ban đầu có độ dài mong muốn. Ví dụ, dữ liệu có độ dài 448 được nhồi thêm 512 bits để được độ dài 960 bits.

- Số lượng bit nhồi thêm nằm trong khoảng 1 đến 512.
- Các bit được nhồi gồm 1 bit “1” và các bit 0 theo sau.

Bước 2: thêm vào độ dài

- Độ dài của khối dữ liệu ban đầu được biểu diễn dưới dạng nhị phân 64 bit và được thêm vào cuối chuỗi nhị phân kết quả của bước 1.
- Nếu độ dài của khối dữ liệu ban đầu > 264 , chỉ 64 bits thấp được sử dụng, nghĩa là giá trị được thêm vào bằng $K \bmod 264$.
- Kết quả có được từ 2 bước đầu là một khối dữ liệu có độ dài là bội số của 512. Khối dữ liệu được biểu diễn:
- Bằng một dãy L khối 512 bit Y_0, Y_1, \dots, Y_{L-1} .
- Bằng một dãy N từ (word) 32 bit M_0, M_1, M_{N-1} . Vậy $N = L \times 16$ ($32 \times 16 = 512$).

Bước 3: khởi tạo bộ đệm MD (MD buffer)

- Một bộ đệm 128 bit được dùng lưu trữ các giá trị băm trung gian và kết quả. Bộ đệm được biểu diễn bằng 4 thanh ghi 32 bit với các giá trị khởi tạo ở dạng littleendian (byte có trọng số nhỏ nhất trong từ nằm ở địa chỉ thấp nhất) như sau:

$$A = 67\ 45\ 23\ 01$$

$$B = EF\ CD\ AB\ 89$$

$$C = 98\ BA\ DC\ FE$$

$$D = 10\ 32\ 54\ 76$$

- Các giá trị này tương đương với các từ 32 bit sau:

$$A = 01\ 23\ 45\ 67$$

$$B = 89\ AB\ CD\ EF$$

$$C = FE\ DC\ BA\ 98$$

$$D = 76\ 54\ 32\ 10$$

Bước 4: xử lý các khối dữ liệu 512 bit

- Trọng tâm của giải thuật là hàm nén (compression function) gồm 4 “vòng” xử lý. Các vòng này có cấu trúc giống nhau nhưng sử dụng các hàm luận lý khác nhau gồm F, G, H và I như sau:

$$F(X,Y,Z) = X \wedge Y \vee \neg X \wedge Z$$

$$G(X,Y,Z) = X \wedge Z \vee Y \wedge \neg Z$$

$$H(X,Y,Z) = X \text{ xor } Y \text{ xor } Z$$

$$I(X,Y,Z) = Y \text{ xor } (X \vee \neg Z)$$

Mảng 64 phần tử được tính theo công thức: $T[i] = 232 \times \text{abs}(\sin(i))$, i được tính theo radian.

- Kết quả của 4 vòng được cộng theo modulo 232 với đầu vào CV_q để tạo CV_{q+1}.
- Các giá trị trong bảng T:

T[1] = d76aa478	T[17] = f61e2562	T[33] = fffa3942	T[49] = f4292244
T[2] = e8c7b756	T[18] = c040b340	T[34] = 8771f681	T[50] = 432aff97
T[3] = 242070db	T[19] = 265e5a51	T[35] = 6d9d6122	T[51] = ab9423a7
T[4] = c1bdceee	T[20] = e9b6c7aa	T[36] = fde5380c	T[52] = fc93a039
T[5] = f57c0faf	T[21] = d62f105d	T[37] = a4beea44	T[53] = 655b59c3
T[6] = 4787c62a	T[22] = 2441453	T[38] = 4bdecfa9	T[54] = 8f0ccc92
T[7] = a8304613	T[23] = d8a1e681	T[39] = f6bb4b60	T[55] = ffeff47d
T[8] = fd469501	T[24] = e7d3fbc8	T[40] = bebfbc70	T[56] = 85845dd1
T[9] = 698098d8	T[25] = 21e1cde6	T[41] = 289b7ec6	T[57] = 6fa87e4f
T[10] = 8b44f7af	T[26] = c33707d6	T[42] = eaa127fa	T[58] = fe2ce6e0
T[11] = ffff5bb1	T[27] = f4d50d87	T[43] = d4ef3085	T[59] = a3014314
T[12] = 895cd7be	T[28] = 455a14ed	T[44] = 4881d05	T[60] = 4e0811a1
T[13] = 6b901122	T[29] = a9e3e905	T[45] = d9d4d039	T[61] = f7537e82
T[14] = fd987193	T[30] = fcefa3f8	T[46] = e6db99e5	T[62] = bd3af235
T[15] = a679438e	T[31] = 676f02d9	T[47] = 1fa27cf8	T[63] = 2ad7d2bb
T[16] = 49b40821	T[32] = 8d2a4c8a	T[48] = c4ac5665	T[64] = eb86d391

Bước 5: Xuất kết quả

- Sau khi xử lý hết L khối 512 bit, đầu ra của lần xử lý thứ L là giá trị băm 128 bits.

3.2.2.3. Ứng dụng

- Chữ kí điện tử.
- Dùng trong các ứng dụng bảo mật.
- Kiểm tra tính toàn vẹn của tập tin được truyền đi.
- Lưu trữ mật khẩu.
- Ứng dụng trong các phần mềm để đảm bảo rằng tập tin tải về không bị lỗi.

3.2.3. Hàm băm SHA-1

3.2.3.1. Giới thiệu

SHA [24] (Secure Hash Algorithm hay thuật giải băm an toàn) là năm thuật giải được chấp nhận bởi FIPS dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao. Những thuật giải này được gọi là "an toàn" bởi vì, theo nguyên văn của chuẩn FIPS 180-2 phát hành ngày 1 tháng 8 năm 2002.

Năm thuật giải SHA là SHA-1 [25] (trả lại kết quả dài 160 bit), SHA-224 (trả lại kết quả dài 224 bit), SHA-256 (trả lại kết quả dài 256 bit), SHA-384 (trả lại kết quả dài 384 bit), và SHA-512 (trả lại kết quả dài 512 bit).

SHA-1 được sử dụng rộng rãi trong nhiều ứng dụng và giao thức an ninh khác nhau, bao gồm TLS và SSL, PGP, SSH, S/MIME, và IPSec. SHA-1 được coi là thuật giải thay thế MD5, một thuật giải băm 128 bit phổ biến khác.

3.2.3.2. Giải thuật

Gồm 5 bước

Đầu vào: chuỗi có độ dài tối đa 2^{64} bits.

Đầu ra: giá trị băm có độ dài 160 bits.

Bước 1: nhồi thêm dữ liệu

- Thông điệp được nhồi thêm các bits sao cho độ dài $l \equiv 448 \pmod{512}$ hay $l = n * 512 + 448$ (n, l nguyên).

- Thông điệp luôn luôn được nhồi thêm dữ liệu.
- Số bits nhồi thêm nằm trong khoảng 1 đến 512.
- Phần dữ liệu nhồi thêm bao gồm một bit 1 và theo sau là các bit 0.

Bước 2: thêm vào độ dài

- Độ dài của khối dữ liệu ban đầu được biểu diễn dưới dạng nhị phân 64 bit và được thêm vào cuối chuỗi nhị phân kết quả của bước 1.
- Độ dài được biểu diễn dưới dạng nhị phân 64 bit không dấu.
- Kết quả có được từ 2 bước đầu là một khối dữ liệu có độ dài là bội số của 512. Khối dữ liệu được biểu diễn:
- Bằng một dãy L khối 512 bit Y_0, Y_1, \dots, Y_{L-1} .
- Bằng một dãy N từ (word) 32 bit M_0, M_1, \dots, M_{N-1} . Vậy $N = L \times 16$ ($32 \times 16 = 512$)

Bước 3: khởi tạo bộ đệm MD (MD buffer)

- Một bộ đệm 160 bit được dùng lưu trữ các giá trị băm trung gian và kết quả. Bộ đệm được biểu diễn bằng 5 thanh ghi 32 bit với các giá trị khởi tạo ở dạng bigiendian (byte có trọng số lớn nhất trong từ nằm ở địa chỉ thấp nhất) như sau:

$A = 01\ 23\ 45\ 67$

$B = 89\ AB\ CD\ EF$

$C = FE\ DC\ BA\ 98$

$D = 76\ 54\ 32\ 10$

$E = C3\ D2\ E1\ F0$

- Các giá trị này tương đương với các từ 32 bit sau:

$A = 01\ 23\ 45\ 67$

$B = 89\ AB\ CD\ EF$

$C = FE\ DC\ BA\ 98$

$D = 76\ 54\ 32\ 10$

E = C3 D2 E1 F0

Bước 4: xử lý các khối dữ liệu 512 bit

- Trọng tâm của giải thuật bao gồm 4 vòng lặp thực hiện tất cả 80 bước. 4 vòng lặp có cấu trúc như nhau, chỉ khác nhau ở các hàm logic f_1, f_2, f_3, f_4 .
- Mỗi vòng có đầu vào gồm khối 512 bit hiện thời và một bộ đệm 160 bit ABCDE. Các thao tác sẽ cập nhật giá trị bộ đệm.
- Mỗi bước sử dụng một hằng số K_t ($0 \leq t \leq 79$)

$$K_t = 5A827999 \quad (0 \leq t \leq 19)$$

$$K_t = 6ED9EBA1 \quad (20 \leq t \leq 39)$$

$$K_t = 8F1BBCDC \quad (40 \leq t \leq 59)$$

$$K_t = CA62C1D6 \quad (60 \leq t \leq 79)$$

- Đầu ra của 4 vòng (bước 80) được cộng với đầu ra của bước CV_q để tạo ra CV_{q+1}

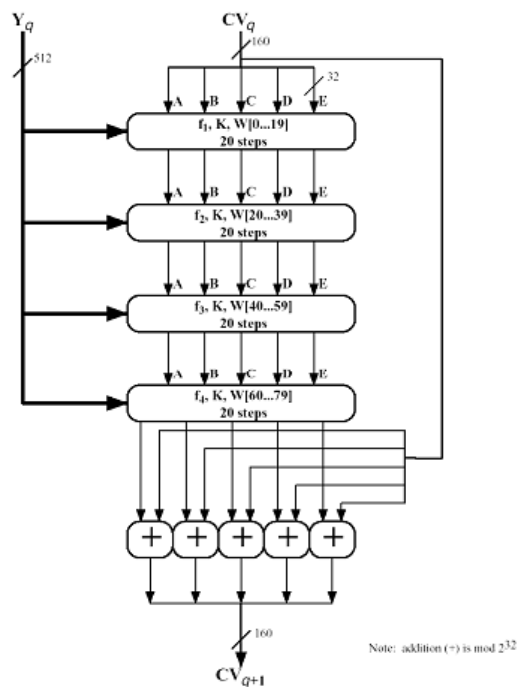


Figure 9.5 SHA-1 Processing of a Single 512-bit Block (SHA-1 Compression Function)

Bước 5: xuất kết quả

- Sau khi thao tác trên toàn bộ L blocks. Kết quả của khối thứ L là bảng băm 160 bit

3.2.3.3. Ứng dụng

SHA-1 là 1 phần trong các ứng dụng bảo mật được sử dụng rộng rãi trong các giao thức như: TLS và SSL, PGP, SSH và IPSEC...

Các SHA-1 có thể được sử dụng với các DSA trong thư điện tử, chuyển tiền điện tử, phân phối phần mềm, lưu trữ dữ liệu, và các ứng dụng khác cần đảm bảo tính toàn vẹn DL và xác thực nguồn gốc DL. Các SHA-1 cũng có thể sử dụng bất cứ khi nào nó là cần thiết để tạo ra 1 phiên bản đặc của tin nhắn.

Hàm SHA-1 còn được sử dụng trên Wii của Nintendo để xác minh chữ ký thời gian khởi động.

Các hàm băm SHA được dùng làm cơ sở cho mã khối SHACAL.

3.2.4. So sánh 2 phương pháp mã hóa

*** Giống nhau**

Cả hai thuật toán MD5, SHA-1 [27] được xem là "đa chức năng". Chúng có thể nhận mọi dạng dữ liệu đầu vào, từ tin nhắn email cho đến hạt nhân (kernel) của hệ điều hành, cũng như tạo ra một dấu vân tay số duy nhất. Chỉ thay đổi một ký tự bất kỳ bên trong file đầu vào cũng tạo ra những dấu vân tay hoàn toàn khác nhau.

MD5 và SHA-1 đều cộng thêm các bit “giả” để tạo thành những khối chia hết cho 512 bit, nhưng SHA-1 sử dụng cùng một hàm phi tuyến f cho cả bốn vòng.

Thuật toán MD5 và SHA-1 đều gồm 5 bước là: nhồi dữ liệu, thêm độ dài, khởi tạo bộ đệm, xử lý các khối dữ liệu 512 bits, xuất kết quả.

Tính đơn giản: cả hai đều được mô tả đơn giản và dễ dàng cài đặt trên phần cứng và phần mềm.

*** Khác nhau**

- Hao tổn tài nguyên
- Tốc độ
 - Cả hai dựa trên phép toán 32 bit, thực hiện tốt trên các kiến trúc 32 bit.
 - SHA-1 thực hiện nhiều hơn 16 bước và thao tác trên thanh ghi 160 bit nên tốc độ thực hiện chậm hơn.
- Độ an toàn (khả năng chống tấn công)
 - Để tạo ra thông điệp có giá trị băm cho trước, cần 2¹²⁸ thao tác với MD5 và 2¹⁶⁰ với SHA-1.
 - Để tìm 2 thông điệp có cùng giá trị băm, cần 2⁶⁴ thao tác với MD5 và 2⁸⁰ với SHA-1.

Algorithm	Max Message size (bits)	Block size (bits)	Word size	Output size (bits)	Security (bits)
MD5	$< 2^{64}$	512	32	128	< 64
SHA-1	$< 2^{64}$	512	32	160	< 80
SHA-224	$< 2^{64}$	512	32	224	112
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

Bảng 3.1 - So sánh các thông số của các thuật toán hàm băm an toàn [24]

3.2.5. Khả năng chống tấn công

Hàm băm mật mã phải có khả năng chống cự các loại tấn công mật mã, tối thiểu phải đảm bảo có 3 tính chất sau:

Kháng tiền ảnh (Pre-image resistance): Với một mã băm h bất kỳ, khó tìm được một thông điệp M nào mà $h = \text{Hash}(M)$. Điều này làm chúng ta liên tưởng tới tính một chiều của hàm số. Trong góc độ hàm số toán học, mã băm là ảnh còn thông điệp là tạo ảnh của mã băm, hay gọi là tiền ảnh. Sức kháng cự tấn công từ ảnh ngược về tiền ảnh gọi là kháng tiền ảnh. Một hàm băm có kháng tiền ảnh yếu là lỗ hổng cho các cuộc tấn công tiền ảnh.

Kháng tiền ảnh thứ hai (Second pre-image resistance): Với một thông điệp M_1 bất kỳ, khó tìm được một thông điệp thứ hai M_2 sao cho $M_1 \neq M_2$ và $\text{Hash}(M_1) = \text{Hash}(M_2)$. Xác suất xảy ra biến cố có thông điệp M_2 như thế tương tự biến cố “Cùng ngày sinh như bạn”. Một hàm băm có kháng tiền ảnh thứ hai yếu là lỗ hổng cho các cuộc tấn công tiền ảnh thứ hai.

Kháng xung đột (Collision resistance): Khó tìm được một cặp thông điệp M_1 và M_2 sao cho $M_1 \neq M_2$ và $\text{Hash}(M_1) = \text{Hash}(M_2)$. Cặp như thế được gọi là xung đột băm mật mã. Tính chất này đôi khi còn được gọi là kháng xung đột mạnh. Nó yêu cầu chiều dài băm ít nhất phải dài hơn hai lần so với yêu cầu của kháng tiền ảnh, nếu không xung đột có thể xảy ra bởi một cuộc tấn công Ngày sinh.

3.2.6. Phương pháp mã hóa

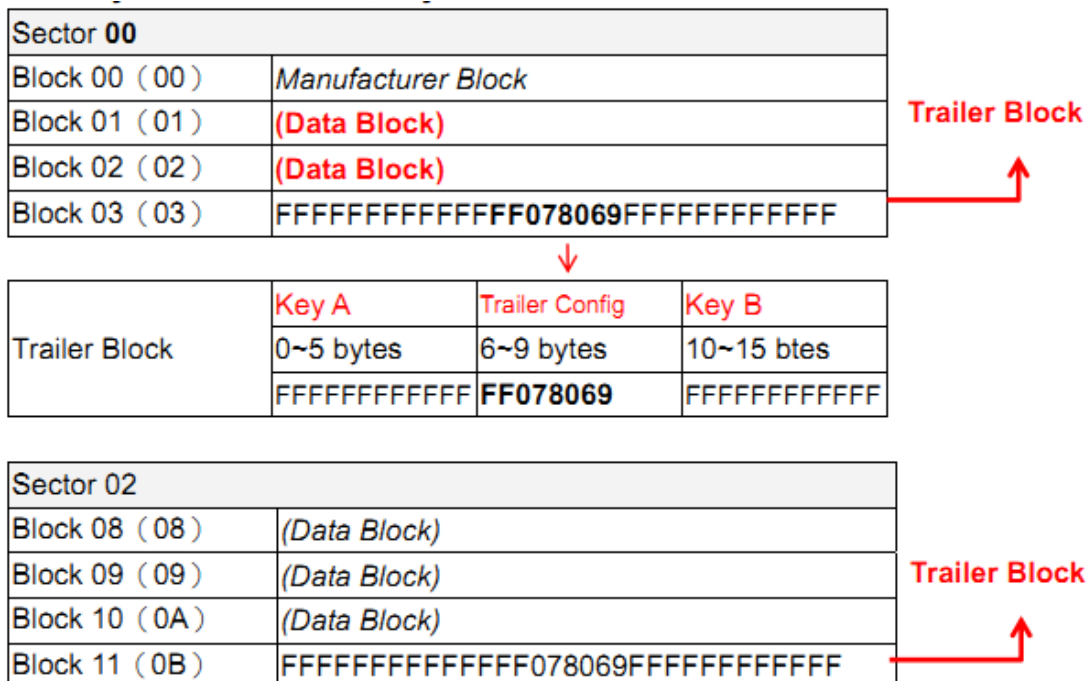
3.2.6.1. Hệ thống mã Mifare

Sector 00		Sector 08	
Block 00 (00)	Manufacturer Block	Block 32 (20)	
Block 01 (01)		Block 33 (21)	
Block 02 (02)		Block 34 (22)	
Block 03 (03)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF	Block 35 (23)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector 01		Sector 09	
Block 04 (04)	SOR	Block 36 (24)	
Block 05 (05)		Block 37 (25)	
Block 06 (06)		Block 38 (26)	
Block 07 (07)		Block 39 (27)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector 02		Sector 10	
Block 08 (08)		Block 40 (28)	
Block 09 (09)		Block 41 (29)	
Block 10 (0A)		Block 42 (2A)	
Block 11 (0B)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF	Block 43 (2B)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector 03		Sector 11	
Block 12 (0C)		Block 44 (2C)	
Block 13 (0D)		Block 45 (2D)	
Block 14 (0E)		Block 46 (2E)	
Block 15 (0F)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF	Block 47 (2F)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFF

Sector 04		Sector 12	
Block 16 (10)		Block 48 (30)	
Block 17 (11)		Block 49 (31)	
Block 18 (12)		Block 50 (32)	
Block 19 (13)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF	Block 51 (33)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF
Sector 05		Sector 13	
Block 20 (14)		Block 52 (34)	
Block 21 (15)		Block 53 (35)	
Block 22 (16)		Block 54 (36)	
Block 23 (17)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF	Block 55 (37)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF
Sector 06		Sector 14	
Block 24 (18)		Block 56 (38)	
Block 25 (19)		Block 57 (39)	
Block 26 (1A)		Block 58 (3A)	
Block 27 (1B)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF	Block 59 (3B)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF
Sector 07		Sector 15	
Block 28 (1C)		Block 60 (3C)	
Block 29 (1D)		Block 61 (3D)	
Block 30 (1E)		Block 62 (3E)	
Block 31 (1F)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF	Block 63 (3F)	FFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF

SOR
Event Log

Hình 3.4 – Hệ thống thẻ RFID [19]



Hình 3.5 – Cấu trúc thẻ RFID [19]

Khối nhà sản xuất (Manufacturer Block)

Đây là khối dữ liệu đầu tiên đầu tiên của hệ thống (Block 00), chứa dữ liệu của nhà sản xuất. Vì yêu cầu của hệ thống và an ninh nên nhà sản xuất sẽ bảo vệ và không cho phép ghi và sao chép khối này.

Khối dữ liệu (Data Block)

Tính từ Sector 01 đến Sector 14, tất cả các phần gồm có 3 khối dữ liệu 16 byte dành cho lưu trữ dữ liệu.

Khối trailer (Trailer Block)

Mỗi phần có một khối trailer chứa các điều kiện truy cập cho cả bốn khối của phần đó, được lưu trữ khoảng 6-9 byte. Nhà sản khuyến cáo không nên ghi dữ liệu vào khối này.

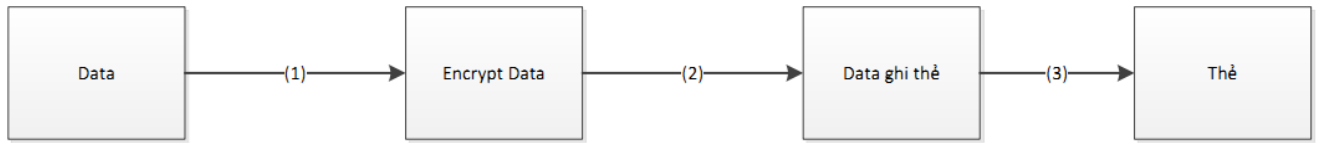
Quy tắc hệ thống mở SOYAL

Quy tắc hệ thống mở SOYAL (SOR) là giao thức mà SOYAL xây dựng dựa trên MIFARE® MF1 IC S50, tuân thủ tiêu chuẩn ISO14443A để cung cấp một giao diện độc quyền đảm bảo an ninh cho các ứng dụng khác nhau dành cho các đối tác của Soyol. Trước khi sử dụng quy tắc hệ thống mở SOYAL, người dùng được yêu cầu phải có một giấy phép phân phối cá nhân từ SOYAL.

3.2.6.2. Phương pháp mã hóa

Sau khi đã so sánh 2 phương pháp mã hóa MD5 và SHA-1 và dựa vào bảng so sánh các thông số của hàm băm. Luận văn chọn phương pháp mã hóa SHA-1 với lý do SHA1 xử lý thông điệp đầu ra cao hơn MD5 (160 bit so với 128 bit) và độ an toàn cao hơn (<80 bit so với <64 bit) và có thể mở rộng phương pháp mã hóa để có độ an toàn cao hơn, ví dụ: SHA-512.

*** Mô hình mã hóa dữ liệu**



Hình 3.6 – Mô hình mã hóa dữ liệu chung

1. Dữ liệu được mã hóa với thuật toán SHA1. Sau khi mã hóa bằng SHA1 dữ liệu sẽ có chiều dài cố định 20 bytes. Data được tạo thành theo quy tắc nối chuỗi.

Ví dụ mã hóa mật khẩu: Data = <Key cố định>|<Key ngẫu nhiên>|<Mật khẩu> (Data là dữ liệu trước khi mã hóa)

2. Dữ liệu sau khi mã hóa được chia thành 5 block, mỗi block 4 bytes để ghi thẻ.

3. Ghi từng block vào thẻ cho đến hết 5 block. Tổng thời gian khoảng 1 giây.

*** Cách thức ghi dữ liệu vào thẻ RFID**

Block	Part	Part No.	Block	Part	Part No.
0	Manufacturer Block		32		
1			33		
2			34		
3	Trailer Block		35	Trailer Block	
4	1	1	36		
5	1	2	37		
6	1	3	38		
7	Trailer Block		39	Trailer Block	
8	1	4	40		
9	1	5	41		
10	2	1	42		
11	Trailer Block		43	Trailer Block	
12	2	2	44		
13	2	3	45		
14	2	4	46		
15	Trailer Block		47	Trailer Block	
16	2	5	48		

17	3	1	49		
18	3	2	50		
19	Trailer Block		51	Trailer Block	
20	3	3	52		
21	3	4	53		
22	3	5	54		
23	Trailer Block		55	Trailer Block	
24			56		
25			57		
26			58		
27	Trailer Block		59	Trailer Block	
28			60		
29			61		
30			62		
31	Trailer Block		63	Trailer Block	

Bảng 3.2 – Luồng dữ liệu bên trong hệ thống thẻ Soyal RFID

Thẻ bao gồm 64 block. Dữ liệu được ghi theo quy luật:

- Bỏ Block 00 → 03 vì Block 00 (Manufacturer Block) và Block 03 (Trailer Block) là 2 block mà nhà sản xuất đã khóa không cho ghi vào.
- Bắt đầu ghi từ block thứ 4. Ghi 3 block bỏ 1 block.
- Mỗi block ghi 4 bytes dữ liệu, mỗi Part gồm 5 block. Tổng cộng là ghi 20 byte dữ liệu (Phù hợp với yêu cầu đặt ra mã hóa SHA1 với đầu ra là 160 bit)



Bỏ hoặc chưa sử dụng

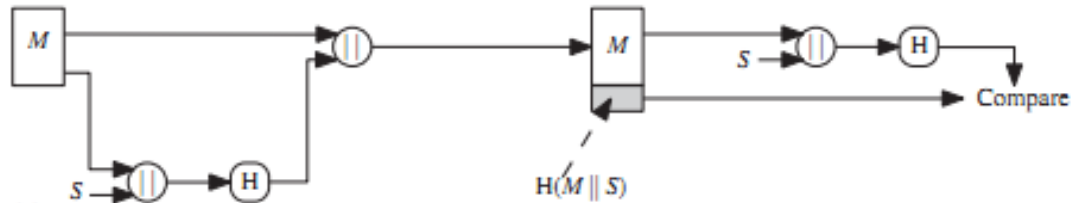
Part 1 Ghi thông tin sinh viên: mã sinh viên

Part 2 Ghi thông tin mật khẩu

Part 3 Ghi thông tin thanh toán: số dư, mã giao dịch cuối

* Phương pháp mã hóa

Phương pháp mã hóa được thực hiện theo sơ đồ sau:



Hình 3.7 – Sơ đồ mã hóa dữ liệu [32]

Trong hệ thống $M = \langle \text{key cố định} \rangle | \langle \text{data} \rangle | \langle \text{key ngẫu nhiên} \rangle$

Trong message chèn thêm key cố định và key ngẫu nhiên. Vì đảm bảo không thay đổi dữ liệu, tốc độ xử lý nhanh, do không cần thêm bước mã hóa dữ liệu, và giải mã. Dữ liệu chỉ hash và so sánh.

Đối với ứng dụng điểm danh sinh viên

$h = H(M(\langle \text{Key cố định} \rangle | \langle \text{Key phát sinh ngẫu nhiên} \rangle | \langle \text{Mã số sinh viên} \rangle))$

Đối với ứng dụng thanh toán tại căn tin

$h = H(M(\langle \text{Key cố định} \rangle | \langle \text{Key phát sinh ngẫu nhiên} \rangle | \langle \text{Số dư} \rangle | \langle \text{Mã giao dịch cuối} \rangle))$

Trong đó:

M: là message tức thông tin cần trao đổi giữa hai bên (còn gọi là dữ liệu gốc)

H: hash function, sử dụng SHA1

h: kết quả hash, $h = H(M)$

s: Key cố định và Key phát sinh ngẫu nhiên

Key cố định: là key sử dụng chung cho toàn hệ thống, tất cả thẻ sẽ được mã hóa với key này.

Key phát sinh ngẫu nhiên: key phát sinh ngẫu nhiên, tương ứng với từng thẻ, mỗi thẻ ngoài mã hóa với key cố định sẽ mã cùng với key phát sinh ngẫu nhiên.

Mã số sinh viên: mã số của sinh viên, do trường cung cấp.

Số dư: là số dư hiện tại của thẻ. Sau khi thanh toán hoặc nạp tiền sẽ cập nhật lại số dư này.

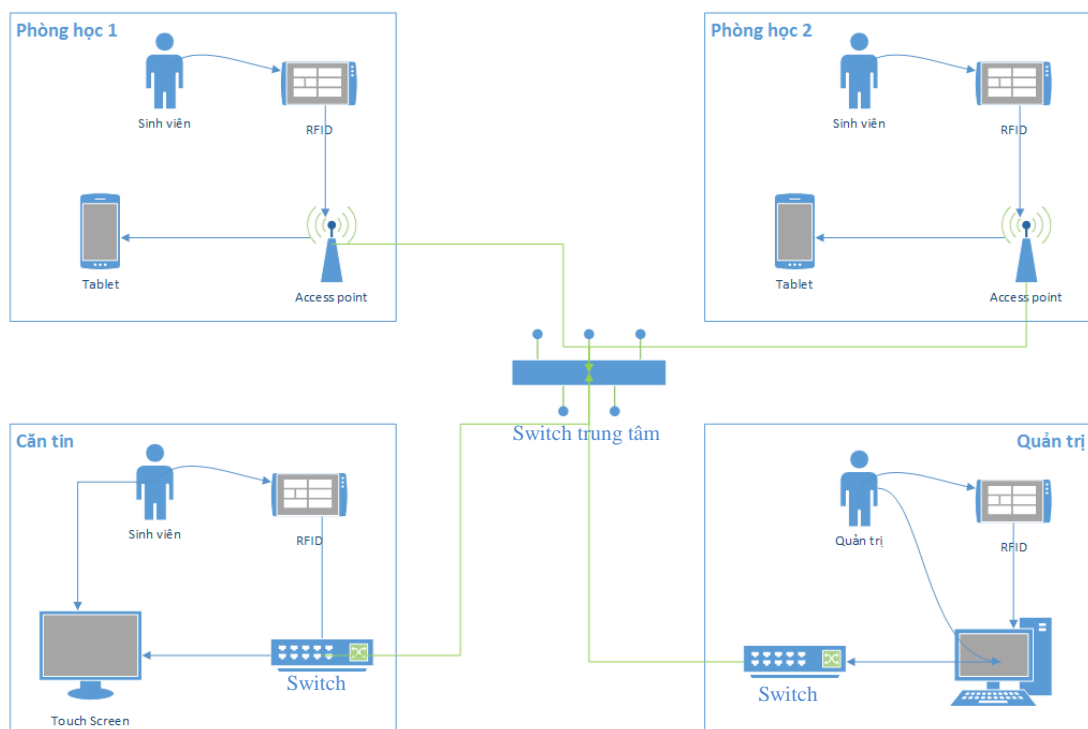
Mã giao dịch cuối: là mã giao dịch cuối cùng của người dùng trên hệ thống, sinh ra sau khi thanh toán hoặc nạp tiền, mã giao dịch do hệ thống thanh toán sinh ra.

CHƯƠNG 4: XÂY DỰNG HỆ THỐNG

4.1. Yêu cầu hệ thống

Với mục tiêu đặt ra ban đầu, ngoài việc nghiên cứu những phương pháp để mã hóa dữ liệu trên thẻ. Luận văn còn tập trung xây dựng 2 ứng dụng là điểm danh sinh viên và thanh toán tại căn tin.

4.1.1. Mô hình hệ thống



Hình 4.1 – Mô hình hệ thống

4.1.2. Yêu cầu chức năng

4.1.2.1. Chức năng cho sinh viên

- Điểm danh tại phòng học
- Thực hiện thanh toán tại căn tin
- Đổi mật khẩu
- Kiểm tra thông tin tài khoản

4.1.2.2. Chức năng cho Quản trị

- Phát hành thẻ
- Cập nhật thẻ
- Hủy thẻ
- Báo cáo điểm danh
- Thêm, cập nhật, xóa món ăn
- Thêm, cập nhật, xóa danh mục món ăn

4.1.2.3. Chức năng cho kế toán

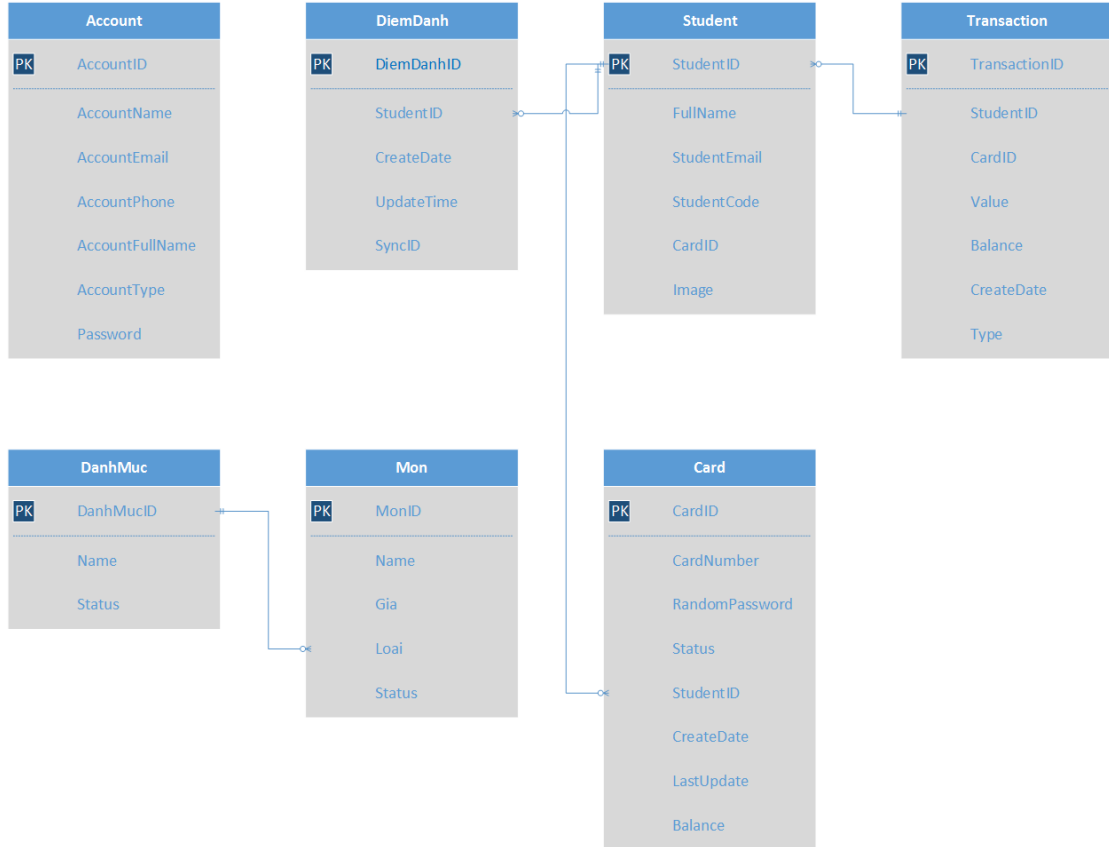
- Nạp tiền vào tài khoản

4.1.3. Yêu cầu phi chức năng

- Bảo mật (Security): Dữ liệu trên thẻ được hash đảm bảo tính toàn vẹn của dữ liệu, chống thay đổi dữ liệu trên thẻ.
- Hiệu suất (Performance): Thời gian thực hiện điểm danh 1 giây, thanh toán là 3 giây.
- Tính sẵn sàng (Availability): Hoạt động 24/ 24
- Tiện dụng (Usability) : Dễ sử dụng, số lượng thao tác ít.

4.2. Thiết kế dữ liệu

4.2.1. Sơ đồ dữ liệu



Hình 4.2 – Sơ đồ dữ liệu

4.2.2. Mô tả dữ liệu

Bảng Account : lưu thông tin tài khoản, dùng để đăng nhập website, phần mềm Admin, POS.

Tên cột	Kiểu dữ liệu	Mô tả
AccountID	bigint	ID tài khoản, tự động tăng
AccountName	varchar(100)	tên tài khoản, dùng để đăng nhập web, POS, Admin
AccountEmail	varchar(100)	Email tài khoản
AccountPhone	varchar(100)	số điện thoại
AccountFullName	nvarchar(100)	Tên đầy đủ
AccountType	int	Loại tài khoản
Password	varchar(100)	Mật khẩu

Bảng Card : lưu thông tin thẻ

Tên cột	Kiểu dữ liệu	Mô tả
CardID	bigint	ID của thẻ, tự tăng khi insert
CardNumber	varchar(100)	Số thẻ, số này do nhà sản xuất quy định, không thay đổi được
RandomPassword	varchar(100)	Mật khẩu ngẫu nhiên cho từng thẻ. Dạng guid.
Status	int	Tình trạng thẻ
StudentID	bigint	ID sinh viên tương ứng của thẻ.
CreateDate	datetime	Ngày tạo thông tin sinh viên
LastUpdate	datetime	Thời gian cập nhật thông tin sinh viên, lưu lần cuối cùng.
Balance	int	Số dư thẻ

Bảng DiemDanh: lưu thông tin điểm danh của sinh viên.

Tên cột	Kiểu dữ liệu	Mô tả
DiemDanhID	int	tự tăng mỗi lần insert
CreateDate	datetime	Ngày giờ điểm danh
StudentID	binary(8)	ID của sinh viên
UpdateTime	datetime	Ngày giờ cập nhật thông tin
SyncID	int	ID đồng bộ, id này do thiết bị (tablet) sinh

Bảng DanhMuc: lưu thông tin danh mục món ăn (thể hiện trên máy POS).

Tên cột	Kiểu dữ liệu	Mô tả
DanhMucID	int	ID danh mục, tự tăng khi insert
Name	nvarchar(100)	Tên danh mục sản phẩm
Status	int	Tình trạng danh mục

Bảng Mon: lưu thông tin món ăn (thể hiện trên máy POS)

Tên cột	Kiểu dữ liệu	Mô tả
MonID	int	ID món ăn, tự tăng khi insert
Name	nvarchar(100)	Tên món ăn
Gia	int	Giá món ăn
Loai	int	Loại (danh mục) món ăn
Status	int	Tình trạng món ăn

Bảng Student: lưu thông tin sinh viên

Tên cột	Kiểu dữ liệu	Mô tả
StudentID	bigint	ID sinh viên, tự động tăng khi insert
FullName	nvarchar(100)	Tên đầy đủ của sinh viên

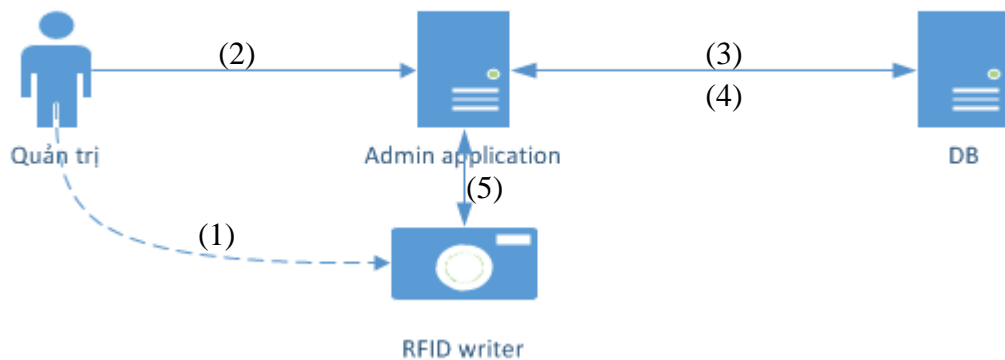
StudentEmail	varchar(100)	Email sinh viên
StudentCode	varchar(100)	Mã sinh viên
CardID	bigint	ID thẻ sinh viên
Image	text	Hình ảnh của sinh viên

Bảng Transaction : lưu thông tin thanh toán

Tên cột	Kiểu dữ liệu	Mô tả
TransactionID	int	Mã giao dịch, tự tăng khi insert
CardID	int	ID thẻ sinh viên
StudentID	int	ID của sinh viên
Value	int	Giá trị giao dịch
Balance	int	Số dư sau khi giao dịch
CreateDate	datetime	Ngày tạo giao dịch.
Type	int	Loại giao dịch (nạp tiền/ thanh toán)

4.3. Mô hình thực hiện

4.3.1. Ghi thông tin vào thẻ



Hình 4.3 – Mô hình ghi thông tin vào thẻ

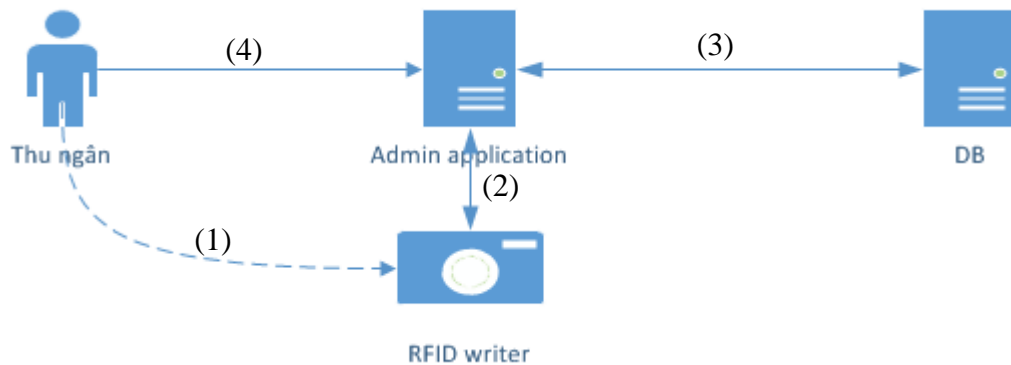
Mô hình hoạt động như sau:

- (1). Quản trị nhập thông tin sinh viên cần ghi thẻ: bao gồm MSSV + Họ tên + Mã lớp,...
- (2). Nhập thông tin Sinh viên cần ghi thẻ: bao gồm MSSV + Họ tên + Mã lớp,...
- (3). Phát sinh ra key ngẫu nhiên 6 ký tự (mỗi thẻ phát sinh một key) và ghi thông tin thẻ vào Database (DB)

(4). Chương trình mã hóa thông tin bằng thuật toán hash SHA1. Gồm các thông tin (<Key cố định>|<key ngẫu nhiên>|<MSSV>).

(5). Lưu thông tin mã số thẻ tương ứng với thông tin Sinh viên và cập nhật thẻ đã phát hành.

4.3.2. Ghi thông tin nạp tiền



Hình 4.5 – Mô hình ghi thông tin nạp tiền

Mô hình hoạt động như sau:

(1). Thu ngân tấp thẻ vào thiết bị.

(2). Thiết bị đọc các thông tin trên thẻ và dữ liệu đã được mã hóa theo thuật toán SHA1(<Key cố định>|<key phát sinh ngẫu nhiên>|<MSSV>) truyền về ứng dụng. Ứng dụng sẽ kiểm tra thông tin trong cơ sở dữ liệu tương ứng với mã thẻ có tồn tại trong cơ sở dữ liệu của ứng dụng không?

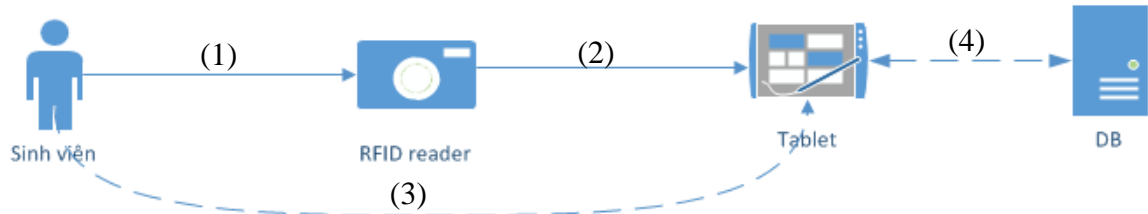
Nếu có, hiển thị thông tin Sinh viên lên màn hình và qua bước 3.

Nếu không, hiển thị thông báo thất bại. Kết thúc quá trình.

(3). Ứng dụng đọc thông tin dữ liệu số dư mã hóa. Sau đó so sánh với dữ liệu trong cơ sở dữ liệu bằng thuật toán SHA1(<Key cố định>|<key ngẫu nhiên>|<số dư>|<mã giao dịch cuối>). Nếu khớp, hiển thị số dư lên màn hình.

(4). Thu ngân nhập số tiền cần nạp. Ứng dụng phát sinh mã giao dịch, sau đó ghi vào cơ sở dữ liệu và ghi vào thẻ.

4.3.3. Điểm danh sinh viên



Hình 4.4 – Mô hình điểm danh sinh viên

Mô hình hoạt động như sau:

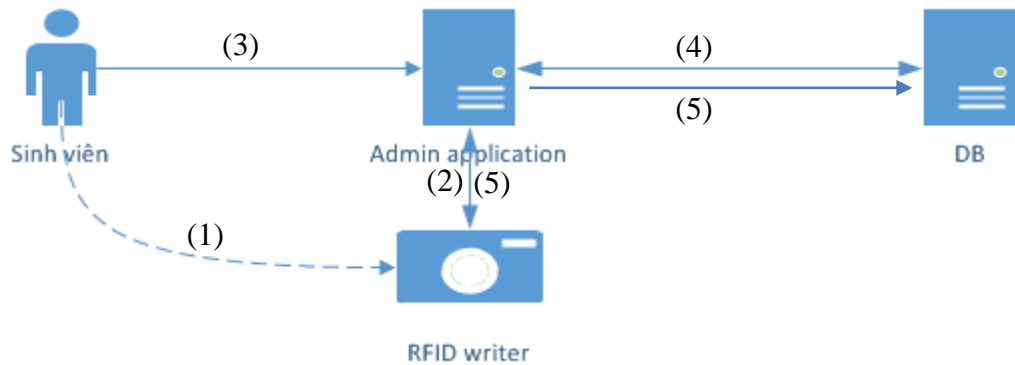
- (1). Sinh viên tấp thẻ vào thiết bị đọc
- (2). Thiết bị đọc đọc các thông tin số thẻ và dữ liệu đã được mã hóa theo thuật toán SHA1 (<Key cố định>|<key phát sinh ngẫu nhiên>|<MSSV>) truyền về tablet. Tablet sẽ kiểm tra thông tin trong cơ sở dữ liệu tương ứng với mã thẻ có tồn tại trong cơ sở dữ liệu của tablet không?

Nếu có, hiển thị trên tablet các thông tin như: MSSV, Họ tên, thời gian điểm danh, ...

Nếu không, thì hiển thị thông báo thẻ không tồn tại trên màn hình tablet.

- (3). Sinh viên kiểm tra thông tin điểm danh trên màn hình tablet.
- (4). Định kỳ tablet và server sẽ đồng bộ dữ liệu với nhau, tablet truyền thông tin điểm danh về server, server truyền thông tin thẻ về tablet.

4.3.4. Thanh toán



Hình 4.6 – Mô hình thanh toán

Mô hình hoạt động như sau:

- (1). Sau khi chọn món, sinh viên tấp thẻ vào thiết bị.
- (2). Thiết bị đọc đọc các thông tin số thẻ và dữ liệu đã được mã hóa theo thuật toán SHA1 (<Key cố định>|<key phát sinh ngẫu nhiên>|<MSSV>) truyền về ứng dụng. Ứng dụng sẽ kiểm tra thông tin trong cơ sở dữ liệu tương ứng với mã thẻ có tồn tại trong cơ sở dữ liệu của ứng dụng không?

Nếu có, hiển thị các thông tin của Sinh viên lên màn hình và qua bước 3.

Nếu không thì hiển thị thông báo thất, kết thúc quá trình.

- (3). Sinh viên nhập password vào màn hình. Ứng dụng đọc thông tin password đã mã hóa và mã hóa password sinh viên vừa nhập theo thuật toán SHA1(<key cố định>|<key ngẫu nhiên>|<password>), nếu khớp sang bước 4, không khớp kết thúc quá trình.
- (4). Ứng dụng đọc thông tin dữ liệu số dư mã hóa. Sau đó so sánh với dữ liệu trong cơ sở dữ liệu. Nếu khớp, thì kiểm tra số dư so với số tiền thanh toán, nếu số dư < số tiền thanh toán thì kết thúc quá trình, nếu đủ sang bước 5.
- (5). Ứng dụng trừ tiền trong thẻ và phát sinh mã giao dịch sau đó ghi vào cơ sở dữ liệu và ghi vào thẻ thông tin mã hóa SHA1(<Key cố định>|<key ngẫu nhiên>|<số dư>|<mã giao dịch cuối>).

4.4. Môi trường cài đặt và các công nghệ sử dụng

Môi trường cài đặt hệ thống: hệ điều hành Windows 7, hệ điều hành Android 4.0 trở lên.

Ngôn ngữ lập trình: C# [29,33], Java [30]

Công cụ hỗ trợ lập trình: Visual Studio 2010 [34], SQL Server Management Studio, Android Studio (phụ lục 1)

Database: MS SQL 2008

Thiết bị:

- Các thiết bị của Soyal: thẻ RFID, đầu đọc Mifare AR-721H, đầu ghi Mifare AR-737P 13.56 MHz
- Tablet 7 inch
- Router Wireless

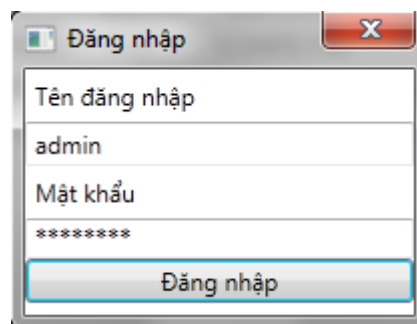
CHƯƠNG 5: KẾT QUẢ ĐẠT ĐƯỢC

5.1. Giao diện thiết kế

5.1.1. Giao diện quản trị thẻ

* Màn hình đăng nhập admin

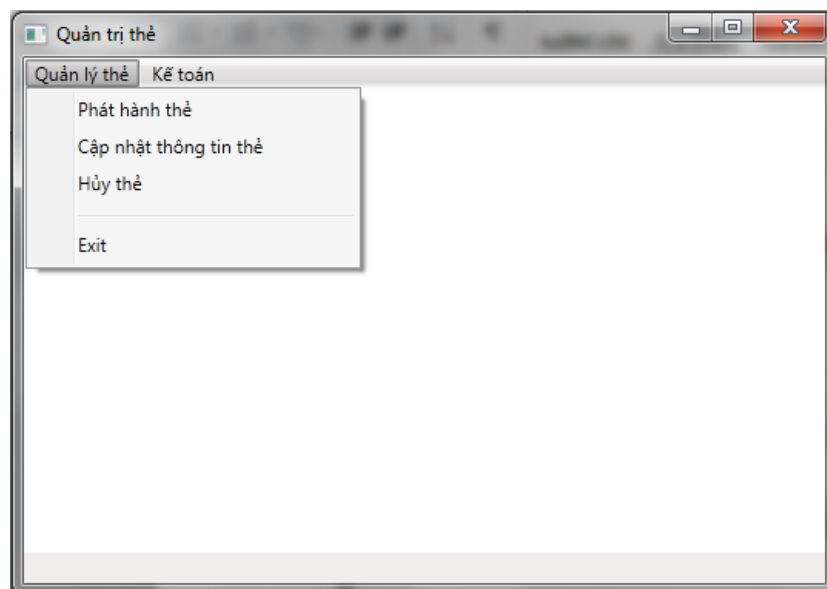
- Tên đăng nhập: admin
- Mật khẩu: 123456



Hình 5.1 – Giao diện đăng nhập

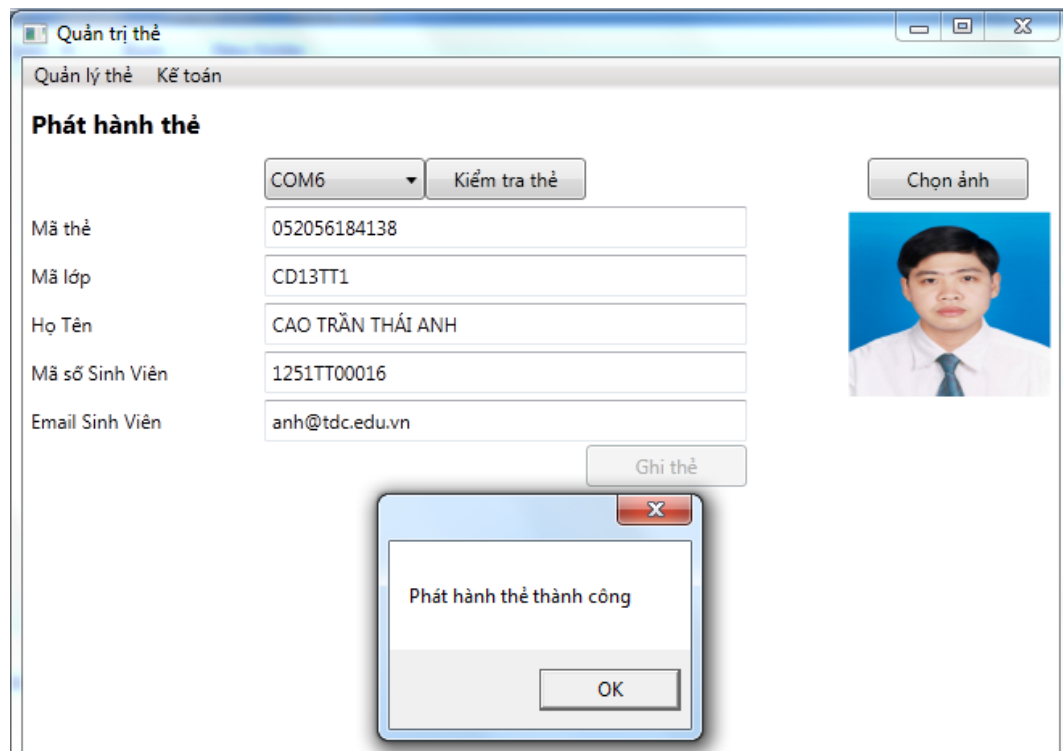
Màn hình Quản trị thẻ sau khi đăng nhập, gồm 2 chức năng chính:

Quản lý thẻ: gồm các chức năng Phát hành thẻ; Cập nhật thông tin thẻ và Hủy thẻ



Hình 5.2 – Giao diện quản trị thẻ

Phát hành thẻ



Hình 5.3 – Giao diện phát hành thẻ

Quy trình thực hiện

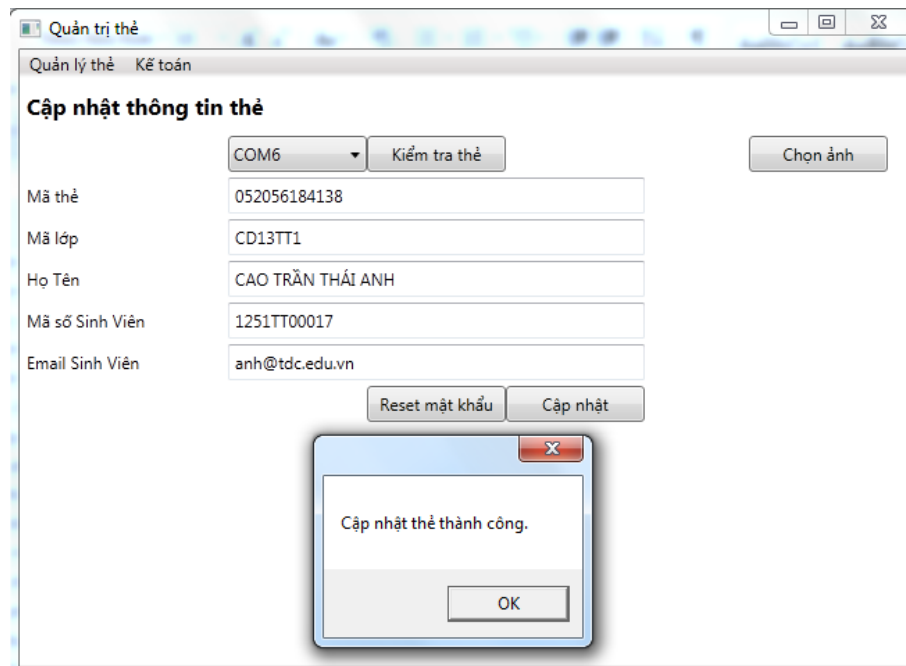
Bước 1: Táp thẻ vào đầu ghi Mifare AR-737P

Bước 2: Click chọn Kiểm tra thẻ → Hiện thị mã thẻ

Bước 3: Điền đầy đủ các thông tin: Họ tên; Mã số sinh viên; Mã lớp; Chọn ảnh

Bước 4: Click vào Ghi thẻ → Hiện thông báo Phát hành thẻ thành công.

Cập nhật thông tin thẻ



Hình 5.4 – Giao diện cập nhật thông tin thẻ

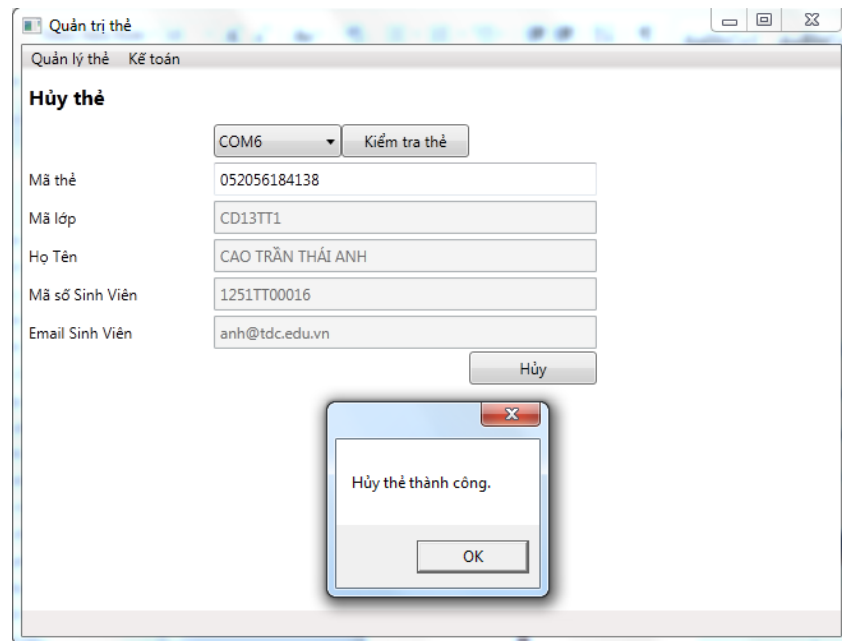
Quy trình thực hiện

Bước 1: Táp thẻ vào đầu ghi Mifare AR-737P

Bước 2: Click chọn Kiểm tra thẻ → Hiện thị các thông tin đã ghi trong thẻ

Bước 3: Chỉnh sửa các thông tin bị sai

Bước 4: Click vào Cập nhật → Hiện thông báo Cập nhật thẻ thành công.

Hủy thẻ**Hình 5.5 – Giao diện hủy thẻ**

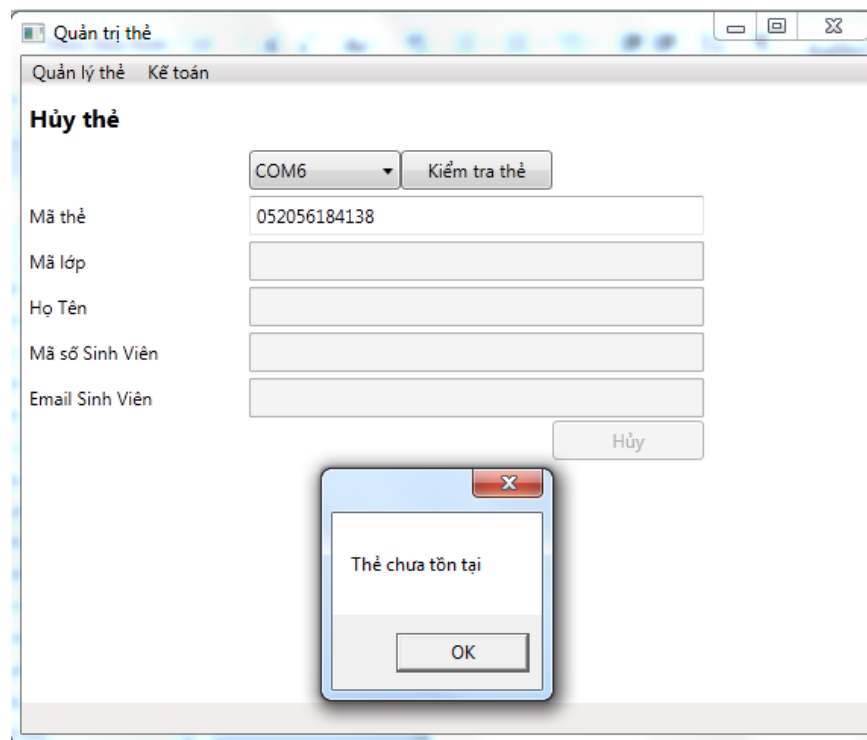
Quy trình thực hiện

Bước 1: Táp thẻ vào đầu ghi Mifare AR-737P

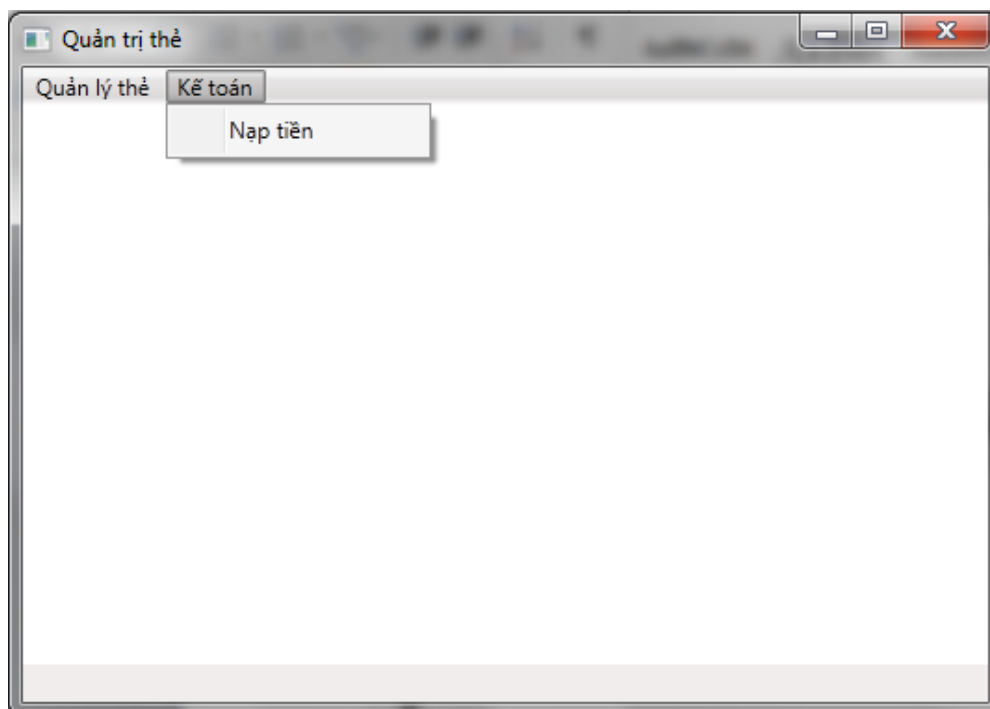
Bước 2: Click chọn Kiểm tra thẻ → Hiện thị các thông tin đã ghi trong thẻ

Bước 3: Click vào Hủy → Hiện thông báo Hủy thẻ thành công

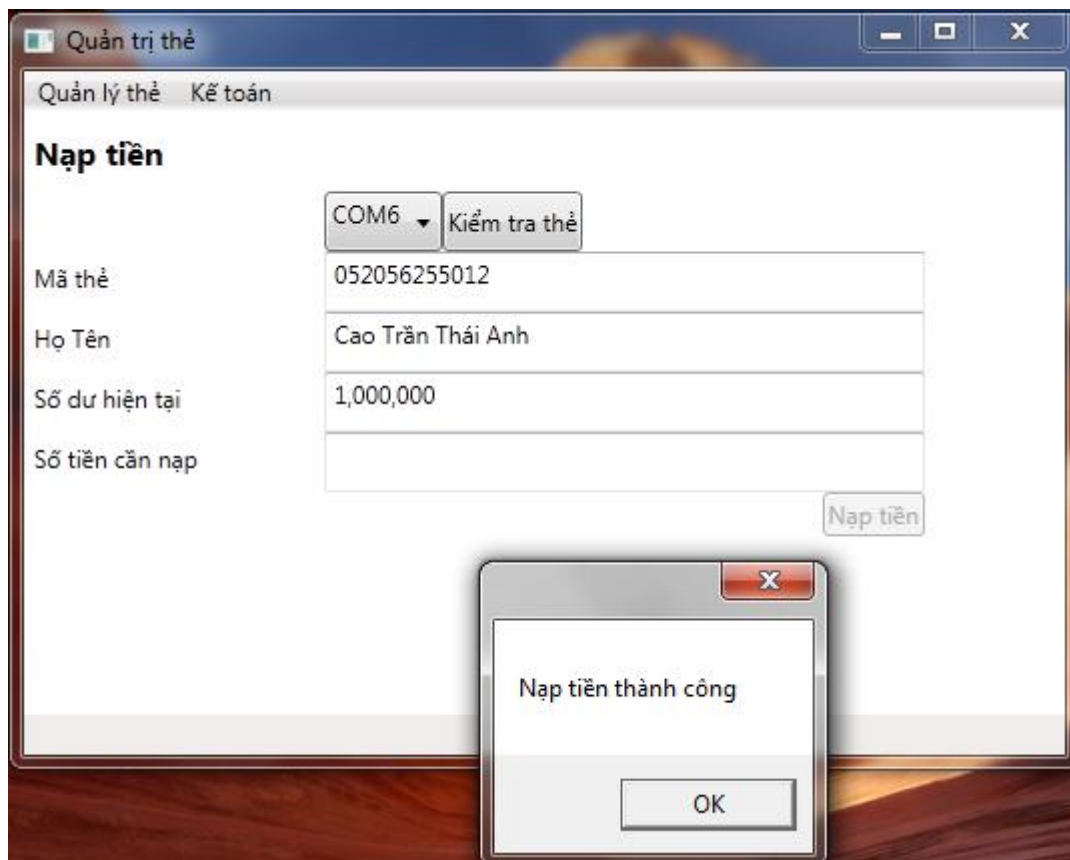
Bước 4: Kiểm tra lại thẻ xem hủy thành công hay không? Click chọn Kiểm tra thẻ → Hiện thị thông báo Thẻ chưa tồn tại.



Kế toán: gồm chức năng nạp tiền



Nạp tiền



Hình 5.6 – Giao diện nạp tiền

Quy trình thực hiện

Bước 1: Táp thẻ vào đầu ghi Mifare AR-737P

Bước 2: Click chọn Kiểm tra thẻ → Hiện thị các thông tin đã ghi trong thẻ

Bước 3: Nhập số tiền cần nạp → Hiện thông báo Hủy thẻ thành công

Bước 4: Click chọn Nạp tiền → Hiện thị thông báo Nạp tiền thành công

5.1.2. Giao diện điểm danh sinh viên

Để thực hiện mô hình này cần các thiết bị sau:

- Đầu đọc Mifare AR-721H
- Wireless Router
- Tablet và ứng dụng Adroid Điểm danh sinh viên

Quy trình thực hiện

Bước 1: Thiết lập và khai các thông tin đề 3 thiết bị này nhận nhau thông qua địa chỉ IP (bước này người dùng không phải thực hiện)

Bước 2: Táp thẻ RFID đã được phát hành vào Đầu đọc Mifare AR-721H → Hiện thông tin sinh viên trên tablet



Hình 5.7 – Giao diện điểm danh

Ghi chú: Mô hình này có thể sử dụng offline, thông tin thẻ sẽ lưu tại tablet

5.1.3. Giao diện thanh toán bằng thẻ tại căn tin

* Màn hình đăng nhập POS (Hệ thống thanh toán tại căn tin)

- Tên đăng nhập: admin
- Mật khẩu: 123456

Đăng nhập

Tên đăng nhập

admin

Mật khẩu

Đăng nhập

Màn hình POS sau khi đăng nhập, gồm 2 chức năng chính: Thanh toán và xem Thông tin tài khoản

Chọn nhóm

Điểm tâm

Món mặn

Nước uống

Ăn vặt

Chọn món

Hóa đơn

Tên	Giá	S.Lượng	Đơn giá
-----	-----	---------	---------

Thành tiền

Chọn lại

Thanh toán

Thông tin tài khoản

2015-05-10 13:13:50

Thanh toán

Chọn nhóm

Điểm tâm

Món mặn

Nước uống

An vát

Chọn món

Trứng Opla
10,000

Bánh mì thịt
10,000

Hủ tiêu
15,000

Phở
20,000

Hóa đơn

Tên	Giá	S.Lượng	Đơn giá
Phở	20,000	1	20,000

Thành tiền

20,000

Chọn lại

Thanh toán

Thông tin tài khoản

2015-05-10 13:14:58

Hình 5.8 – Giao diện thanh toán

Quy trình thực hiện

Bước 1: Táp thẻ vào đầu ghi Mifare AR-737P

Bước 2: Click Chọn nhóm → Hiện thị các món ăn

Bước 3: Chọn món ăn → Hiện thông tin trong mục Hóa đơn

Bước 4: Click chọn Thanh toán → Hiện bảng nhập Mật khẩu và nhập mật khẩu mặc định khi phát hành thẻ là: 123456

Nhập mật khẩu

1	2	3
4	5	6
7	8	9
0	Tiếp tục	

Bước 5: Click vào Tiếp tục → Hiện thị thông tin tài khoản và số tiền cần thanh toán

Số thẻ	052056255012
Số dư	1,000,000
Họ tên	Cao Trần Thái Anh
Thanh toán	20,000
<input type="button" value="Hủy"/> <input type="button" value="Thực hiện"/>	

Bước 6: Click vào Thực hiện → Hiện thị thông báo Thanh toán thành công và đồng thời in hóa đơn thanh toán.

Chọn nhóm

Điểm tâm

Món mặn

Nước uống

An vat

Chọn món

Trứng Opla
10,000

Bánh mì thịt
10,000

Hủ tiêu
15,000

Phở
20,000

Hóa đơn

Tên	Giá	S.Lượng	Đơn giá
Phở	20,000	1	20,000

Thành tiền

20,000

Chọn lại

Thanh toán

Thông tin tài khoản

Thanh toán thành công

OK

2015-05-10 13:24:17

Bước 7: Click chọn OK → Kết thúc quá trình giao dịch

Thông tin tài khoản

Quy trình thực hiện

Bước 1: Táp thẻ vào đầu ghi Mifare AR-737P

Bước 2: Click chọn Thanh toán → Hiện bảng nhập Mật khẩu và nhập mật khẩu mặc định khi phát hành thẻ là: 123456

Nhập mật khẩu

***** Xóa

1	2	3
4	5	6
7	8	9
0	Tiếp tục	

Bước 3: Click vào Tiếp tục → Hiện thị thông tin tài khoản

Thông tin tài khoản

Số thẻ	052056255012
Họ tên	Cao Trần Thái Anh
Mã Sinh viên	1251TT00013
Số dư	980,000

Đổi mật khẩu Thoát

Đổi mật khẩu: Bắt buộc phải thực hiện

Quy trình thực hiện

Bước 1: Táp thẻ vào đầu ghi Mifare AR-737P

Bước 2: Click chọn Thanh toán → Hiện bảng nhập Mật khẩu và nhập mật khẩu mặc định khi phát hành thẻ là: 123456

Nhập mật khẩu

***** Xóa

1 2 3

4 5 6

7 8 9

0 Tiếp tục

Bước 3: Click vào Tiếp tục → Hiện thị thông tin tài khoản

Thông tin tài khoản

Số thẻ 052056255012

Họ tên Cao Trần Thái Anh

Mã Sinh viên 1251TT00013

Số dư 980,000

Đổi mật khẩu Thoát

Bước 4: Click vào Đổi mật khẩu → Hiện thị bảng Nhập mật khẩu mới

Bước 5: Nhập mật khẩu → click vào Tiếp tục → Nhập mật khẩu lần 2 → click vào Tiếp tục → Hiện thị thông báo Đổi mật khẩu thành công

Bước 6: Click vào OK → Kết thúc quá trình đổi mật khẩu

5.2. Triển khai

Hệ thống đang được triển khai tại các cơ quan và doanh nghiệp sau:

- Trường Cao đẳng Công nghệ Thủ Đức
- Công ty TNHH Công nghiệp Vinh Hiền
- Công ty TNHH In Bao bì Ngân Hà
- Công ty TNHH Grace International

5.3. Thử nghiệm hệ thống

Sau khoảng thời gian 2 tháng thử nghiệm tại các cơ quan và doanh nghiệp, có khoảng 250 thẻ RFID được tạo mới.

Theo nhận xét của các cơ quan và doanh nghiệp thì hệ thống điểm danh sinh viên và thanh toán bằng thẻ tại căn tin đều cho kết quả khá tốt và nhận được đánh giá cao (Phiếu khảo sát - phụ lục 2)

5.4. Kết quả đạt được và hướng phát triển

Từ chương 1 đến chương 3, luận văn đã trình bày toàn bộ các tìm hiểu của tôi về hệ thống thẻ RFID nói chung và hệ thống thẻ Mifare, đầu đọc Mifare và đầu ghi Mifare của nhà sản xuất Soyal. Các chương đầu lần lượt trình bày lý do tại sao đề tài được chọn để thực hiện, các nghiên cứu đã có liên quan đến hệ thống thiết bị Mifare của Soyal, chương 3 trình bày về phương pháp mã hóa dữ liệu và mô hình thực hiện phương pháp mã hóa trên thẻ RFID, chương 4 và chương 5 trình bày phần thực hiện thực nghiệm của đề tài: xây dựng ứng dụng điểm danh sinh viên và ứng dụng thanh toán bằng thẻ tại căn tin; Triển khai và đánh giá hệ thống tại các cơ quan và doanh nghiệp. Nội dung trình bày bám sát mục tiêu đề ra ban đầu của luận văn **“Bảo mật dữ liệu trên thẻ RFID - Ứng dụng điểm danh và thanh toán”**.

5.4.1. Kết quả đạt được

- Ứng dụng thành công thuật toán băm SHA1 nhằm mã hóa và bảo mật được dữ liệu trên thẻ RFID để: bảo mật thông tin, chống thay đổi, chống copy.
- Xây dựng thành công 2 ứng dụng điểm danh và thanh toán tại căn tin bằng thẻ RFID.
- Ứng dụng có khả năng xử lý tự động việc điểm danh sinh viên và tạo sự tiện lợi trong việc thanh toán của người dùng khi sử dụng các dịch vụ tại căn tin.
- Hiệu suất (Performance): Thời gian thực hiện điểm danh 1 giây, thanh toán khoảng 3 giây (đã thực hiện bằng phương pháp thủ công là đo bằng đồng hồ trong quá trình thử nghiệm hệ thống).

- Tính sẵn sàng (Availability): Hoạt động 24/ 24, hệ thống sử dụng offline.
- Tiện dụng (Usability): Dễ sử dụng, số lượng thao tác ít.
- Ứng dụng được triển khai thực tế và được đánh giá cao.

Đánh giá chung: với những kết quả đạt được như trên, hệ thống RFID gồm 2 ứng dụng là điểm danh và thanh toán tại căn tin bằng thẻ RFID đáp ứng được yêu cầu đặt ra ban đầu.

5.4.2. Hướng phát triển

- Kết hợp nhiều phương pháp bảo mật dữ liệu trên thẻ RFID.
- Cải thiện thời gian đọc dữ liệu giữa đầu đọc, đầu ghi và thẻ RFID.
- Tăng tốc độ xử lý thuật toán.
- Đề tài còn có thể mở rộng và phát triển theo các hướng ứng dụng sau:
 - Thẻ giữ xe.
 - Thẻ thư viện.
 - Thẻ ra / vào trường.

5.5. Kết luận

Toàn bộ nội dung trình bày trong luận văn là kết quả quá trình nghiên cứu, tìm hiểu của tôi. Các kết quả trình bày trong 5.4.1 là kết quả trong quá trình làm việc, tìm hiểu, học hỏi của tôi. Phần hướng phát triển trình bày trong 5.4.2 là vấn đề chúng tôi ấp ủ và mong muốn thực hiện được trong thời gian tới nhằm giúp cho con người có thể giám sát, quản lý dễ dàng hơn, ít mắc lỗi, tốn ít thời gian, giảm thiểu nhân lực quản lý và bảo vệ dữ liệu của người sử dụng thẻ.

TÀI LIỆU THAM KHẢO

TIẾNG VIỆT

- [1] Bùi Trọng Dục (2007). Nghiên cứu RFID. Luận văn thạc sĩ khoa học – Đại học Bách khoa Hà Nội.
- [2] Nguyễn Văn Hiệp. Công nghệ nhận dạng vô tuyến RFID. Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh.
- [3] Trần Phan Bình (2010). Thiết kế hệ thống quản lý bệnh nhân dùng công nghệ RFID, Đại học Sư phạm Kỹ thuật Hưng Yên.

TIẾNG ANH

- [4] Klaus Finkenzeller (2003). RFID Handbook, Second Edition. Giesecke & Devrient DmbH, Munich, Germany.
- [5] Shahram Moradpour, Manish Bhuptani (2005). RFID Field Guide: Deploying Radio Frequency Identification Systems. Prentice Hall PTR.

TRỰC TUYẾN

- [6] Radio frequency identification, http://en.wikipedia.org/wiki/Radio-frequency_identification
- [7] RFID system, <http://www.rfidjournal.com/>
- [8] Các giải pháp ứng dụng công nghệ RFID tại Việt Nam, <http://smartid.com.vn/>
- [9] Ứng dụng công nghệ RFID tại Mỹ, http://khoahoc.tv/congngghemoi/cong-nghe-moi/46224_giay-thong-minh.aspx
- [10] Ứng dụng công nghệ RFID tại Mỹ, http://khoahoc.tv/congngghemoi/cong-nghe-moi/42484_hoc-sinh-my-duoc-gan-chip-rfid.aspx
- [11] Ứng dụng công nghệ RFID tại Hàn Quốc, http://khoahoc.tv/congngghemoi/cong-nghe-moi/20693_han-quoc-dua-rfid-vao-cuoc-song.aspx

- [12] Ứng dụng công nghệ RFID vào hệ thống ra vào xe lửa tại Malaysia, <http://lifehacker.com/turn-your-rfid-train-pass-or-travel-card-into-a-keychain-1588962002>
- [13] Tình hình phát triển công nghệ RFID tại Việt Nam, <http://www.pcworld.com.vn/articles/kinh-doanh/giai-phap/2009/06/1194171/phan-tien-rfid-tai-viet-nam/>
- [14] Các ứng dụng công nghệ RFID tại Việt Nam: trạm thu phí, bệnh viện, <http://www.thongtincongnghes.com/article/12461>
- [15] Giải pháp kiểm soát ra vào ký túc xá, http://www.hcmus.edu.vn/index.php?option=com_content&task=view&id=6672&Itemid=239
- [16] Giải pháp hệ thống quản lý điều hành kho thông minh, <http://www.selab.hcmus.edu.vn/index.php/nghien-cuu/he-thong-nhung/de-tai-he-thong-nhung/110-nghien-cuu-xay-dung-he-thong-quan-ly-dieu-hanh-kho-thong-minh-smart-warehouse-dua-tren-cong-nghe-rfid-va-he-thong-nhung>
- [17] Giải pháp quản lý thư viện, http://www.hust.edu.vn/web/vi/tin-tuc/-/asset_publisher/WJ2e/content/giai-phap-quan-ly-thu-vien-tu-%C4%91ong-bang-cong-nghe-rfid;jsessionid=2879582191A13B10545D85F5AFE7DC49?redirect=%2Fweb%2Fvi%2Ftin-tuc
- [18] Thẻ Mifare, <https://vi.wikipedia.org/wiki/MIFARE>
- [19] Thẻ Mifare Soyal, <http://www.soyal.com/>
- [20] Thông số kỹ thuật thẻ Mifare, <http://www.soyal.vn/dich-vu-ho-tro/driver-catalog.html>
- [21] Thông tin sản phẩm thẻ Mifare, <http://www.soyal.vn/san-pham/dau-doc-chinh/dau-doc-kiem-soat-ra-vao-soyal-ar-721h.html#thong-tin-san-pham>

[22] Thông số kỹ thuật đầu đọc Mifare Soyal AR-737P, <http://www.soyal.com/product.php?act=view&id=48>

[23] Hàm băm mật mã MD5, <http://vi.wikipedia.org/wiki/MD5>

[24] Hàm băm mật mã SHA, <http://vi.wikipedia.org/wiki/SHA>

[25] Hàm băm mật mã SHA1, <http://en.wikipedia.org/wiki/SHA-1>

[26] Ưu điểm và hạn chế của hệ thống RFID, mic.gov.vn/admin/assets/detai/2007/88_07.doc

[27] So sánh hàm băm MD5 và SHA1, <http://luanvan.co/luan-van/de-tai-gioi-thieu-ma-hoa-du-lieu-sha1-md5-va-demo-ung-dung-52980/>

[28] Android, <http://vi.wikipedia.org/wiki/Android>

[29] C#, <https://msdn.microsoft.com/en-us/library/kx37x362.aspx>

EBOOK

[30] Java Tutorial, <http://www.tutorialspoint.com/>

[31] Android Studio, 2015, http://www.ebookfrenzy.com/pdf_previews/AndroidStudioEssentialsPreview.pdf

[32] William Stallings, 2006, Cryptography and Network Security Principles and Practice, 5th Edition, <https://ovals.files.wordpress.com/2013/03/cryptography-and-network-security-principles-and-practices-4th-ed-william-stallings.pdf>

[33] Faraz Rasheed, C# School, www.programmersheaven.com

[34] Visual Studio 2010, <http://tailieu.vn/doc/moving-to-microsoft-visual-studio-2010-1445963.html>

Phụ lục

Phụ lục 1 – Giới thiệu về Android

1. Giới thiệu về Android

Android [28] là một hệ điều hành dựa trên nền tảng Linux được thiết kế dành cho các thiết bị di động có màn hình cảm ứng như điện thoại thông minh và máy tính bảng. Android ra mắt vào năm 2007, chiếc điện thoại đầu tiên chạy Android được bán vào tháng 10 năm 2008.

2. Kiến trúc hệ điều hành Android

Hệ điều hành android có 4 tầng từ dưới lên trên là tầng hạt nhân Linux (phiên bản 2.6) tầng Libraries & Android runtime, tầng Application Framework và trên cùng là tầng Application.



2.1. Tầng hạt nhân Linux (Linux Kernel layer)

Hệ điều hành android được phát triển dựa trên hạt nhân linux, cụ thể là hạt nhân linux phiên bản 2.6. điều đó được thể hiện ở lớp dưới cùng này. Tất cả mọi hoạt động của điện thoại muốn thi hành được thì đều được thực hiện ở mức cấp thấp bao gồm: quản lý bộ nhớ (memory management), giao tiếp với phần cứng (driver model), thực hiện bảo mật (security), quản lý tiến trình (process).

Tuy được phát triển dựa vào nhân linux nhưng thực ra nhân linux đã được nâng cấp và sửa đổi rất nhiều để phù hợp với tính chất của thiết bị cầm tay như hạn chế về bộ vi xử lý, dung lượng bộ nhớ, kích thước màn hình, nhu cầu kết nối mạng không dây.

2.2. Tầng Libraries và Android runtime

Phần Libraries: phần này có nhiều thư viện được viết bằng C/C++ để các phần mềm có thể sử dụng, các thư viện đó được tập hợp thành 1 nhóm như:

- Thư viện hệ thống (System C library): thư viện dựa trên chuẩn C, được sử dụng chỉ bởi hệ điều hành
- Thư viện Media (Media Libraries): có nhiều code để hỗ trợ việc phát và ghi các loại định dạng âm thanh, hình ảnh, video thông dụng.
- Thư viện web (LibWebCore): đây là thành phần để xem nội dung trên web, được sử dụng để xây dựng phần mềm duyệt web cũng như để các ứng dụng khác có thể nhúng vào. Hỗ trợ nhiều công nghệ mạnh mẽ như HTML5, JavaScript, CSS, DOM, Ajax...
- Thư viện SQLite: là hệ cơ sở dữ liệu để các ứng dụng có thể sử dụng.

2.3. Phần Android runtime

Phần này chứa các thư viện mà một chương trình viết bằng ngôn ngữ Java có thể hoạt động. Phần này có hai bộ phận tương tự như mô hình chạy Java trên máy tính thường. Thứ nhất là các thư viện lõi (Core library), chứa các lớp như Java Io, Collection, File Access. Thứ hai là một máy ảo Java (Dalvik Virtual Machine). Mặc dù cũng được viết bởi ngôn ngữ Java nhưng một số ứng dụng Java của hệ điều hành android không chạy bằng JRE của Sun (nay là Oracle) mà là chạy bằng máy ảo Dalvik do Google phát triển.

2.4. Tầng Application Framework

Tầng này xây dựng công cụ - các phần tử ở mức cao để lập trình viên có thể nhanh chóng xây dựng ứng dụng. Nó được viết bằng Java, có khả năng sử dụng chung để tiết kiệm tài nguyên.

2.5. Tầng Application

Đây là lớp ứng dụng giao tiếp với người dùng, bao gồm các ứng dụng như:

Các ứng dụng cơ bản, được cài đặt đi liền với hệ điều hành là gọi điện thoại, quản lý danh bạ, duyệt web, nhắn tin, lịch làm việc, bản đồ, quay phim chụp ảnh,...

Các ứng dụng được cài thêm như các phần mềm từ điển, trò chơi,...

Các phần mềm có đặc điểm là viết bằng Java, phần mở rộng là apk.

3. Android Studio

3.1. Giới thiệu

Android Studio [31], môi trường lập trình phát triển ứng dụng mới vừa được giới thiệu tại Google I/O 2013. Dựa trên “IntelliJ IDEA Community Edition”, công cụ này hoạt động giống WYSIWYG, cho phép lập trình viên tạo ứng dụng, dễ dàng thực hiện các thay đổi và xem trước trong thời gian thực, đồng thời cũng có khả năng tăng tốc sản phẩm, thiết kế giao diện đẹp hơn trước. Đặc biệt là tiếng Việt cũng được hỗ trợ trong Android Studio.

3.2. Các đặc điểm

- Được xây dựng dựa trên IntelliJ IDEA Community Edition, Java IDE phổ biến của JetBrains.
- Hệ thống xây dựng dựa trên Gradle linh động
- Tạo lập nhiều phương án và Multiple AP cho các API Levels khác nhau
- Hỗ trợ template được mở rộng cho các dịch vụ của Google và các thiết bị khác nhau.
- Biên tập layout phong phú hỗ trợ chỉnh sửa theme
- Công cụ lint để bắt hiệu suất, khả năng sử dụng, phiên bản tương thích và các vấn đề liên quan khác.
- Bảo vệ chuyên nghiệp ProGuard và khả năng tạo sign app.
- Hỗ trợ Build-in cho nền tảng đám mây của Google, từ đó có thể dễ dàng tích hợp Google Cloud Messaging và App Engine.

3.3. Các phiên bản android

Phần lớn các thiết bị Android cho tới nay vẫn chạy hệ điều hành phiên bản 4.1.x Jelly Bean được phát hành ngày 9 tháng 7 năm 2012 nhờ tính ổn định và hỗ trợ tốt các máy có cấu hình thấp.

Phiên bản ⇅	Tên mã ⇅	Ngày phát hành ⇅	Cấp API ⇅	Phân bố (20 tháng 7 năm 2014) ⇅
5.0	<i>Lollipop</i>	tháng 7 năm 2014	20	Dành cho người phát hành
4.4	<i>KitKat</i>	tháng 10 năm 2013	19	17,9%
4.3	<i>Jelly Bean</i>	25 tháng 7 năm 2013	18	10,5%
4.2.x	<i>Jelly Bean</i>	13 tháng 11 năm 2012	17	18,8%
4.1.x	<i>Jelly Bean</i>	9 tháng 7 năm 2012	16	25,2%
4.0.x	<i>Ice Cream Sandwich</i>	16 tháng 12 năm 2011	15	11,4%
3.2	<i>Honeycomb</i>	15 tháng 7 năm 2011	13	0%
3.1	<i>Honeycomb</i>	10 tháng 5 năm 2011	12	0%
2.3.3–2.3.7	<i>Gingerbread</i>	9 tháng 2 năm 2011	10	13%
2.3–2.3.2	<i>Gingerbread</i>	6 tháng 12 năm 2010	9	0,5%
2.2	<i>Froyo</i>	20 tháng 5 năm 2010	8	0,7%
2.0–2.1	<i>Eclair</i>	26 tháng 10 năm 2009	7	0%
1.6	<i>Donut</i>	15 tháng 9 năm 2009	4	0%

Phụ lục 2: Phiếu khảo sát

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

PHIẾU KHẢO SÁT

Xin chân thành cảm ơn Quý Cơ quan/Doanh nghiệp đã đồng ý cho tôi thử nghiệm 2 ứng dụng quản lý Sinh viên và Thanh toán tại Căn tin. Tôi rất cảm kích nếu Cơ quan/Doanh nghiệp dành một chút thời gian để nhận xét, đánh giá về 2 ứng dụng theo mẫu dưới đây. Những đóng góp quý báu của Cơ quan/Doanh nghiệp sẽ giúp tôi hoàn thiện và bổ sung thêm những tính năng của 2 ứng dụng này trong tương lai.

Trân trọng!

Tên Cơ quan/Doanh nghiệp:

Địa chỉ:

NỘI DUNG ĐÁNH GIÁ

Cơ quan/Doanh nghiệp đánh giá thế nào về tính hữu ích của 2 ứng dụng?

1= Chẳng có ích gì, 5= Rất hữu ích

	1	2	3	4	5	
Chẳng có ích gì						Rất hữu ích

Cơ quan/Doanh nghiệp đánh giá thế nào về tốc độ xử lý dữ liệu của 2 ứng dụng?

1= Rất tệ, 5= Rất tốt

	1	2	3	4	5	
Rất tệ						Rất tốt

Những tính năng nào của 2 ứng dụng mà Cơ quan/Doanh nghiệp ưng ý?

- ☐ Bảo mật dữ liệu trên thẻ
- ☐ Thanh toán qua thẻ
- ☐ Điểm danh/Chấm công offline
- ☐ Thanh toán offline
- ☐ Ý kiến khác:

Cơ quan/Doanh nghiệp đã từng sử dụng hệ thống quản lý nào dưới đây

- ☐ Điểm danh/Chấm công bằng công nghệ vân tay
- ☐ Điểm danh/Chấm công/Thanh toán sử dụng công nghệ RFID
- ☐ Điểm danh/Chấm công/Thanh toán sử dụng công nghệ NFC
- ☐ Những công nghệ khác:
- ☐ Chưa từng sử dụng

Cơ quan/Doanh nghiệp có muốn lắp đặt và sử dụng 2 ứng dụng này trong tương lai?

- ☐ Có
- ☐ Không

Các ý kiến góp ý khác

.....

.....

.....

.....

Đại diện Cơ quan/Doanh nghiệp