

ĐẠI HỌC QUỐC GIA TP.HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA ĐIỆN – ĐIỆN TỬ
BỘ MÔN VIỄN THÔNG

-----oo-----



LUẬN VĂN TỐT NGHIỆP ĐẠI HỌC

**ỨNG DỤNG MÃ HÓA RSA THIẾT KẾ BÃI GIỮ XE
THÔNG MINH**

**GVHD: TS. Lưu Thanh Trà và
ThS. Đinh Quốc Hùng**
SVTH: Phạm Hiển Long
MSSV: 1412103

TP. HỒ CHÍ MINH, THÁNG 6 NĂM 2019



ĐẠI HỌC QUỐC GIA TP.HỒ CHÍ MINH CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
TRƯỜNG ĐẠI HỌC BÁCH KHOA

Độc lập – Tự do – Hạnh phúc.

-----☆-----

-----☆-----

Số: _____ /BKDT
Khoa: **Điện – Điện tử**
Bộ Môn: **Viễn Thông**

NHIỆM VỤ LUẬN VĂN TỐT NGHIỆP

1. HỌ VÀ TÊN: PHẠM HIỀN LONG
2. NGÀNH: **ĐIỆN TỬ - VIỄN THÔNG**
3. Đề tài: Ứng dụng mã hóa RSA thiết kế bãi giữ xe thông minh
4. Nhiệm vụ (Yêu cầu về nội dung và số liệu ban đầu):

Tìm hiểu về mã hóa RSA . Ứng dụng nó vào chư ký điện tử Từ đó thiết kế một hệ thống bãi giữ xe thông minh, cụ thể trong Luận văn là máy tính nhúng Raspberry. Cuối cùng là đánh giá kết quả thực hiện, hướng phát triển cho đề tài.

5. Ngày giao nhiệm vụ luận văn: 14/1/2019.....
6. Ngày hoàn thành nhiệm vụ: 21/6/2019.....
7. Họ và tên người hướng dẫn:
TS. Lưu Thanh Trà
ThS. Đinh Quốc Hùng.....

Phản hướng dẫn

.....
.....

Nội dung và yêu cầu LVTN đã được thông qua Bộ Môn.

Tp.HCM, ngày..... tháng..... năm 20
CHỦ NHIỆM BỘ MÔN

NGƯỜI HƯỚNG DẪN CHÍNH

PHẦN DÀNH CHO KHOA, BỘ MÔN:

Người duyệt (châm sơ bộ):.....

Đơn vị:.....

Ngày bảo vệ :

Điểm tổng kết:

Nơi lưu trữ luận văn:

LỜI CẢM ƠN

Lời đầu tiên, em xin gửi lời cảm ơn chân thành đến tất cả quý Thầy/Cô giảng dạy tại khoa Điện tử Viễn Thông cũng như quý Thầy/Cô ở Trường Đại học Bách Khoa TP.HCM đã trang bị cho em những kiến thức cơ sở quý báu cũng như giúp đỡ em trong suốt quá trình học tập tại trường.

Qua đây em xin bày tỏ lòng biết ơn sâu sắc đối với thầy Lưu Thanh Trà và thầy Đinh Quốc Hùng, người đã dành nhiều thời gian, tâm huyết hướng dẫn tận tình trong thời gian thực hiện đề tài Luận văn tốt nghiệp.

Em xin gửi lời cảm ơn chân thành đến quý Thầy/Cô đã dành thời gian quý báu để nhận xét và cho em những lời khuyên xác đáng, chỉ ra những sai sót trong Luận văn tốt nghiệp. Đây là những đóng góp quý báu giúp em nhận ra những sai sót và kiến thức còn thiếu.

Cuối cùng, em xin gửi lời cảm ơn đến ba mẹ, những người thân trong gia đình đã hết lòng ủng hộ, động viên để em có thể vượt qua khó khăn trong quá trình học tập và hoàn thành Luận văn tốt nghiệp này.

Tp. Hồ Chí Minh, ngày 11 tháng 6 năm 2019 .

Sinh viên

TÓM TẮT LUẬN VĂN

Trong thời đại công nghiệp hiện nay, mọi hoạt động trong xã hội đều hướng tới sự tự động , ít có sự can thiệp của con người. Do đó, việc một bãi giữ xe có tính tự động là một điều cần thiết. Hơn nữa, việc xác thực và bảo mật ở các bãi giữ xe luôn gặp vấn đề khó khi có qua nhiều xe và ngày càng có nhiều tội phạm có thể phá hệ thống giữ xe. Vì vậy việc sử dụng một hệ thống bảo mật và xác thực cao là rất cần thiết

Luận văn này trình bày quá trình thiết kế hệ thống xác thực bãi giữ xe , thông qua mã hóa RSA . Mã hóa RSA được sử dụng để thực hiện chữ ký điện tử và nén vào QR Code . Quá trình giao tiếp của khách hàng sẽ thông qua chiếc điện thoại smartphone . Hệ thống xác thực sẽ sử dụng máy tính nhúng raspberry và camera

Để xác thực chữ ký điện tử chúng ta sẽ dùng các thuật toán mã hóa và giải mã RSA . Ngôn ngữ lập trình sử dụng trong luận văn gồm Python , Java (Netbean và Android) .

Nội dung chính gồm các chương:

Chương 1: Tìm hiểu đề tài

Chương 2: Cơ sở lý thuyết

Chương 3: Thiết kế phần cứng và phần mềm

Chương 4: Thực hiện phần cứng và phần mềm

Chương 5: Hoạt động , đánh giá

Chương 6: Kết luận



Mục lục

1 Chương 1 : TÌM HIỂU ĐỀ TÀI	6
1.1 Các loại giữ xe hiện nay	6
1.1.1 Bãi giữ xe truyền thống	6
1.1.2 Thẻ từ RFID	7
1.1.3 Yêu cầu về bãi giữ xe	8
1.1.4 Khảo sát các giải pháp	9
1.2 Nhu cầu về một bãi giữ xe thông minh	10
1.3 Lựa chọn phương án cho bãi giữ xe	11
1.3.1 Board xác thực	11
1.3.2 Giao tiếp giữa khách hàng và board xác thực	11
1.3.3 Tìm hiểu về khóa	13
1.3.4 Lựa chọn loại mã hóa	13
1.4 Tổng kết	14
2 Chương 2 : CƠ SỞ LÝ THUYẾT	15
2.1 Các loại mã đọc	15
2.1.1 Barcode	15
2.1.2 QR Code	16
2.1.3 So sánh giữa Barcode và QR Code	17
2.2 Lựa chọn hàm băm	18
2.2.1 Tính chất hàm băm	18
2.2.2 Một số loại mã băm	19
2.3 Mã hóa bất đối xứng	19
2.3.1 Quá trình hoạt động của hệ mã hóa bất đối xứng	19
2.3.2 Lựa chọn loại mã hóa	20
2.3.3 Khóa trong hệ mã hóa bất đối xứng	20
2.3.4 Lý thuyết số	21
2.3.5 Quá trình tạo khóa	22
2.3.6 Mã hóa và giải mã trong RSA	23
2.4 Chữ ký điện tử	23
2.4.1 Luật giao dịch điện tử (Việt Nam), điều 4 định nghĩa	23
2.4.2 Công nghệ xác minh chữ ký điện tử	24
2.5 Chuỗi JSON	24
3 Chương 3 : THIẾT KẾ PHẦN CỨNG VÀ PHẦN MỀM	26
3.1 Thành phần hệ thống	27
3.1.1 Cấu trúc và chức năng mỗi phần tử	28
3.2 Các ứng dụng trong luận văn	32



3.2.1	Ứng dụng gửi xe	32
3.2.2	Ứng dụng trả xe	32
3.2.3	Ứng dụng cho mượn xe (Ủy quyền)	33
3.2.4	Ứng dụng mượn xe	35
3.3	Cơ sở dữ liệu khách hàng	37
3.4	Hệ thống xác thực trên Raspberry	37
3.5	PKI (Public-Key Infrastructures)	39
3.5.1	CA Server	39
3.5.2	Public-Key Infrastructures	39
3.6	Tổng kết	39
4	Chương 4 : THỰC HIỆN PHẦN CỨNG VÀ PHẦN MỀM	40
4.1	Sơ đồ nối dây	40
4.2	Phần mềm Gửi xe trên Android	42
4.3	Phần mềm Trả xe và Cho mượn trên Android	45
4.3.1	Trả xe	45
4.3.2	Cho mượn xe	46
4.4	Phần mềm mượn xe	46
4.5	Cơ sở dữ liệu trên raspberry	47
4.6	Hệ thống xác thực trên Raspberry	48
4.7	Ứng dụng CA Server trên Java-Netbeans	51
4.8	Tổng Kết	53
5	Chương 5 : HOẠT ĐỘNG , ĐÁNH GIÁ	54
5.1	Mức độ hoàn thành trong luận văn	54
5.2	Kịch bản sử dụng	55
5.3	Hoạt Động , Đánh Giá	57
5.4	Mở rộng , hướng phát triển	60
5.4.1	Hierarchial Model	60
5.4.2	Ứng dụng mô hình Hierarchial vào hệ thống	61
5.5	Tổng Kết	62
6	Chương 6 : KẾT LUẬN	63

Danh sách hình vẽ

1.1	Phiếu giữ xe	7
1.2	Khách hàng tại bãi giữ xe	7
1.3	Mô hình thẻ từ RFID	8
1.4	Máy tính nhúng Raspberry Pi 3	12
1.5	Hình ảnh quá trình mã hóa công khai	13
2.1	Hình ảnh một Barcode	16
2.2	Hình ảnh một QR Code	16
2.3	Cấu trúc 1 QR Code	17
2.4	Kết quả băm 1 chuỗi từ Netbean	18
2.5	Quá trình hoạt động của hệ mã hóa RSA	20
2.6	Khóa và mở khóa trong mã hóa bất đối xứng	21
2.7	Hệ thống tạo khóa trên CA Server trong luận văn	22
2.8	Mô hình tạo và xác thực chữ ký điện tử trong luận văn	24
2.9	Cấu trúc của 1 chuỗi JSON	24
2.10	Cấu trúc 1 chuỗi JSON trong đề tài	25
3.1	Hệ thống thực tế	26
3.2	Hệ thống thực tế	27
3.3	Raspberry Pi 3 Model B	28
3.4	Camera Pi 3 5MP	29
3.5	Module Realy 5VDC	30
3.6	Màn hình LCD	31
3.7	Các thành phần phụ kết nối với Raspberry	31
3.8	Giao diện ứng dụng gửi xe	32
3.9	Giao diện ứng dụng mượn xe và trả xe	33
3.10	Khách hàng tạo QR Code để trả xe	34
3.11	Khách hàng tạo QR Code cho mượn xe	35
3.12	Khách hàng nhận được email từ nhà xe	36
3.13	Khách hàng khi tạo QR Code	36
3.14	Camera được bật lên khi khách hàng lưu QR Code của người cho mượn	37
3.15	Cơ sở dữ liệu khách hàng trên raspberry	38
3.16	Hệ thống xác thực khi đang thực hiện	38
4.1	Sơ đồ nối dây của hệ thống	41
4.2	Sơ đồ chân Raspberry PI 3	42
4.3	Lưu đồ giải thuật cho ứng dụng gửi xe	43
4.4	Nội dung của QR Code khi scan vào raspberry	44
4.5	Lưu đồ giải thuật ứng dụng trả xe và cho mượn	45

4.6	Lưu đồ giải thuật của ứng dụng mượn xe	47
4.7	Cơ sở dữ liệu của Raspberry	48
4.8	Lưu đồ giải thuật hệ thống xác thực	49
4.9	PKI trong luận văn	51
4.10	Database cho khách hàng trong PKI	52
4.11	Hệ thống thông báo khi tạo khóa thành công	52
4.12	Hệ thống thông báo khi thêm khách hàng thành công	53
5.1	Khách hàng gửi xe thành công	56
5.2	Relay hệ thống bật	56
5.3	Khách hàng cho mượn xe	57
5.4	Khách hàng lưu QR Code cho mượn	58
5.5	Hệ thống hoạt động với 20 người	58
5.6	Hệ thống hoạt động với 40 người	59
5.7	Mô hình PKI Hierarchical	61
5.8	Mô hình PKI Hierarchical	61

Danh sách bảng

1.1	Các giải pháp đặt ra	10
1.2	So sánh các board xác thực	12
5.1	Các mục tiêu đặt ra và mức độ hoàn thành	55
5.2	So sánh lưu lượng xe của các giải pháp	60

Chương 1

TÌM HIỂU ĐỀ TÀI

Hiện nay , đa phần trong thực tế hiện nay chúng thường thấy bãi giữ xe sử dụng thẻ từ , hoặc các hệ thống xác thực sinh trắc học . Các hệ thống này tuy tiện dụng nhưng lại chứa khá nhiều tính không tiện dung . Như khách hàng phải đem theo thẻ , hoặc nhiều lúc hệ thống thông dùng sinh trắc học có thể bị mở khóa khi biết được đặc điểm của chủ sở hữu . Cho nên trong luận văn này sẽ giới thiệu một hệ thống tốt hơn có thể giao tiếp thân thiện hơn với khách hàng thông qua smart phone . có thể kiểm soát được ai đang mượn xe , hoặc hệ thống có thể mở rộng lên với rất nhiều xe . Và điều quan trọng chính là bảo mật rất an toàn , có thể mất hơn 1000 năm mới bẻ được khóa , dường như đó là mức an toàn tuyệt đối . Chương 1 sẽ tìm hiểu đề tài và lựa chọn các phương án để thực hiện

1.1 Các loại giữ xe hiện nay

1.1.1 Bãi giữ xe truyền thống

Hiện nay ở Việt Nam bãi giữ xe luôn là một vấn đề đáng được quan tâm . Các bãi giữ xe quá tải , hàng người nối đuôi nhau, hay thái độ phục vụ của nhân viên ,... luôn làm cho khách hàng phiền toái . Người kỹ sư luôn nghĩ rằng phải làm cách nào để có thể có một bãi giữ xe an toàn , tự động , hiện đại hơn so với các bãi giữ xe truyền thống một nhân viên ghi số lên yên xe hay bấm tờ giấy trên kính chiếu hậu khi vào , đưa cho khách hàng một mẫu giấy có cùng số . Và khi ra người nhân viên kiểm tra lại số trên tờ giấy đó .Đương nhiên trên tờ giấy đó chắc chắn phải có chữ ký thủ công của người nhân viên hay chủ bãi giữ xe . Thường khi giữ xe bằng phương pháp này chắc chắn chúng ta thường khóa cổ xe lại .



Hình 1.1: Phiếu giữ xe



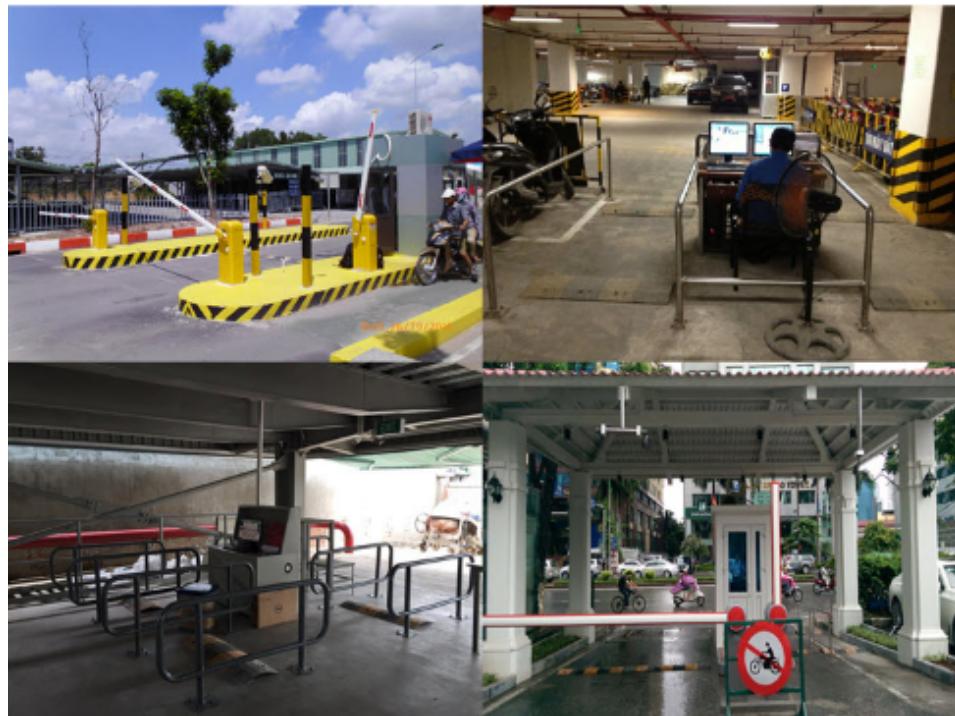
Hình 1.2: Khách hàng tại bãi giữ xe

Dương nhiên cách này có quá nhiều khuyết điểm . Khi số lượng xe gửi nhỏ thì tốt nhưng khi số lượng xe quá nhiều . Lúc này việc kiểm tra bằng mắt thường của người nhân viên có thể xảy ra sai sót . Và việc quản lý xe chỉ bằng một mẫu giấy thì có vẻ khá nguy hiểm . Lúc đó một ý tưởng tuyệt vời đã được sáng kiến là tích hợp thẻ xe đó thành thẻ từ RFID

1.1.2 Thẻ từ RFID

Như vậy gần như mọi vấn đề trên đã được giải quyết , an toàn , hiện đại và tự động . Người nhân viên giữ xe chỉ việc nhìn lên màn hình giữ xe kiểm tra số hay mã hoặc được ghi trong thẻ từ . Nội dung ghi trong thẻ từ có thể là thời gian hoặc số hoặc biển số xe . Cuối cùng sắp xếp và phát thẻ từ. Còn khách hàng khi cần gửi xe hay trả xe thì đi vào vạch quy định nhận lấy thẻ từ hoặc đưa lại thẻ từ cho nhân viên

Nhưng lúc đó các vấn đề tiếp theo được đặt ra cho thấy thẻ từ cũng gấp một số vấn đề phức tạp



Hình 1.3: Mô hình thẻ từ RFID

Khó khăn khi sử dụng thẻ từ:

1. Một vấn đề được nảy sinh ngay lập tức đó là khách hàng phải giữ thẻ từ ở mọi lúc mọi nơi . Và khi gấp vấn đề về thẻ mất thẻ , gây thẻ thì đầu tiên người tốn tiền sẽ là khách hàng , khi mỗi lần xảy ra trường hợp này thì khách hàng có thể mất từ 50000 - 100000 VND
2. Do khách hàng luôn phải giữ thẻ bên mình nên tiếp tục nảy sinh ra một vấn đề đau đầu . Có quá nhiều thẻ nằm trên một người . Thẻ ngân hàng , thẻ ở cửa hàng tiện ích , thẻ sinh viên , và giờ thêm cả thẻ gửi xe nữa .Thêm vào đó nếu hệ thống được lắp đặt tự động ở một công ty hay tòa nhà , lúc này không có nhân viên và mỗi người được phát một thẻ RFID cố định . Vậy vấn đề sẽ xảy ra nếu chúng ta tới công ty mà quên thẻ từ ở nhà.
3. Trường hợp khi cho mượn xe thì nhà xe không quản lý được việc cho mượn xe . Khách hàng A khi mượn xe khách hàng B thì chỉ cần gấp khách hàng B lấy thẻ từ và chìa khóa , nhà xe không quản lý được việc này
4. Vấn đề quan trọng nhất là hệ thống chỉ hoạt động được trong một tòa nhà . Khi hệ thống mở rộng lên nhiều tòa nhà thì sẽ khó có mô hình phát triển

1.1.3 Yêu cầu về bãi giữ xe

Như vậy một vấn đề được đặt ra là làm thế nào thiết kế được một hệ thống an toàn , tự động , mà còn có thể mở rộng lớn hơn sau này .

Yêu cầu tối thiểu của hệ thống :

- Giải quyết vấn đề xác thực một cách chính xác
- Giải quyết được tính tự động tức là việc xác thực kiểm tra sẽ do máy tính không còn thông qua mắt con người
- Tối ưu tính tiện dụng , giải quyết được bài toán khách hàng phải đem thẻ RFID theo bên mình
- Giải quyết được tối thiểu một vài trường hợp mượn xe mà nhà xe vẫn quản lý được người mượn và người cho mượn
- Giá cả hợp lý , board xác thực nằm trong tầm 1 2 triệu VND

1.1.4 Khảo sát các giải pháp

Có nhiều giải pháp được đặt ra . Bảng 1.1 trình bày kết quả khảo sát . Các giải pháp bên dưới đều có thể giải quyết được một số vấn đề . Chẳng hạn như hệ thống sinh trắc học . Khi gửi xe khách hàng có thể nói vào thiết bị tại nhà xe hoặc nhà xe có camera để nhận diện khuôn mặt , tương ứng với biển số xe . Giải pháp này giải quyết được triệt để vấn đề thẻ từ RFID nhưng những vấn đề sinh trắc học xảy ra đòi hỏi phải nhận diện được khuôn mặt đó hay là tấm ảnh họa mặt nạ.

Tương tự như vậy khi sử dụng ghi nhớ mật khẩu khi xe vào nhà xe sẽ tạo 1 mật khẩu tương ứng với biển số xe . Khi đó khách hàng phải nhớ mật khẩu đến khi ra hệ thống xác thực sẽ yêu cầu khách hàng nhập lại . Phương án này cũng có thể giải quyết được vấn đề thẻ từ nhưng việc phải ghi nhớ mật khẩu làm cho mật khẩu không thể quá phức tạp dẫn đến không an toàn và có thể làm phiền khách hàng

Ngoài ra , còn có thể cài tiến thẻ từ RFID , tức 1 thẻ RFID có thể làm tất cả mọi nhiệm vụ từ cửa hàng tiện ích đến khi gửi xe . Nhưng khi đó quá phụ thuộc vào thẻ từ và khi mất có thể xảy ra nhiều vấn đề . Đồng thời khi đó thì các cửa và phần mềm xác thực của bãi giữ xe cũng phải thống nhất với các cửa hàng khác , điều đó cũng gây vài khó khăn

Các giải pháp	Ưu điểm và khuyết điểm
Các hệ thống xác thực sử dụng sinh trắc học (face ID , vân tay ,giọng nói,...)	Tiện nghi cao loại bỏ được thẻ từ . Nhưng dễ ảnh hưởng khi các yếu tố sinh trắc như vân tay, mống mắt bị thay đổi . Hơn nữa nếu hệ thống dùng face ID , thì khi biết được chủ sở hữu có thể sẽ bị bẻ khóa
Sử dụng thẻ từ RFID cài tiến có thẻ 1 thẻ làm nhiều nhiệm vụ , thẻ ở cửa hàng tiện ích có thẻ gửi xe luôn	Tiện nghi chưa cao vì cơ bản vẫn chưa loại bỏ được thẻ từ . Đòi hỏi về thiết bị khá tốn kém khi nhà xe phải tích hợp thêm đầu đọc thẻ ở cửa hàng tiện ích .Ngoài ra tính bảo mật của thẻ từ chưa phải là cao nhất
Các hệ thống xác thực dùng phương pháp truyền thống, sử dụng mật khẩu do người dùng nhập vào	Tiện nghi cao vì người dùng không cần phải mang theo bên mình các thẻ , nhưng đòi hỏi người dùng phải nhớ , và tính bảo mật không được cao

Bảng 1.1: Các giải pháp đặt ra

1.2 Nhu cầu về một bãi giữ xe thông minh

Như vậy mỗi giải pháp chúng ta đạt ra điều có hai điều khá quan trọng Thứ nhất là tính bảo mật . Các giải pháp giữ xe được đề ra tính bảo mật chưa phải là cao nhất .Thứ hai đó tuy không phải là vấn đề trước mắt nhưng rất cần thiết sau này đó là tính mở rộng sau này . Chúng ta thử phân tích tính bảo mật trước .Giả sử hệ thống dùng thẻ từ RFID . Như vậy trong thẻ từ nếu như chúng ta có một đầu đọc hì chúng ta sẽ biết được nội dung ở bên trong và đồng thời thẻ từ đó sẽ có thẻ lấy xe sau khi gửi . Nếu có ai đọc được nội dung thẻ từ chuyển nó qua một thẻ tràn khác thì hoàn toàn có thể lấy xe ra . Với các hệ thống faceID thì cách bẻ hệ thống có thể xảy ra nhiều nhất chính là scan một hình ảnh hay mặt nạ giống với khách hàng khi gửi xe là có thể lấy được xe. Tương tự với hệ thống sử dụng cách nhập mật khẩu . Nếu có ai đó quan sát được lúc người gửi xe hay quay phim lại thì hoàn toàn có thể bẻ gãy hệ thống được. Như vậy điều chúng ta cần là một nhu cầu về bãi giữ xe thông minh mà khi đó công cụ để gửi

xe vào khi bị quan sát thấy hay bị can thiệp bởi các thiết bị điện tử thì không thể lấy được xe ra . Do đó chúng ta cần một giải pháp về mã hóa . Khi khách hàng gửi xe sẽ tạo một loại mã đọc , khách hàng trả xe cũng tạo lại một loại mã đọc nhưng khách về nội dung và nội dung về mã đọc khi trả xe sẽ có ảnh hưởng đến nhà xe . Điều này sẽ làm cho khi khách hàng gửi xe và nếu có bị ai đó chụp lại màn hình thì lúc này cũng không thể crack được hệ thống và lấy được xe ra .

Tiếp tục chúng ta xét đến tính mở rộng của một hệ thống . Dường như các bãi giữ xe khó có thể mở rộng theo một mô hình nào đó , và khách hàng thường được không cố định khi khách hàng vào . Đó cũng là một điểm mạnh khi khách hàng không cần phải bận tâm đó là bãi giữ xe nào và của chủ sở hữu nào và khi cần thì có thể gửi xe ngay . Nhưng với hệ thống giữ xe sử dụng mã hóa vì khi gửi xe các hệ thống xác thực của nhà xe cần phải dùng các key lưu trong cơ sở dữ liệu để xác thực như vậy khi khách hàng đang ký ở một bãi xe khách nung muôn gửi ở một bãi xe khách cũng do chúng ta thiết kế hệ thống xác thực nhưng khác chủ sở hữu ví dụ hai tòa nhà có hai chủ sở hữu khác nhau vậy khi khách hàng ở toàn nhà một muốn gửi xe cho tòa nhà khách hàng hai thì lúc này cần phải có một mô hình để liên kết các toàn nhà lại với nhau . Điều này hoàn toàn có thể xảy ra khi có rất nhiều mô hình mở rộng trên một hệ thống mạng ứng dụng mã hóa

Như vậy cho dù là tính ảo mật hay tính mở rộng thi chúng ta cũng cần một hệ thống bãi giữ xe thông minh có tính bảo mật dường như tuyệt đối và đồng thời cũng phải có phương án mở rộng để có thể mở rộng nó khi cần thiết

1.3 Lựa chọn phương án cho bãi giữ xe

Như vậy chúng ta cần lựa chọn phương án cho một giải pháp bãi giữ xe thông minh này

1.3.1 Board xác thực

Yêu cầu:

- Có kết nối camera để có thể nhận diện và xử lý ảnh
- Có thể lập trình để giải mã hoặc mã hóa và điều khiển các relay để đóng hoặc mở .

Như vậy dựa vào bảng khảo sát 1.2 chúng ta thấy rằng chúng ta có thể dùng các board xác thực khác nhau nhưng do chi phí cũng như tính thích hợp thì chúng ta sẽ chọn máy tính nhúng sẽ phù hợp với luận văn này.Như vậy chúng ta có thể sử dụng máy tính nhúng raspberry pi 3 để sử dụng và module camera pi 3 có tích hợp sẵn trên kit

1.3.2 Giao tiếp giữa khách hàng và board xác thực

Như vậy chúng ta cần thiết kế một cách thức để khách hàng có thể giao tiếp với nhau thông qua board xác thực . Thực tế chúng ta có rất nhiều loại mã đọc sẽ trình bày kỹ hơn trong mục 2.1 . Thường chúng ta sẽ có barcode hoặc QR Code. Và với thời đại hiện nay thì việc sở hữu 1 chiếc smart phone là một điều thường thấy . Như vậy chúng ta có thể sử dụng điện thoại cá nhân lập trình trên phần mềm android hoặc IOS . Ngoài ra trên chiếc điện thoại chúng ta có sẵn bộ vi xử lý cùng với camera trên điện thoại . Như vậy điều chúng ta cần là những app trên điện thoại android . Nhưng vì tính phổ biến nên trong luận văn này các app sẽ được viết trên android

Các tính năng	Máy tính nhúng	Máy tính	Các board xử lý ảnh chuyên dụng
Kích thước	Nhỏ gọn	Lớn	Nhỏ gọn
Tốc độ xử lý	Thấp	Cao	Rất cao
Camera có thể sử dụng	camera pi 3, camera USB	camera USB, webcam	camera công nghiệp
Tính chuyên dụng và khả năng lập trình	Lập trình dễ dàng, kết nối vi điều khiển tốt	Lập trình dễ dàng, đa dạng phần mềm hỗ trợ, kết nối vi điều khiển tốt	Lập trình dễ dàng trên phần mềm có sẵn của nhà sản xuất
Gía thành	Rẻ	Cao	Rất cao

Bảng 1.2: So sánh các board xác thực



Hình 1.4: Máy tính nhúng Raspberry Pi 3

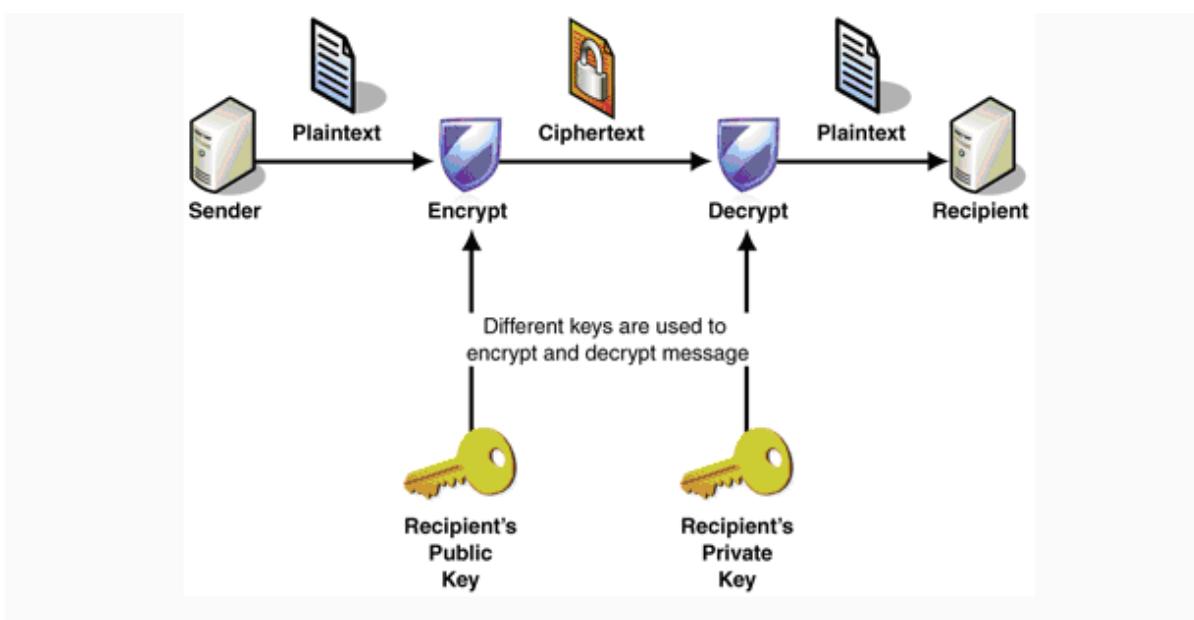
1.3.3 Tìm hiểu về khóa

Như vậy trong hệ thống này chúng ta sẽ sử dụng các loại mã hóa . Độ an toàn của thuật toán mã hóa độ dài của khóa và độ phức tạp của thuật toán . Nhưng độ dài của khóa dễ bị bẻ gãy hơn . Giả sử rằng độ phức tạp của thuật toán là lý tưởng , như vậy để bẻ gãy hệ thống này chỉ còn cách thử với mỗi khóa . Nếu khóa dài 8 bits thì có thể có $2^8 = 256$ khóa . Nếu khóa dài 128 bits thì có 2^{128} khóa có thể . Giả sử rằng siêu máy tính GPU có thể xử lý 10 tỷ phép tính 1 giây thì nếu dò mật khẩu sẽ mất khoảng 10^{21} năm . Nếu dài 256 bits thì mất khoảng thời gian lâu hơn rất nhiều . Một số loại mã hóa thì độ dài của khóa sẽ ảnh hưởng đến độ bảo mật . Cho nên mức độ an toàn của một khóa sẽ được lựa chọn là 1024 bits

1.3.4 Lựa chọn loại mã hóa

Trong thực tế thường có 2 loại mã hóa , mã hóa đối xứng hoặc mã hóa bất đối xứng .

- Mã hoá đối xứng (hay còn gọi là mã hoá bí mật): Nói đơn giản là người ta dùng cùng một chìa khoá để khoá và mở thông tin cần được giữ bí mật. Và cả hai bên gửi và nhận thông tin đều phải có chìa khoá này
- Mã hoá bất đối xứng (hay còn gọi là mã hoá công khai): Có thể hiểu là người ta dùng hai chìa khoá khác nhau để khoá và mở khoá thông tin bí mật. public key sẽ được công khai, và được gửi đi đến đối tượng cần mã hoá thông tin, còn private key được giữ bí mật, và nó đóng vai trò như chìa khoá vạn năng có thể mở được tất cả thông tin được khoá bằng public key



Hình 1.5: Hình ảnh quá trình mã hóa công khai

Trong luận văn do khách hàng giữ xe và nhà xe đều đóng vai trò quan trọng trong bảo mật , do đó khách hàng giữ xe và nhà xe phải sử dụng 2 loại khóa khách nhau để an toàn cho việc giữ xe nên trong luận văn này ,chúng ta sẽ sử dụng mã hóa bất đối xứng công khai. Hình ?? mô tả sơ lược quá trình mã hóa công khai .An ninh của mã hóa RSA sẽ phụ thuộc khá lớn vào

chiều dài của khóa . Kích thước khóa an toàn là từ 1024 bits trở lên . Gần đây nhất năm 1999 đã phá mã được 512 bits (155 chữ số thập phân). Đây cũng là một lý do khiến cho chiều dài của khóa là 1024 bits

1.4 Tổng kết

Như vậy trong chương này chúng ta sẽ lên ý tưởng cho một phương pháp bãi giữ xe thông minh . Và đề tài đặt ra là thiết kế một bãi giữ xe thông minh dành cho 200-300 người ở một tòa nhà sử dụng hệ thống mã hóa và giải mã để xác thực . Và cũng đồng thời có thể mở rộng hệ thống đó cho tương lai sau này.

Hệ thống này kiểm soát truy cập mới áp dụng những công nghệ mạnh mẽ cung cấp mức độ an toàn cao hơn so với các hệ thống hiện có trên thị trường. Hệ thống mới được triển khai với phần mềm trên smart phone của người dùng, loại bỏ các thẻ RFID mang lại sự tiện dụng cao hơn, giảm chi phí đầu tư so với các hệ thống hiện tại.

Việc kết hợp với hệ thống bãi giữ xe góp phần giảm thiểu nhân lực trực bãi xe. Hệ thống này đã có sản phẩm demo những vẫn cần hoàn thiện hơn nếu được áp dụng trong tương lai.

Chương 2

CƠ SỞ LÝ THUYẾT

Sau khi phân tích và tìm hiểu được cách cải thiện . Chương 2 này sẽ giải quyết vấn đề thiết kế gồm các cơ sở lý thuyết , các định nghĩa để thực hiện như hàm băm , mã hóa RSA,... Đồng thời đưa ra phương thức thiết kế một bãi giữ xe sao cho phù hợp với yêu cầu đặt ra

2.1 Các loại mã đọc

Như vậy việc chúng ta cần lúc này là làm sao có thể ứng dụng mã hóa vào các bãi giữ xe . Việc cần lúc này là có thẻ giao tiếp từ người dùng tới hệ thống xác thực . Chẳng hạn như hệ thống sử dụng thẻ từ thì giao tiếp qua các thẻ , sử dụng faceID thì chắn chắc phải có camera nhận dạng khuôn mặt khách hàng ,...Như vậy chúng ta cần một giao thức để có thẻ giao tiếp với hệ thống xác thực (rapberry + camera) . Như vậy có một phương pháp để khách hàng có thể giao tiếp với hệ thống xác thực đó là mã hóa hoặc giải mã thông qua các trường chữ trong các mã code . Vì các mã code này có thể giao tiếp với camera .Như vậy trong thực tế chúng ta có 2 loại mã code thường gặp đó là Barcode và QR Code

2.1.1 Barcode

Ai đã mua đồ ở các cửa hàng tiện lợi thì đều đã nhìn thấy barcode, tuy nhiên không biết họ có nhận ra là các mã barcode đó đều hoàn toàn khác nhau. 1 barcode là 1 tấm ảnh hiển thị thông tin mà máy quét có thể đọc được về thông tin của sản phẩm được ghi vào nó, là 1 tập hợp các đường thẳng đen song song với chiều rộng (width) khác nhau, hình thành 1 hình chữ nhật nhỏ, dính lên 1 góc của sản phẩm.

Hình 2.1 cho thấy 1 barcode. Mã barcode trên sản phẩm chứa thông tin về nhà sản xuất, loại sản phẩm, giá, .. những thông tin mà có thể đọc được bằng những máy đọc chuyên dụng. Bởi vì nó chứa thông tin chỉ theo 1 chiều ngang (horizontal direction), nên nó được gọi là chứa thông tin 1D (1-dimensional).

Cấu trúc 1 Barcode

Ví dụ nếu hệ thống sử dụng mã barcode theo chuẩn EAN của thìMã số EAN-13 gồm 13 con số có cấu tạo như sau: từ trái sang phải

- Mã quốc gia: hai hoặc ba con số đầu



Hình 2.1: Hình ảnh một Barcode

- Mã doanh nghiệp: có thể gồm từ bốn, năm hoặc sáu con số
- Mã mặt hàng: có thể là năm, bốn, hoặc ba con số tùy thuộc vào mã doanh nghiệp
- Số cuối cùng là số kiểm tra

2.1.2 QR Code

Là viết tắt của "Quick Response" (phản hồi nhanh chóng), thường được viết tắt là QR code, và ứng dụng khá giống với barcode, và nó chính là 1 loại barcode. QRCode cũng chứa thông tin của sản phẩm mà được ghi vào nó, nhưng không giống barcode, QR chứa thông tin 2D (2-dimentional), tức là cả chiều dọc và chiều ngang (vertical and horizontal directions).

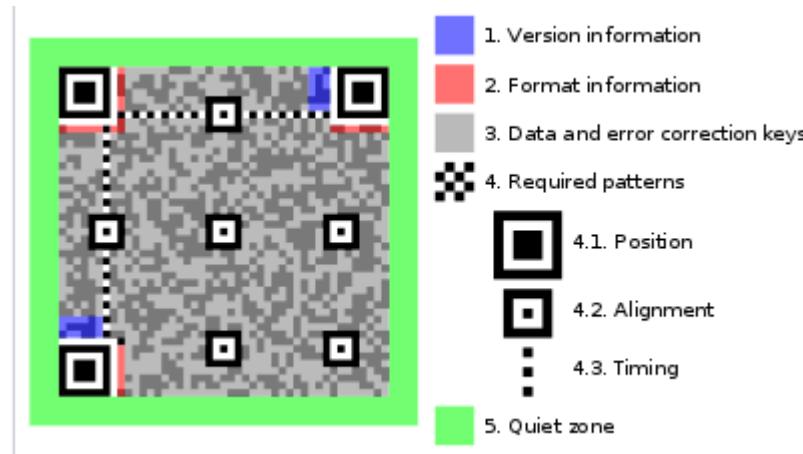


Hình 2.2: Hình ảnh một QR Code

Hình 2.2 cho thấy 1 QR Code.QR codes chứa được rất nhiều thông tin trên đó. Từ những tổ chức to lớn đến các cửa hàng tạp hóa bên đường, đều có thể tạo ra mã QR code của riêng họ và attach chúng vào sản phẩm của họ.

Cấu trúc 1 QR Code

Một QR code bao gồm nhiều ô vuông được sắp xếp trong 1 khối vuông với nền màu trắng, và có thể được giải mã với 1 camera.Những ô vuông này đều mang những chức năng riêng biệt và mục đích khác nhau



Hình 2.3: Cấu trúc 1 QR Code

Thành phần của 1 QR code bao gồm những đặc trưng cơ bản sau:

Vùng 1 (vùng màu xanh dương): vùng xác định phiên bản của QR code từ Version 1 (21x21 modules) đến Version 40 (177x177 modules)

Vùng 2 (vùng màu hồng): thông tin về định dạng (format) của QR code

Vùng 3 (vùng màu xám): dữ liệu và các thành phần để sửa lỗi

Vùng 5 (vùng màu xanh lá): được gọi là quiet zone hoặc margin, sử dụng để cách ly mã code

Vùng 4: các đặc trưng bắt buộc của QR code

2.1.3 So sánh giữa Barcode và QR Code

Mặc dù BarCode và QR Code cùng phục vụ mục đích là lưu trữ thông tin về 1 sản phẩm hoặc 1 tổ chức, nhưng chúng có hai sự khác biệt lớn và rất quan trọng

- Khả năng lưu trữ thông tin** Trong khi barcode chỉ giữ được thông tin theo chiều ngang (horizontal direction), QR code có thể giữ thông tin cả chiều ngang (horizontal direction) và chiều dọc (vertical direction). Với sự khác biệt về cấu trúc này, QR code có thể lưu trữ thông tin nhiều gấp hàng trăm lần (hundreds of times) so với bar code, do đó nó có thể lưu trữ thông tin tốt hơn trong 1 khoảng diện tích nhỏ hơn so với barcode.
- Khả năng chịu lỗi** Đây chính là ưu điểm vượt trội của QR code so với barcode. QR code có khả năng chịu lỗi từ 7-30%. Điều này có nghĩa là gì? Tức là, trong trường hợp QR code in trên sản phẩm bị bẩn hay trầy xước, trong mức cho phép 7-30%, chúng ta vẫn có thể lấy được thông tin trên đó 1 cách chính xác. Nhờ tính năng chịu lỗi vô cùng lớn này, nhiều công ty đã đưa logo hay hình ảnh của họ vào code để phòng trường hợp có bất kì câu hỏi nào liên quan.

Qua hai sự khách biết chúng ta thấy khả năng vượt trội của QR Code so với Barcode . Hơn nữa với thời đại hiện nay việc mỗi người sở hữu một chiếc smart phone là một điều bình thường và thông qua các ứng dụng trên CHPlay và Appstore thì QR Code cũng trở nên thân thiện hơn. Mặc dù Barcode đã phát triển mạnh trong những thập kỷ vừa qua, nhưng với sự ra đời của QR code với những tính năng hoàn toàn vượt trội, và với sự phát triển mạnh mẽ của Smart phone, QR đã và đang trở thành xu hướng (trend) trong các sản phẩm và dịch vụ hằng ngày . Như vậy chúng ta sẽ chọn QR Code để giao tiếp với hệ thống xác thực trong luận văn này

2.2 Lựa chọn hàm băm

Hàm băm nhận input là một chuỗi chiều dài không cố định, và output một chuỗi chiều dài cố định . Output thường được gọi là: hash code, hash value, hoặc là message digest Hàm băm là nền tảng cho nhiều ứng dụng mã hóa . Có nhiều thuật toán sử dụng hàm băm trong số đó phương pháp SHA và MD được sử dụng khá phổ biến

```
Output - digital.signature.rsa (run) ×
run:
input:1412103
output844e749f3357244af81507e1edb298d7
BUILD SUCCESSFUL (total time: 0 seconds)
```

Hình 2.4: Kết quả băm 1 chuỗi từ Netbean

Hình 2.4 cho thấy kết quả của băm của chuỗi **1412103** là **844e749f3357244af81507e1edb298d7**

2.2.1 Tính chất hàm băm

Một hàm băm lý tưởng sẽ có 4 tính chất sau

- Kháng xung đột (hai thông điệp khác nhau có giá trị băm như nhau)
- Kháng tiền ảnh: với một mã băm h bất kỳ, khó tìm được một thông điệp m nào sao cho $h = \text{hash}(m)$.

- Kháng tiền ảnh thứ hai: với một thông điệp m bất kỳ, khó tìm được một thông điệp m' sao cho m' khác m và $MD-5(m) = MD-5(m')$.

2.2.2 Một số loại mã băm

MD5

MD-5 là một thuật toán băm vẫn còn được sử dụng rộng rãi nhưng đã được phát hiện có lỗi bảo mật do thuật toán này có nguy cơ mắc lỗi xung đột. MD-5 bị phá giải là do lỗi xung đột, không phải do lỗi tiền ảnh hay tiền ảnh thứ hai

SHA

SHA hay thuật toán băm bảo mật (Secure Hashing Algorithm) là một họ những thuật toán băm mật mã .Hiện tại có ba thuật toán đã được định nghĩa:

- SHA-1: Hàm băm có chiều dài 160-bit tương tự thuật toán MD-5 trước đó. SHA-1 đã bị phát hiện có chứa điểm yếu mật mã, do đó tiêu chuẩn này đã không còn được sử dụng cho đa số mục đích mã hóa kể từ sau năm 2010
- SHA-2: Là một họ hai hàm băm tương tự, với kích thước khối (block size) khác nhau, có tên là SHA-256 và SHA-512. Các hàm băm này khác nhau về word size; SHA-256 sử dụng 32-bit words còn SHA-512 sử dụng 64-bit words. Mỗi hàm băm còn có phiên bản rút gọn được chuẩn hóa, có tên là SHA-224 và SHA-384.

Trong luận văn chúng ta sử dụng hàm băm dùng để xác thực và dùng nó trên một con vi xử lý nên ta cần quan tâm một số đặc điểm sau:

- MD-5, SHA-1, SHA-256 (và SHA-224) sử dụng phép toán 32-bit, chạy nhanh trên CPU x86 và cả ARM và, đặc biệt là trên GPU
- SHA-512 (và SHA-384) sử dụng các phép toán số học 64-bit

Như vậy chúng ta sẽ chạy hàm băm này trên máy tính nhúng lõi ARM raspberry pi 3 và mục đích là để xác nhận chúng ta có thể dùng MD-5 , SHA-1 . Trong luận văn này sẽ sử dụng hàm băm MD-5 mặc dù có thể có lỗi xung đột trong thuật toán băm nhưng nếu sử dụng cho hệ thống 200-300 người thì điều đó dường như không thể xảy ra

2.3 Mã hóa bất đối xứng

Như vậy chúng ta đã chọn mã hóa bất đối xứng để dùng trong luận văn . Có nhiều loại mã hóa bất đối xứng như RA , ECC ,Rabin,.... Chúng ta thử phân tích tổng quát các loại mã hóa trên

2.3.1 Quá trình hoạt động của hệ mã hóa bất đối xứng

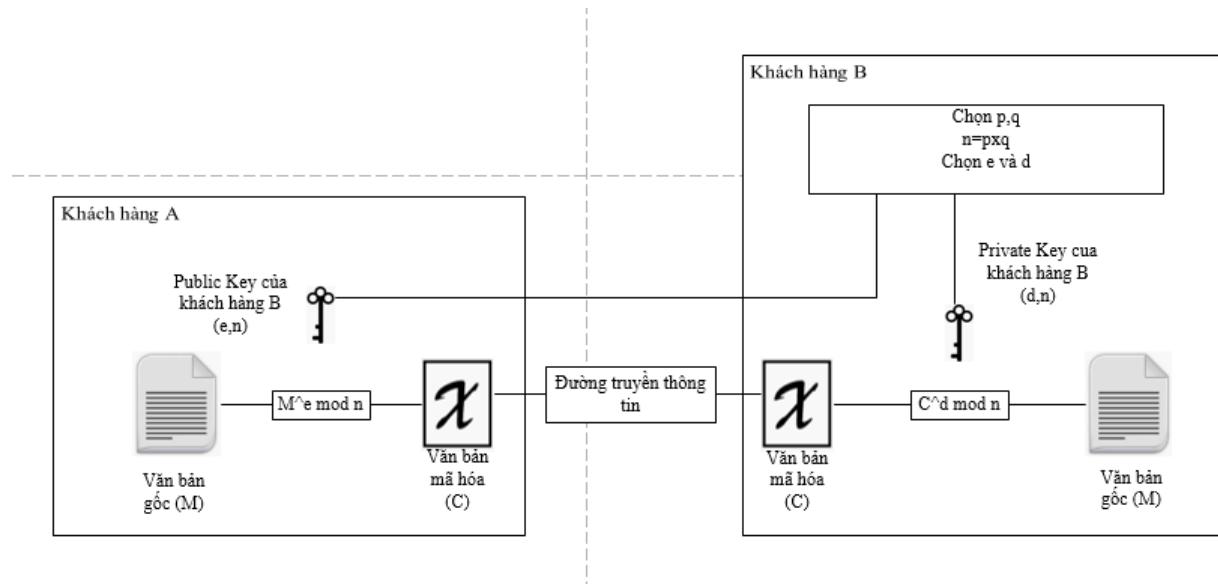
Hình 2.5 cho thấy quá trình hoạt động của hệ mã hóa bất đối xứng . Khi khách hàng A muôn gửi thông điệp cho khách hàng B thì , khách hàng A sẽ dùng Public key được chia sẻ công khai dùng thuật toán mã hóa (có thể là RSA,Rabin,...) mã hóa văn bản gốc . Lúc này ta sẽ được văn bản mã hóa . Khách hàng A sẽ gửi văn bản mã hóa , và lúc này chỉ có thể giải mã khi có được Private key của khách hàng B . Mà Private key của khách được giữ bí mật và chỉ mình khách hàng B biết . Như khi văn bản được mã hóa bằng Public key nào thì chỉ có Private Key tương ứng mới giải mã được

ECC

Trong số rất nhiều thuật toán mã hóa đang được sử dụng và phát triển thì mã hóa đường cong Elliptic ECC (Elliptic Curve Cryptography) là một trong những thuật toán mã hóa mạnh nhất nhưng đồng thời cũng phức tạp nhất. Thuật toán mã hóa khóa công khai mới được đề xuất dựa trên đường cong Elliptic. Một đường cong Elliptic là tập hợp các điểm thỏa mãn một phương trình toán học cụ thể. Các phương trình cho một đường cong Elliptic trông giống như sau: $y^2 = x^3 + ax + b$. Đây là một thuật toán rất dài và phức tạp

RSA

Được đề xuất bởi Ron Rivest , Adi Shamir , Len Adleman vào năm 1977 . Hệ mã hóa khóa công khai phổ dụng nhất . Mức độ an ninh tốt vì mức phí phân tích thừa số 1 số nguyên để bẻ khóa là lớn



Hình 2.5: Quá trình hoạt động của hệ mã hóa RSA

RSA sử dụng 2 thành phần e và d , với e là khóa công khai (Public Key) và d là khóa bí mật (Private Key). Với e thường được dùng để mã hóa và d thường được dùng để giải mã . Các loại mã hóa như Rabin haym Elgamal có thuật toán khác nhau nhưng tính chất tương tự như mã hóa RSA

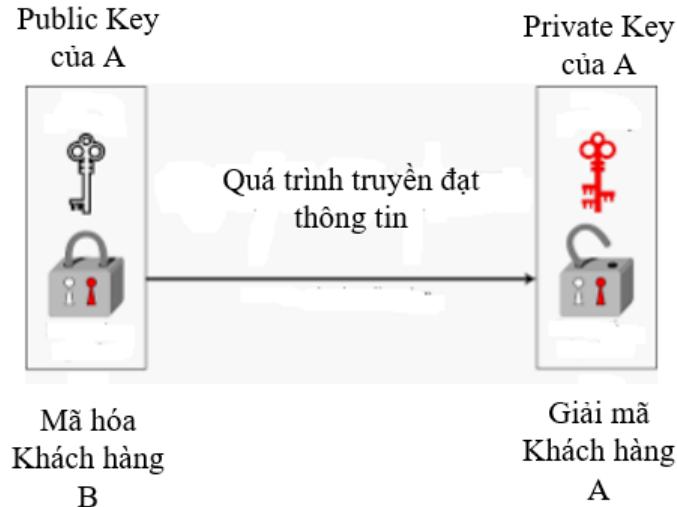
2.3.2 Lựa chọn loại mã hóa

Như vậy do tính chất quá phức tạp và qua khó của mã hóa ECC nên chúng ta sẽ chọn mã hóa RSA cho luận văn này

2.3.3 Khóa trong hệ mã hóa bất đối xứng

Trong hệ thống mã hóa bất đối xứng như đã nói ở phần trước , mỗi khách hàng được xác thực bằng loại khóa riêng biệt là Public key và Private key . Trong quy tắc truyền thông tin thì

Public key sẽ được công khai để mọi người cùng biết , và Private key sẽ chỉ một khách hàng sở hữu biết . Nếu ta dùng Public key của khách hàng A để mã hóa thì chỉ được dùng Private key của chính khách hàng A để giải mã và ngược lại



Hình 2.6: Khóa và mở khóa trong mã hóa bất đối xứng

Hình 2.6 mô tả khi khách hàng B dùng khóa công khai của khách hàng A để khóa (mã hóa) thì chỉ có thể mở khóa (giải mã) bằng khóa bí mật của khách hàng A

2.3.4 Lý thuyết số

Các phép tính thực hiện trong việc mã hóa RSA

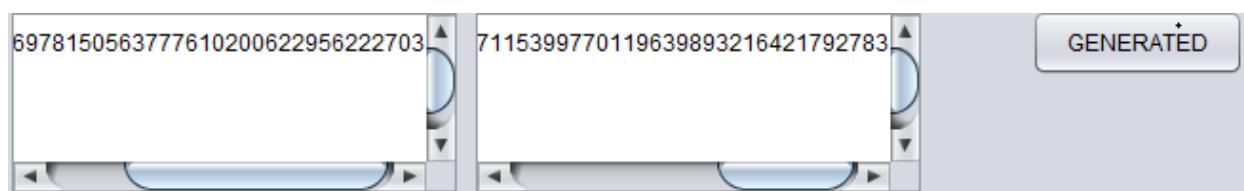
- Phép chia modulo : phép chia lấy dư
 - $a \text{ mod } n = r$ với $a \geq 0 ; n \geq 0 ; 0 \leq r \leq n-1$
- Đồng dư trong phép chia modulo cho n:
 - $a \equiv b \pmod{n}$
- Phép toán modulo phân hoạch tập số tự nhiên N thành n lớp tương đương đồng dư - ứng với các giá trị của r trong tập $0,1,2,3,\dots,n-1$
- Tính chất của modulo:
 - $(a + b) \text{ mod } n = [(a \text{ mod } n) + (b \text{ mod } n)] \text{ mod } n$
 - $(a - b) \text{ mod } n = [(a \text{ mod } n) - (b \text{ mod } n)] \text{ mod } n$
 - $(a \cdot b) \text{ mod } n = [(a \text{ mod } n) \cdot (b \text{ mod } n)] \text{ mod } n$
- Ước số:

- Nếu $a \bmod n = 0$ nghĩa là a chia hết cho n ($a : n$), hay n là ước số của a ($n | a$)
- $\gcd(a,b)$:
 - Ước chung lớn nhất của 2 số , tìm theo thuật toán Euclid
- Số nguyên tố:
 - p được gọi là số nguyên tố nếu p chỉ chia hết cho 1 và chính nó
- Số nguyên tố cùng nhau:
 - $\gcd(a,b) = 1$ thì a , b nguyên tố cùng nhau ký hiệu : $a \perp b$
- Phần tử nghịch đảo của phép nhân modulo:
 - Nếu $a \perp n$ thì : $\exists w$ sao cho $a.w = 1 \bmod n$, w được gọi là phần tử nghịch đảo trong phép chia mod n , ký hiệu a^{-1}
- Định lý Fermat
 - Nếu p là số nguyên tố và a là số nguyên tố không chia hết cho p thì $a^{p-1} \equiv 1 \bmod p$

2.3.5 Quá trình tạo khóa

Khách hàng sẽ được tạo 1 cặp Public key và Private Key như sau :

- Chọn ngẫu nhiên 2 số nguyên tố đủ lớn $p \neq q$
- Tính $n = pq$ và $\Phi(n) = (p - 1)(q - 1)$
- Chọn ngẫu nhiên khóa mã hóa e sao cho $1 < e < \Phi(n)$ và $\gcd(e, \Phi(n)) = 1$ (nguyên tố cùng nhau)
- Tìm khóa giải mã $d \leq n$ thỏa mãn $ed \equiv 1 \pmod{\Phi(n)}$ ($ed - 1$ chia hết cho $\Phi(n)$)
- Công bố khóa công khai Public key = { e, n }
- Giữ khóa bí mật Private key = { d, n }



Hình 2.7: Hệ thống tạo khóa trên CA Server trong luận văn

Hình 2.7 mô tả hệ thống tạo khóa trên CA Server trong luận văn , lèp trình bằng Netbean
Một số lưu ý khi thực hiện tạo khóa

- Cần chọn p và q đủ lớn
- Thường chọn e nhỏ
- Thường có thể chọn cùng giá trị của e cho tất cả người dùng
- Trước đây khuyến nghị giá trị của e là 3 , nhưng hiện nay là quá nhỏ
- Khóa trong toàn bộ luận văn sẽ được chọn là 128 bit (tức p và q là số 128 bit)

2.3.6 Mã hóa và giải mã trong RSA

1. Để thực hiện mã hóa 1 đoạn văn bản gốc , bên gửi cần thực hiện :

- Lấy khóa công khai của bên nhận {e,n}
- Tính $C = M^e \text{ mod } n$ (văn bản đã mã hóa)

2. Để giải mã văn bản C nhận được , bên nhận thực hiện:

- Sử dụng khóa bí mật {d,n}
- Tính $M = C^d \text{ mod } n$

3. Lưu ý : M phải nhỏ hơn n

2.4 Chữ ký điện tử

Chữ ký điện tử (tiếng Anh: electronic signature) là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó.

Chữ ký điện tử được sử dụng trong các giao dịch điện tử. Xuất phát từ thực tế, chữ ký điện tử cũng cần đảm bảo các chức năng: xác định được người chủ của một dữ liệu nào đó: văn bản, ảnh, video,... dữ liệu đó có bị thay đổi hay không.

Hai khái niệm chữ ký số (digital signature) và chữ ký điện tử (electronic signature) thường được dùng thay thế cho nhau mặc dù chúng không hoàn toàn có cùng nghĩa. Chữ ký số chỉ là một tập con của chữ ký điện tử (chữ ký điện tử bao hàm chữ ký số)

2.4.1 Luật giao dịch điện tử (Việt Nam), điều 4 định nghĩa

1. Chứng thư điện tử là thông điệp dữ liệu do tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử phát hành nhằm xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử.
2. Chứng thực chữ ký điện tử là việc xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử.
3. Dữ liệu là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự.

4. Thông điệp dữ liệu là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử.

Trong luận văn này chúng ta sẽ tạo và xác thực chữ ký điện tử dựa vào mã hóa RSA .

2.4.2 Công nghệ xác minh chữ ký điện tử

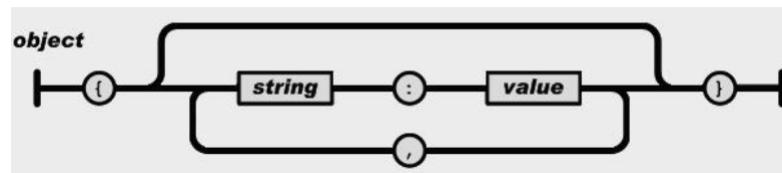
Như vậy chúng ta sẽ ứng dụng mã hóa RSA này để tạo nên chữ ký điện tử . Như vậy mục đích của việc tạo chữ ký điện tử chính là xác thực . Khách hàng A khi muốn xác thực mình là khách hàng thì chắn chắc trường hợp thường sẽ phải gửi một ID để xác thực . Nhưng nếu ai đó cũng xác thực bằng ID này thì làm sao để có thể nhận biết được . Do vậy chúng ta cần phải thêm thêm điều gì đó để xác thực mã ID này . Đó chính là thêm một trường để mã hóa thông tin của ID bằng private key của chính họ . Như vậy chỉ có khách hàng chính thức mới có thể biết được private key của chính mình . Và người muốn xác thực(nhà xe) sẽ biết được public key của khách hàng . Như vậy việc nơi xác thực cần làm chính là giải mã và so sánh . Nếu giải mã ra cho đúng giá trị của ID thì xác thực này là đúng còn sai thì xác thực sẽ bị từ chối



Hình 2.8: Mô hình tạo và xác thực chữ ký điện tử trong luận văn

2.5 Chuỗi JSON

JSON(JavaScript Object Notation) được định nghĩa theo dữ liệu ngôn ngữ javascript tiêu chuẩn ECMA-262 năm 1999 , cấu trúc định dạng văn bản đơn giản với các trường dữ liệu được lồng vào nhau . JSON được sử dụng để trao đổi dữ liệu giữa các thành phần của một hệ thống tương thích với hầu hết các ngôn ngữ C, C++, Java, JavaScript, Perl, Python...



Hình 2.9: Cấu trúc của 1 chuỗi JSON

JSON được xây dựng dựa trên hai cấu trúc chính:

- Tập hợp cặp giá trị name/value, trong nhiều ngôn ngữ khác nhau cặp giá trị này có thể là object, record, struct, dictionary, hash table, keyed list...
- Tập hợp danh sách các giá trị, có thể là array, vector, list hay sequence.

Trong luận văn JSON sẽ có 1 dạng duy nhất . Một đối tượng Object chứa các cặp giá trị string/value không cần thứ tự, được bao trong cặp "", các giá trị bên trong được định dạng "string:value" và chia cách nhau bởi dấu ". ". Value ở đây có thể là chuỗi, số, true- false, null...Hình 19 mô tả cấu trúc 1 chuỗi JSON trong đề tài

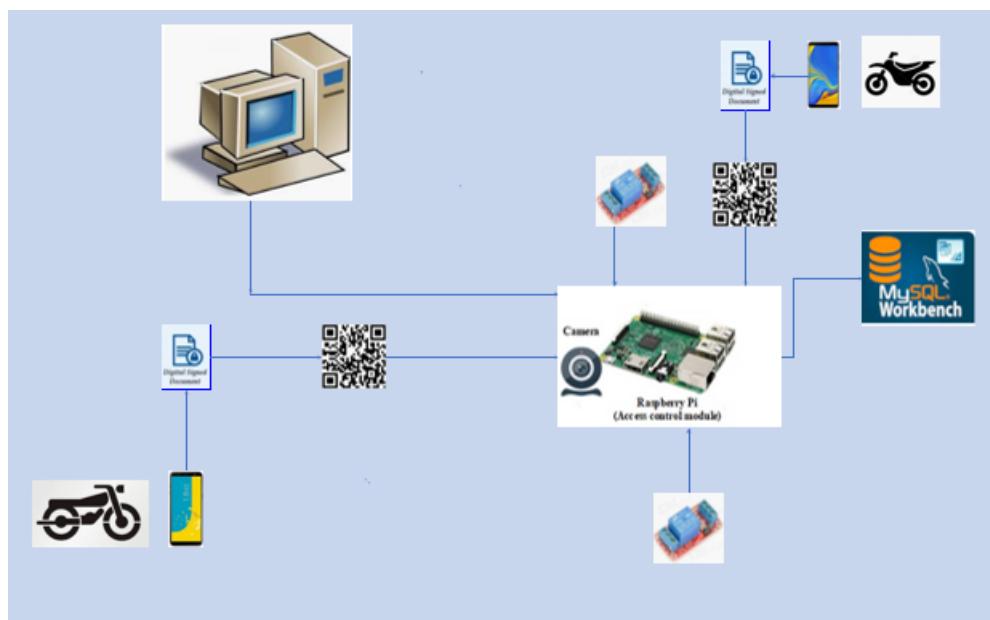
```
(cv) pi@raspberrypi:~/code $ python camera_pi3.py
{"idkhachhang": "1412103", "rsaidkhachhang": "1409054295425046066272783430245155191
5567956203091909440698717352490918806012", "idnhaxe": " ", "timestamp": "1555344855"
, "type": "1"}
```

Hình 2.10: Cấu trúc 1 chuỗi JSON trong đề tài

Chương 3

THIẾT KẾ PHẦN CỨNG VÀ PHẦN MỀM

Từ những lý thuyết trên ta cần thiết kế hệ thống sao cho phù hợp với yêu cầu bài toán đặt ra : Thiết kế 1 hệ thống quản lý , kiểm tra xe tại bãi giữ xe . Hệ thống kiểm tra khách hàng bằng mã QR Code có chứa chữ ký điện tử (mã hóa bắt đối xứng RSA) .QR Code sẽ được truyền tải từ ứng dụng Android tới Raspberry . Hệ thống quản lý khoảng 200-300 khách hàng được xác thực các khóa bằng hạ tầng PKI.X509 Như vậy chúng ta cần thiết kế trên android 1 ứng dụng có thể xác thực được khách hàng



Hình 3.1: Hệ thống thực tế

Hệ thống này sử dụng kỹ thuật :

- Chữ ký điện tử được tạo bằng mã hóa đối xứng RSA
- Các thông tin được nén trong QR Code
- Hệ thống nhận diện QR Code , và QR Code đó truyền tải thông điệp từ điện thoại thông minh và hệ thống xử lý

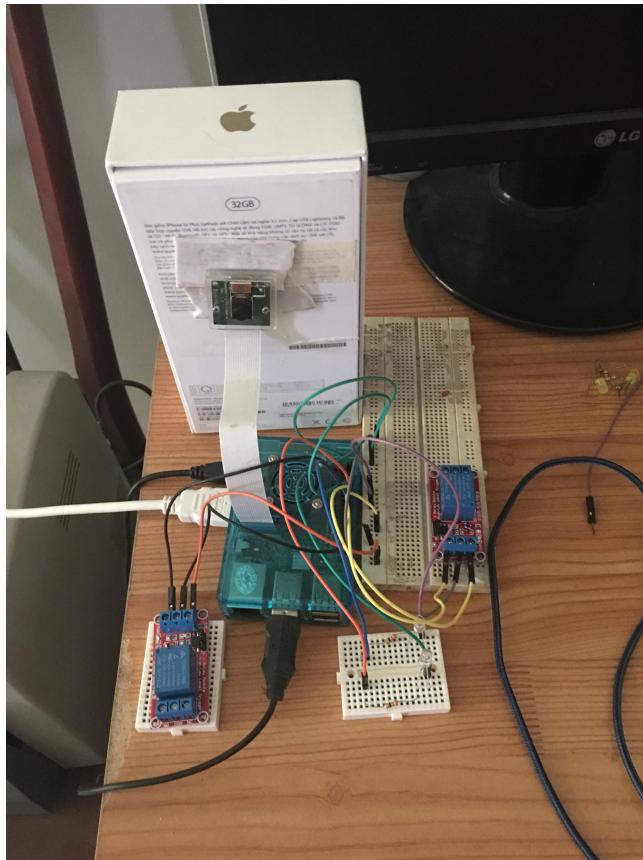
- Giải quyết được tối thiểu một vài trường hợp mượn xe mà nhà xe vẫn quản lý được người mượn và người cho mượn
- Hệ thống các khóa được quản lý bằng CA Server , và mô hình quản lý CA Sever bằng PKI(Public Key Infrastructure)

3.1 Thành phần hệ thống

Raspberry Pi 3 dùng để giải mã QR Code từ thiết bị Android của người dùng, đồng thời mã hóa tạo chữ ký điện tử của nhà xe .Kiểm tra và điều khiển các Relay thích hợp .Chúng ta sử dụng Raspberry vì giá cả hợp lý , nên không sử dụng các board kit trong công nghiệp của Intel hay Samsung

Thiết bị Android gồm 3 ứng dụng GUIXE, TRACHOMUON, MUONXE dùng để tạo QR Code có chứa chữ ký điện tử khách hàng và giải mã QR Code chứa chữ ký điện tử từ nhà xe

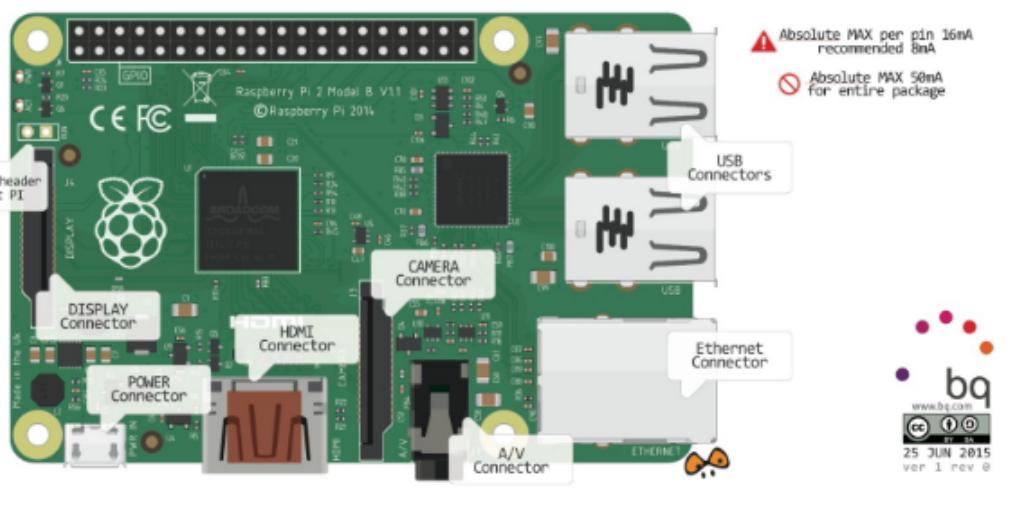
CA Server Là nơi tạo key và lưu trữ key cho khách hàng . Khi có yêu cầu gửi public key của khách hàng thì CA server sẽ ký chứng chỉ đó



Hình 3.2: Hệ thống thực tế

3.1.1 Cấu trúc và chức năng mỗi phần tử

Raspberry Pi 3



Hình 3.3: Raspberry Pi 3 Model B

Máy tính Raspberry Pi 3 Model B (Made in UK) là board mạch máy tính nhúng được sử dụng nhiều nhất hiện nay, ngoài việc sử dụng để hệ điều hành Linux hoặc Windows 10 IoT, máy còn có khả năng xuất tín hiệu ra 40 chân GPIO giúp bạn có thể giao tiếp và điều khiển vô số các board mạch phần cứng khác để thực hiện vô số các ứng dụng khác nhau.

Máy tính Raspberry Pi 3 Model B (Made in UK) được sản xuất tại UK với quy trình gia công và linh kiện chất lượng cao đảm bảo cho việc chạy bền bỉ và lâu dài, máy có kích thước nhỏ gọn, giá thành phải chăng, cách sử dụng dễ dàng, chỉ cần cài hệ điều hành vào thẻ nhớ và cấp nguồn là có thể sử dụng.

Ưu điểm của Raspberry Pi 3 model B so với các phiên bản cũ

- CPU phiên bản mới BCM2837 từ Boardcom với tốc độ 1.2Ghz 4 nhân với kiến trúc ARM Cortex-A53 64-bit. Tốc độ của Raspberry Pi 3 sẽ vượt trội hơn 50%-60% so với phiên bản cũ là Raspberry Pi 2
- Tích hợp Wifi chuẩn 802.11n và Bluetooth 4.1
- Tương thích ngược với thiết kế phần cứng và phần mềm trên các phiên bản cũ là Raspberry Pi 1 và 2

Thông số kỹ thuật chi tiết

- Sản xuất tại: nhà máy Sony tại Anh (Made in UK), chính hãng RS Components
- 1.2GHz 64-bit quad-core ARM Cortex-A53 CPU (BCM2837)
- 1GB RAM (LPDDR2 SDRAM)

- Board có hỗ trợ Wireless LAN - 2.4 GHz 802.11
- Board có hỗ trợ Bluetooth 4.1 + HS Low-energy
- Dùng nguồn 3.5VDC

Camera Pi 3 5MP

Camera Raspberry Pi V1 5MP là Version đầu tiên của module camera cho Raspberry Pi với cảm biến OV5647 độ phân giải 5MP, sử dụng tương thích với tất cả các dòng Raspberry Pi từ trước đến nay, chất lượng hình ảnh tốt, độ phân giải cao và có khả năng quay phim ở chất lượng HD

Để sử dụng Module Camera cho Raspberry Pi tốt và bền Hshop.vn có tặng cho Quý Khách khi mua hàng vỏ Case bằng Mica để chống tĩnh điện từ tay người làm hư cảm biến và bảo vệ mạch



Hình 3.4: Camera Pi 3 5MP

Thông số kỹ thuật

- Độ phân giải: 5MP
- Kích thước: 25x24x9mm
- Cảm biến: OV5647

Module Relay 5VDC

Module 1 Relay với opto cách ly nhỏ gọn, có opto và transistor cách ly giúp cho việc sử dụng trở nên an toàn với board mạch chính, mạch được sử dụng để đóng ngắt nguồn điện công suất cao AC hoặc DC, có thể chọn đóng khi kích mức cao hoặc mức thấp bằng Jumper Tiếp điểm đóng ngắt gồm 3 tiếp điểm NC (thường đóng), NO(thường mở) và COM(chân chung) được cách ly hoàn toàn với board mạch chính, ở trạng thái bình thường chưa kích NC sẽ nối với COM, khi có trạng thái kích COM sẽ chuyển sang nối với NO và mất kết nối với NC



Hình 3.5: Module Realy 5VDC

Thông số kỹ thuật

- Sử dụng điện áp nuôi DC 5V
- Relay mỗi Relay tiêu thụ dòng khoảng 80mA
- Điện thế đóng ngắt tối đa: AC250V 10A hoặc DC30V 10A
- Kích thước: 1.97 in x 1.02 in x 0.75 in (5.0 cm x 2.6 cm x 1.9 cm)

Màn hình LCD Flatron l177wsb

Trong hệ thống , chúng ta cần có 1 màn hình để giao tiếp với Raspberry , xuất ra QR Code từ nhà xe cho khách hàng. Hình 3.6 cho thấy màn hình LCD

Thông số kỹ thuật

- Kích thước màn hình : 17inch
- Độ phân giải tối đa : 1280 x 720
- Khả năng hiển thị màu : 16.2 triệu màu
- Kích thước điểm ảnh : 0.291mm

Board cắm và các dây jump , led màu

Raspberry Pi 3 sẽ liên kết với các led màu và Relay thông qua chân GPIO nối tới các board cắm , và liên kết với nhau bằng các dây jump

Hình 3.7 gồm 3.7(a) các led màu , 3.7(b) các dây jump và hình 3.7(c) board cắm

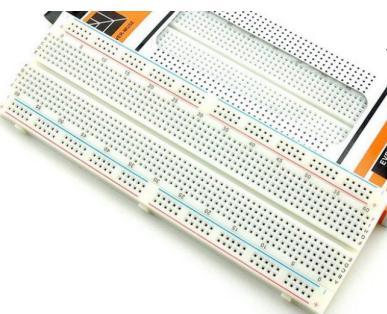


Hình 3.6: Màn hình LCD



(a) Led màu

(b) Dây jump



(c) Board cắm

Hình 3.7: Các thành phần phụ kết nối với Raspberry

3.2 Các ứng dụng trong luận văn

3.2.1 Ứng dụng gửi xe

Như vậy trong ứng dụng gửi xe chúng ta phải tạo ra 1 QR Code chứa chữ ký điện tử khách hàng gồm ID của khách hàng và mã hóa RSA của ID đó .Chúng ta dùng private key của khách hàng để mã hóa sau khi được băm MD5 . ID sẽ dùng để xác nhận khách hàng đó trong cơ sở dữ liệu . Sau đó từ ID này trên raspberry chúng ta sẽ truy xuất ra public key của khách hàng , dùng public key mới có được giải mã chúng ta mới xác nhận được khách hàng . Ngoài ra trên QR Code chúng ta cần phải có 1 timestamp . Time stamp chống lại tấn công lặp lại (reply-attack) , tránh tình trạng có ai đó chụp được màn hình điện thoại thì sẽ ra vào tự do trong hệ thống



Hình 3.8: Giao diện ứng dụng gửi xe

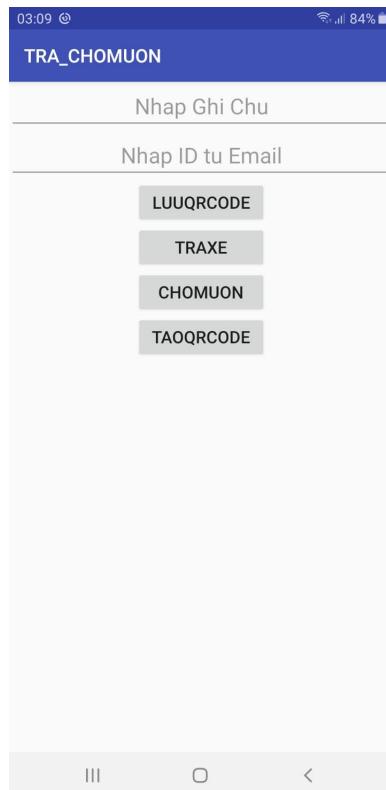
Như vậy trong ứng dụng chúng ta cần một QR Code chứa ID và sau đó chúng ta sẽ băm ID đó bằng phương pháp MD5 . Tiếp tục chúng ta mã hóa nó và đưa 2 trường đó vào trong QR Code . Mô hình giống hình 2.8 phần party A . Khi khách hàng vào họ sẽ sẽ bấm nút ứng dụng và tạo ra 1 QR Code tương ứng

3.2.2 Ứng dụng trả xe

Hiện tại hai ứng dụng này được tích hợp lại thành 1 . Như phần trước đã nêu thì khi trên màn hình raspberry xuất hiện 1 QR Code thì khách hàng cần phải lưu QR Code trên màn hình đó lại . Mà QR Code trên màn hình sẽ chứa chữ ký điện tử của nhà xe gồm mã ID nhà xe và vă

bản mã hóa của nhà xe (mã hóa bằng private key) và trên database của raspberry cũng sẽ lưu lại ID nhà xe tương ứng với ID khách hàng. Vậy trên ứng dụng việc đầu tiên ta cần làm là phải xác nhận chữ ký nhà xe đó là đúng hay sai.

Như vậy khi tạo cơ sở dữ liệu cho mỗi nhà xe thì mỗi khách hàng trên nhà xe đều phải biết public key của nhà xe đó để xác thực chữ ký điện tử của nhà xe nếu đúng thì ứng dụng sẽ lưu phần ID nhà xe vào bộ nhớ trong, nếu sai ứng dụng sẽ không lưu. Như vậy khi khách hàng trả ra thì ứng dụng sẽ lấy phần ID nhà xe đã lưu trong bộ nhớ trong của điện thoại và tạo ra 1 QR Code chứa trường ID nhà xe và ID khách hàng và chữ ký điện tử của khách hàng. Tiếp tục từ ID raspberry sẽ truy xuất public key và mã ID nhà xe của khách hàng đã lưu trước đó, tiếp tục giải mã xác thực chữ ký điện tử, nếu đúng thì tiếp tục kiểm tra ID nhà xe. Nếu đúng tất cả thì raspberry sẽ bật relay phía ra



Hình 3.9: Giao diện ứng dụng mượn xe và trả xe

3.2.3 Ứng dụng cho mượn xe (Ủy quyền)

Trong thực tế có rất nhiều trường hợp mượn xe nhưng trường hợp có khả năng xảy ra cao nhất khi A và B đã gửi xe trong tòa nhà. Đột nhiên A có chuyện gấp khẩn cấp 1 trường hợp liên quan đến tai nạn. Lúc này A sẽ ra ngoài bằng phương tiện khác xe cứu thương. Như xe của A vẫn còn nằm trong bãi giữ xe. Nếu như muốn lấy được xe của A chúng ta chỉ còn cách lấy điện thoại của A theo thực hiện bước trả xe tại trạm. Ngoài ra còn 1 cách nữa đó là sử dụng ứng dụng mượn xe (ứng dụng ủy quyền). Trong luận văn, em làm ứng dụng mượn xe dựa trên quy tắc ký hợp đồng. Như vậy khách hàng B muốn mượn xe khách hàng A. Lúc này khách hàng A sẽ mở ứng dụng trả xe và cho mượn nhán nút cho mượn như vậy trên điện thoại sẽ tạo ra 1 QR Code chứa mã ID nhà xe và chữ ký điện tử của khách hàng A bao gồm mã ID khách

hàng A và văn bản mã hóa ID của khách hàng A và 1 dòng để ghi chú của khách hàng A . Khí đó khách hàng B mở ứng dụng mượn xe và nhấn nút MUON-TRA lúc này ứng dụng sẽ lưu 4 trường trên vào bộ nhớ trong của điện thoại . Và khách hàng B sẽ tới bãi lấy xe , lấy xe của khách hàng A khi tới trạm khách hàng sẽ nhấn nút MUON-GUI trên ứng dụng . Lúc này trên điện thoại sẽ tạo ra 1 QR Code chứa 4 trường đã nêu trên và thêm chưa ký điện tử của khách hàng B gồm mã ID của khách hàng B và văn bản mã hóa RSA của ID khách hàng B và 1 trường timestamp . Như vậy khi xác thực raspberry đầu tiên sẽ vẫn kiểm tra timestamp trước . Tiếp tục sẽ xác thực chữ ký điện tử của khách hàng A tức là chủ xe . Nếu đúng tiếp tục kiểm tra xác thực chữ ký điện tử của khách hàng B . Và cuối cùng là mã ID nhà xe của khách hàng A khi gửi xe đã lưu trong database . Khi đó khách hàng B sẽ lấy được xe của khách hàng B.



Hình 3.10: Khách hàng tạo QR Code để trả xe

Nếu đạt ra trường hợp khách hàng B mượn xe vì mục đích mượn xe thực và khách hàng không gặp phải chấn thương nào . Như vậy quá trình cho mượn xe sẽ vẫn diễn ra như cũ nhưng sẽ xảy ra thêm 1 trường hợp đó là khi khách hàng B muốn gửi xe lại bãi . Lúc này khách hàng B sẽ nhấn lại nút MUON-GUI và tạo ra những trường QR Code như cũ .

Và hệ thống xác thực cũng làm việc như thường . Như vậy khi khách hàng B lấy xe của khách hàng ra khỏi bãi hệ thống xác thực sẽ không xóa mã ID nhà xe của chiếc xe đó , nó chỉ được xóa khi chiếc xe đó gửi lại mà thôi . Và hệ thống xác thực nhận biết xe vào hay ra sẽ dựa vào trường trạng thái trên database , nó sẽ trả cài trị 1 hoặc 0 . 1 tương ứng có xe trong bãi và 0 tương ứng không có xe trong bãi . Dựa vào đó hệ thống sẽ bật relay vào ra thích hợp . Lúc này sẽ xảy ra 1 vấn đề là khi khách hàng B vào rồi thì làm sao nhà xe có thể cung cấp mã

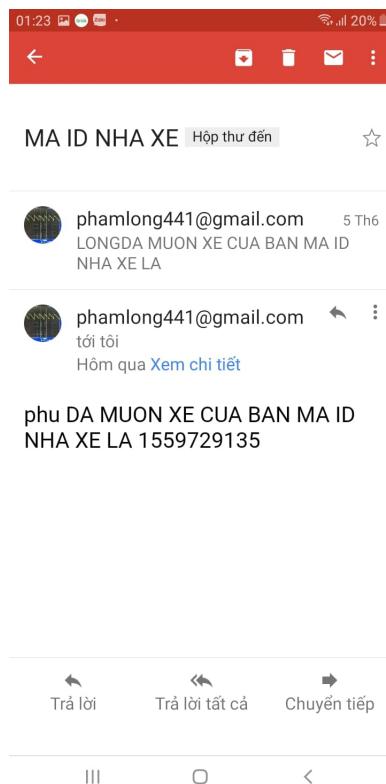


Hình 3.11: Khách hàng tạo QR Code cho mượn xe

ID nhà xe cho khách hàng A là chủ xe được . Một lát sau khách hàng A chắc chắn cũng sẽ rời khỏi bãi xe . Như vậy để tiếp tục , raspberry thay vì gửi mã ID nhà xe cho khách hàng thông qua QR Code trên màn hình thì sẽ gửi mã ID nhà xe qua email cho khách hàng A. Như vậy khi khách hàng A muốn rời khỏi nhà xe , khách hàng A sẽ mở email của mình sẽ copy và mở ứng dụng trả xe và cho mượn xe paste vào phần nhập từ email và nhấn nút TAOQRCode lúc này sẽ tạo ra 1 QR Code tương tự như trường hợp trả xe gồm chữ ký điện tử của A (mã ID khách hàng và văn bản mã hóa ID khách hàng) và mã ID nhà xe và timestamp

3.2.4 Ứng dụng mượn xe

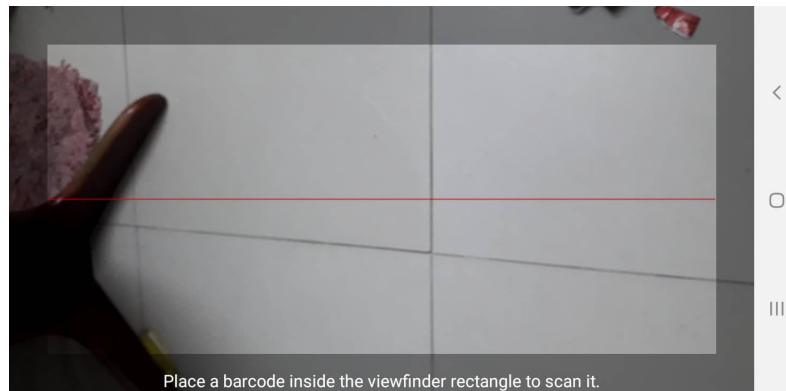
Như đã trình bày ở phần trước chúng ta cần phải thiết kế 1 ứng dụng trung gian để có thể lấy 2 chữ ký của 2 khách hàng . Như đã nói ở trên hệ thống này cần 2 nút . Nút đầu tiên sẽ lưu mã ID nhà xe và chữ ký của khách hàng cho mượn (ID khách hàng và văn bản mã hóa) và ghi chú của khách hàng. Chuỗi được lưu dưới hình thức chuỗi JSON và lưu nó vào bộ nhớ trong . Nút nhấn thử sẽ có nhiệm vụ tải lại nội dung đã lưu và thêm vào chuỗi đó chữ ký điện tử của khách hàng mượn tất cả sẽ nén thành 1 QR Code .Như vậy khi tạo ra QR Code thì lúc này trong QR Code sẽ chứa tối 8 trường : timestamp, type , chữ ký điện tử khách hàng cho mượn(2 trường) , chữ ký điện tử khách hàng mượn (2 trường) , mã ID nhà xe và ghi chú của khách hàng cho mượn



Hình 3.12: Khách hàng nhận được email từ nhà xe



Hình 3.13: Khách hàng khi tạo QR Code



Hình 3.14: Camera được bật lên khi khách hàng lưu QR Code của người cho mượn

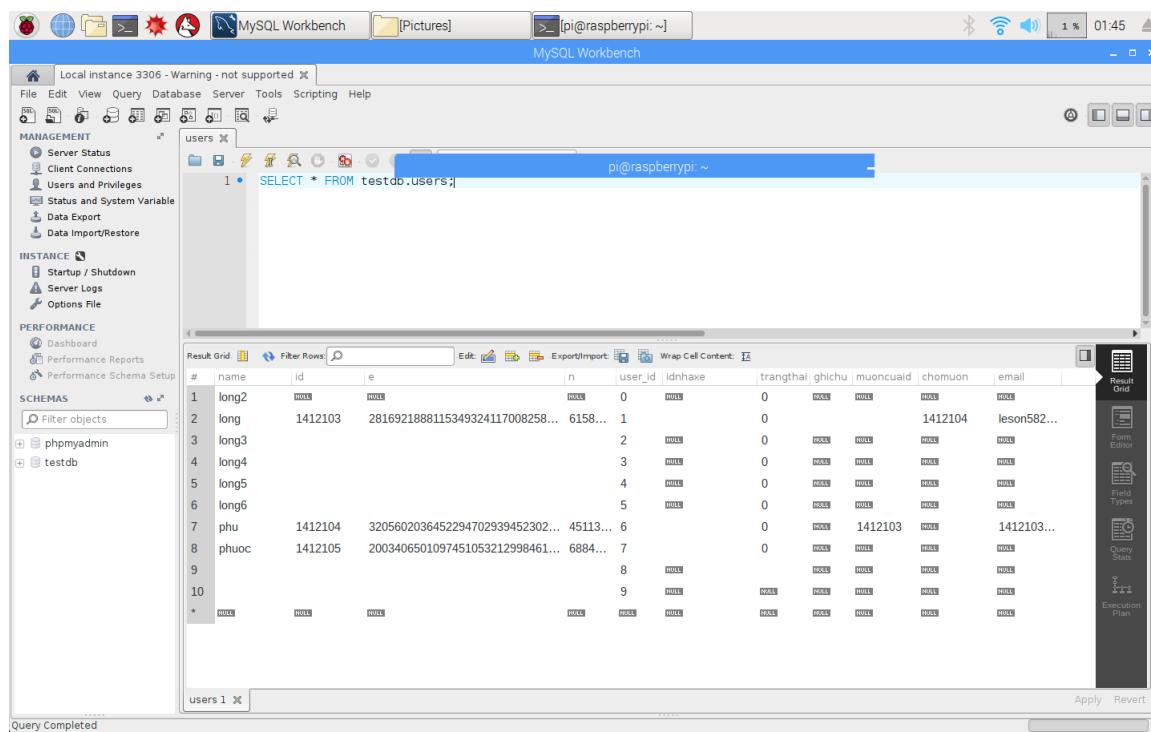
3.3 Cơ sở dữ liệu khách hàng

Như vậy chúng ta cần phải có 1 cơ sở dữ liệu của khách hàng trên raspberry . Để xác định 1 khách hàng chúng ta cần phải biết ID của khách hàng đó và 1 cặp key gồm public key và private key . Ba trường đó mỗi khách hàng đều khác nhau và đặc trưng cho mỗi người . Trên hệ thống chúng ta cần mã hóa và giải mã trên thiết bị android lẫn trên raspberry , nhưng đối với khách hàng chúng ta cần mã hóa ID đó trên thiết bị Andoid dùng private key để mã hóa và giải mã nó bằng public key trên raspberry. Như vậy trên một cơ sở dữ liệu của raspberry chúng ta cần ít nhất 2 trường ID và public key khách hàng . Ngoài ra trên mỗi raspberry chúng ta cần phải có private key của nhà xe (raspberry) , để cho khách hàng xác nhận Theo như lý thuyết thì public key đó bao gồm e và n và private key là d và n .Như vậy chúng ta sẽ tồn ít nhất 5 cột VARCHAR để chứa các thông số này. Ngoài ra chúng ta còn cần các cột khác để phù hợp với phần mềm

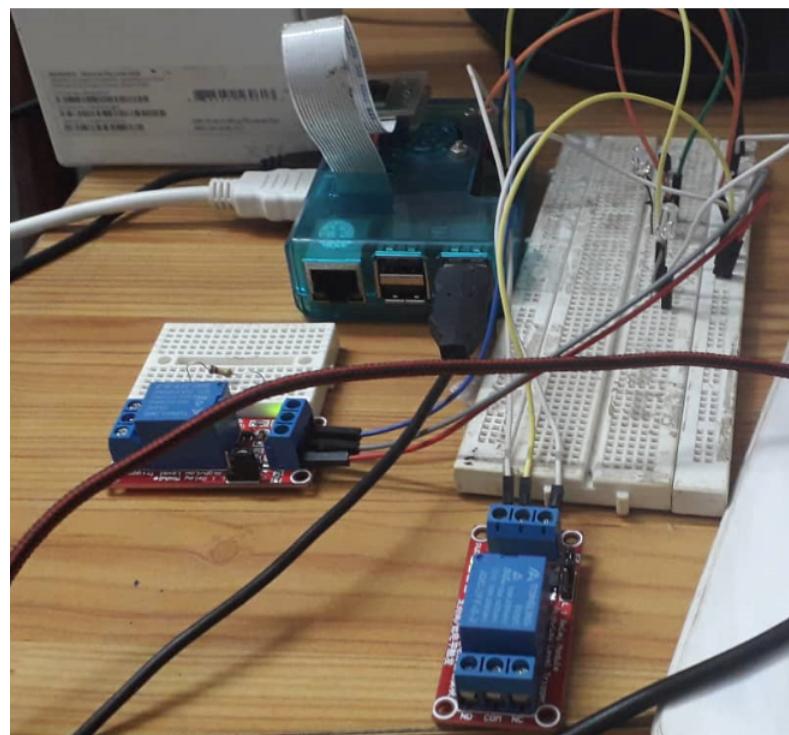
3.4 Hệ thống xác thực trên Raspberry

Gửi xe Như đã nói ở phần trước sau khi khách hàng scan QR Code , trên raspberry chúng ta sẽ nhận được ID khách hàng và văn bản mã hóa . Trên raspberry lúc này chúng ta sẽ truy vấn lên cơ sở dữ liệu từ ID chúng ta sẽ có được public key của khách hàng . Sau đó chúng ta dùng public key này để giải mã chúng ta sẽ được giá trị băm . Và từ ID chúng ta băm . Sau đó so sánh 2 giá trị băm này để xác thực đó có phải là khách hàng không . Nếu xác thực đúng từ màn hình sẽ xuất ra 1 QR Code chứa ID của nhà xe và chữ ký điện tử của ID nhà xe . ID nhà xe sẽ được chọn là thời gian epoch mà khách hàng scan QR Code . Thời gian này sẽ được chuyển hóa thành dạng int32 sau đó chuyển thành dạng string để nén trong QR Code . Đồng thời khi đó relay bên vào sẽ mở . Khi hệ thống xác thực sai thì đèn báo tín hiệu sẽ sáng

Trả xe Còn đối với trường hợp khi trả xe thì khách hàng sẽ phải tạo ra 1 QR Code chứa chữ ký điện tử của mình và ID nhà xe đã lưu trước đó . Hệ thống xác thực sẽ kiểm tra 2 lần gồm xác thực chữ ký điện tử và xác thực ID nhà xe . Nếu đúng cả hai trường hợp thì relay phía ra sẽ mở



Hình 3.15: Cơ sở dữ liệu khách hàng trên raspberry



Hình 3.16: Hệ thống xác thực khi đang thực hiện

Lưu ý Ttấ cả các QR Code khách hàng scan để xác thực ra vào thì đầu tiền luôn kiểm tra timestamp Nếu timestamp còn thời hạn sử dụng thì các bước xác thực tiếp theo mới được tiến hành

3.5 PKI (Public-Key Infrastructures)

3.5.1 CA Server

Như vậy khi một khách hàng cần sử dụng dịch vụ thì cần cung cấp cho hệ thống xác thực public key của mình . Để public key của khách hàng có giá trị thì cần có một Ca server quản lý . Ví dụ khi cần xác thực một khách hàng mà khách hàng đó không nằm trong hệ thống (bãi giữ xe) đó thì lúc này public key của khách hàng đó phải được gửi cùng với 1 chuỗi mã hóa bằng private key của CA mình đăng ký . Lúc này hệ thống bãi giữ xe mới xác thực và giải mã . Nếu đúng thì sẽ đồ ý còn sai sẽ từ chối

3.5.2 Public-Key Infrastructures

PKI là một hệ thống phục vụ cho việc tạo phân phối xác thực chứng nhận dựa trên chuẩn X.509. Nhiệm vụ của PKI cơ bản gồm :

- Là nơi tạo key và lưu trữ key , đồng thời cũng có thể update key nếu khách hàng yêu cầu
- Cung cấp dịch vụ cho hệ thống truy cập . Hệ thống truy cập này chính là raspberry . Raspberry sẽ download thông tin khách . Và mỗi raspberry sẽ có 1 CA server quản lý

3.6 Tổng kết

Như vậy chúng đã đưa ra ý tưởng một hệ thống sẽ hoạt động theo phương thức mã hóa RSA , đồng thời sẽ tương tác qua các ứng dụng Android , và cuối cùng chúng ta sẽ lập trình trên Netbeans để tạo hệ thống quản lý

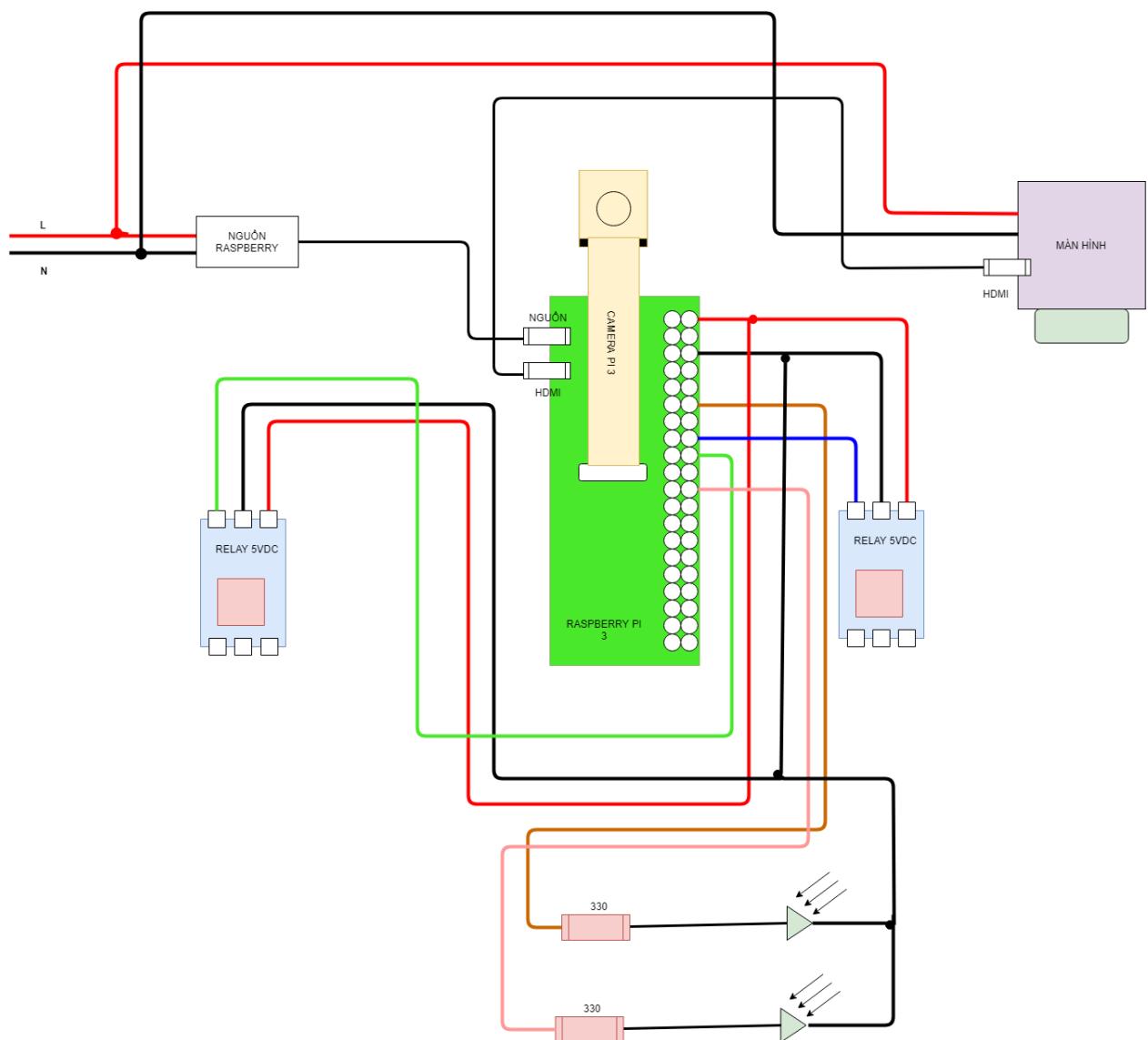
Chương 4

THỰC HIỆN PHẦN CỨNG VÀ PHẦN MỀM

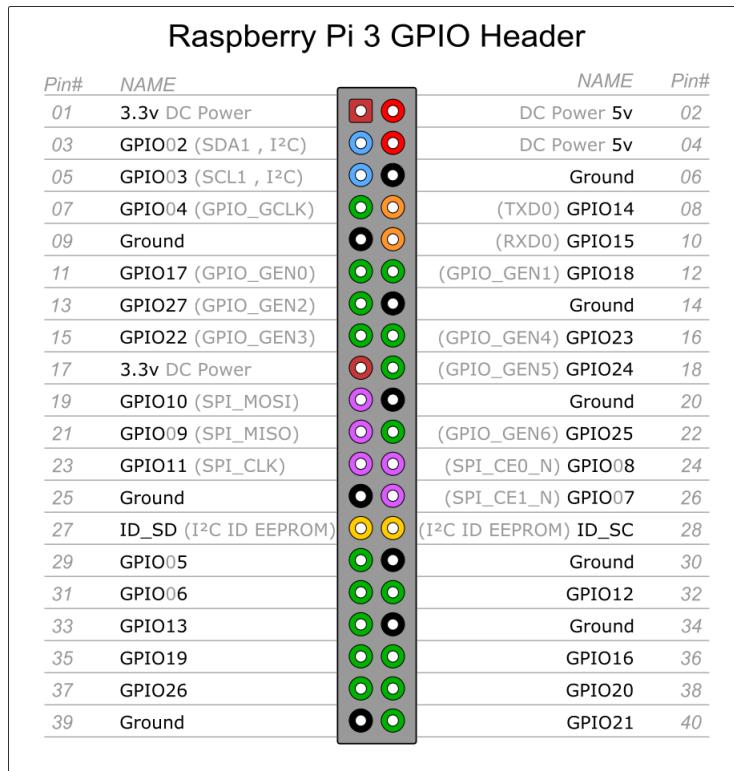
Ở chương 2 chúng ta thiết kế hệ thống này .Chương 3 tiếp tục chúng ta sẽ thực hiện hệ thống này 1 cách chi tiết . Chương 3 sẽ trình bày sơ đồ nối dây , chi tiết các ứng dụng , các trường trong QR Code thực hiện thế nào , và cách thức hoạt động của nó

4.1 Sơ đồ nối dây

Hệ thống sẽ gồm 2 Relay ra vào (Relay bên phải là vào, Relay bên trái là ra , 1 Camera , 1 Màn hình và 2 Led báo hiệu cùng vi điều khiển chính là Raspberry Pi 3 . Raspberry sẽ được cấp nguồn bằng bộ nguồn của nhà phát hành . Màn hình được cấp nguồn 220 V và Relay là 5VDC . Từ raspberry chunh1 ta sẽ dùng cáp chuyển VGA-HDMI và nối vào dây HDMI sau đó nối tới màn hình. Dùng các dây điện nối từ chân GPIO 18 và 25 tới chân điện trở nối với led , chân GPIO 23 VÀ 24 sẽ nối tới chân kích của Relay . Lưu ý Relay kích mức cao . Nguồn của relay sẽ được cấp từ 2 chân DC 5V và GND của raspberry .Hình 35 mô tả sơ đồ chân GPIO của raspberry. Điện trở sử dụng là 330Ω . Như vậy khi khách hàng sử dụng thì sẽ scan QR Code mình tạo được vào camera và raspberry sẽ xử lý và điều khiển các Relay và các led hợp lý



Hình 4.1: Sơ đồ nối dây của hệ thống



Hình 4.2: Sơ đồ chân Raspberry PI 3

4.2 Phần mềm Gửi xe trên Android

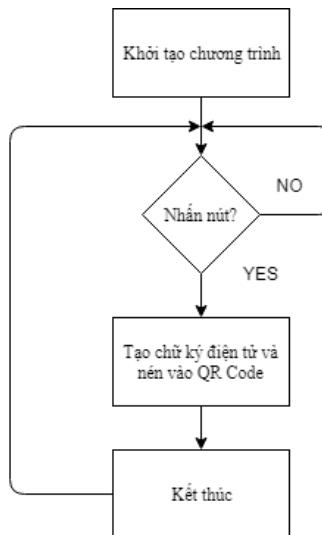
Các trường trong QR Code

- **idkhachhang** : Dạng string chưa id khách hàng . ID khách là khác nhau cho mỗi người
- **rsaидkhachhang** : Dạng string chứa văn bản mã hóa RSA cho ID khách hàng
- **timestamp**: Dạng string chứa time stamp có thời hạn 10s
- **type** . Dạng string khi gửi xe thì type là 1
- **tram** . Dạng strng , cho mã trạm mà khách hàng đã đang ký sử dụng . Dùng cho các phần mở rộng lớn sau này

Như đã trình bày trong phần thiết kế chúng ta cần phải thực hiện 1 đoạn code băm MD5 và mã hóa RSA. Như vậy mã ID khách hàng và private key của khách hàng sẽ được lưu sẵn trong ứng dụng để thực hiện.Như vậy ID khách hàng , private key dùng để mã hóa , và type để cho raspberry biết đây là QR Code phục vụ chứ năng gì.

Để băm một đối tượng trong Android(Java) sử dụng MD5 ta sử dụng class java.security.MessageDigest. Nó nhận đầu vào là một mảng byte và kết quả trả về là một mảng byte đã được băm:

```
MessageDigest md = MessageDigest.getInstance("MD5");
byte[] messageDigest = md.digest(input.getBytes());
```



Hình 4.3: Lưu đồ giải thuật cho ứng dụng gửi xe

Chúng ta cần phải chuyển mảng byte sang dạng hexa vì khi chuỗi input đầu vào chúng ta phải chuyển thành các mảng bytes sau đó mới dùng hàm băm nên khi có kết quả chúng ta sẽ chuyển lại hexa rồi chuyển thành string

```

private static String convertByteToHex(byte[] data) {
StringBuffer sb = new StringBuffer();
for (int i = 0; i < data.length; i++) {
sb.append(Integer.toHexString((data[i] & 0xff) + 0x100, 16).substring(1));
}
return sb.toString();
}
  
```

Sau khi đã có được hai hàm trên như vậy chúng ta đã có được giá trị băm . Để tiếp tục chúng ta sẽ mã hóa RSA giá trị băm này . Chúng ta sử dụng hàm :

```

public synchronized String encrypt(String message) {
return (new BigInteger(message.getBytes())).modPow(d, n).toString();
}
  
```

Hàm này có đầu vào là 1 chuỗi string , chuỗi này chính là chuỗi mà chúng ta băm . Như thuật toán trình bày ở các phần trước chúng là sẽ lấy giá trị này modPow(d,n) , với d, n là private key của khách hàng . D và n đã được lưu sẵn trong phần mềm với định dạng là BigInteger . Như viে chúng ta cần lúc này là chuyển chuỗi băm string thành dạng big integer để có thể thực hiện được phép toán . Chúng ta sử dụng phép toán getBytes và BigInteger .Ví dụ chúng ta có chuỗi băm là : "ab" . Chuỗi này sẽ được chuyển thành dạng mảng byte [97,98] dạng ascii thập phân . Từ mảng bytes này chúng ta sẽ chuyển thành mnag3 nhị phân 01100001 01100010 . Từ mảng nhị phân này sẽ chuyển lại thành dạng int với công thức quen thuộc :

$$0.2^{15} + 1.2^{14} + \dots + 0.2^0$$

Khi đó chúng ta sẽ có kết quả là 24930 cho chuỗi băm là "ab" . Khi mã hóa chúng ta sẽ lấy số 24930 này . Và hàm encrypt sẽ thực hiện các điều bên trên , cuối cùng sẽ trả về loại string để có thể nén vào QR Code . Tiếp tục chúng ta sẽ tạo timestamp :

```
long Key = Instant.now().getEpochSecond();
int Key2=(int) Key;
Key3= Integer.toString(Key2);
```

Hàm getEpochSecond sẽ lấy thời gian ở mốc năm 1970 đến thời điểm hiện tại thành 1 số thập phân . Từ đó chúng ta chuyển về dạng int , cuối cùng là về dạng string để có thể nén vào QR Code

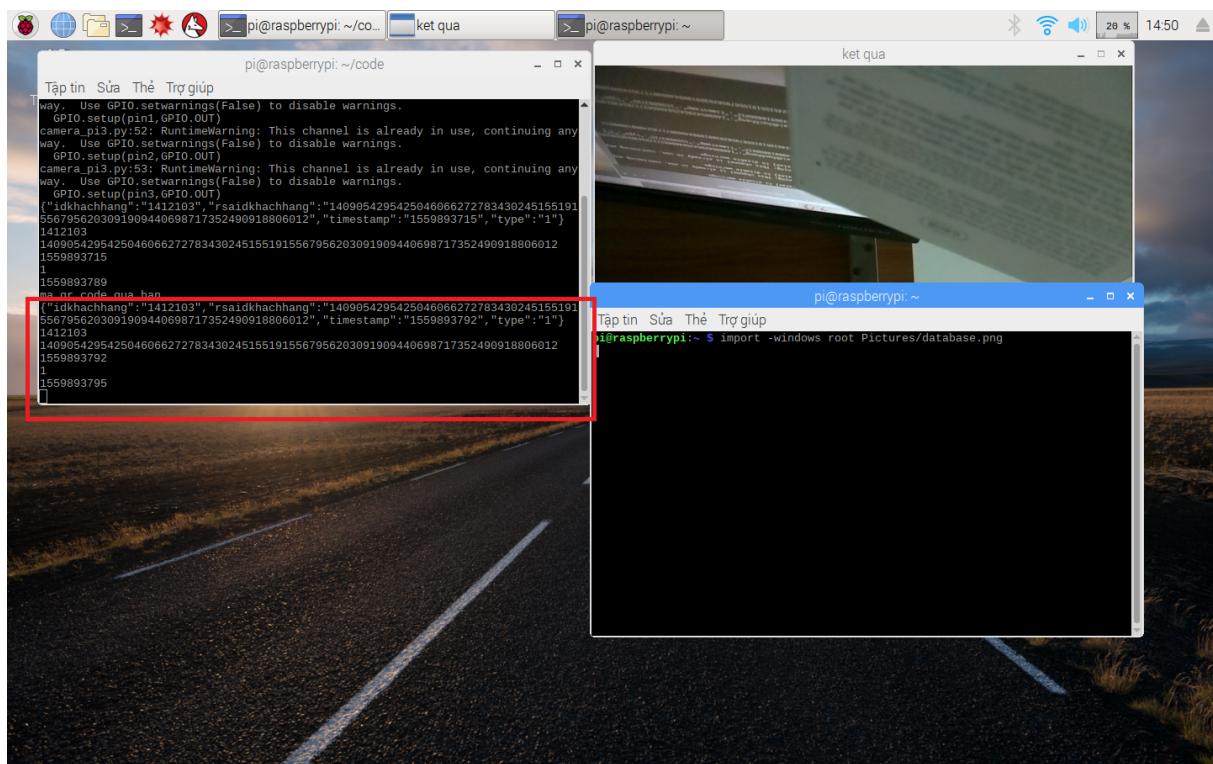
Cuối cùng chúng ta sẽ tạo chuỗi JSON với các trường đã nêu ở trên dưới đây là đoạn 1 code với 1 trường:

```
JSONObject jsonObject = new JSONObject();
try {
jsonObject.put("idkhachhang",Name);
} catch (JSONException e) {
e.printStackTrace();}
```

Lúc này chúng ta sẽ vẽ QR Code lên màn hình với nội dung là 1 chuỗi JSON với các trường vừa tạo

```
BarcodeEncoder barcodeEncoder = new BarcodeEncoder();
Bitmap bitmap = barcodeEncoder.createBitmap(bitMatrix);
imageView.setImageBitmap(bitmap);
```

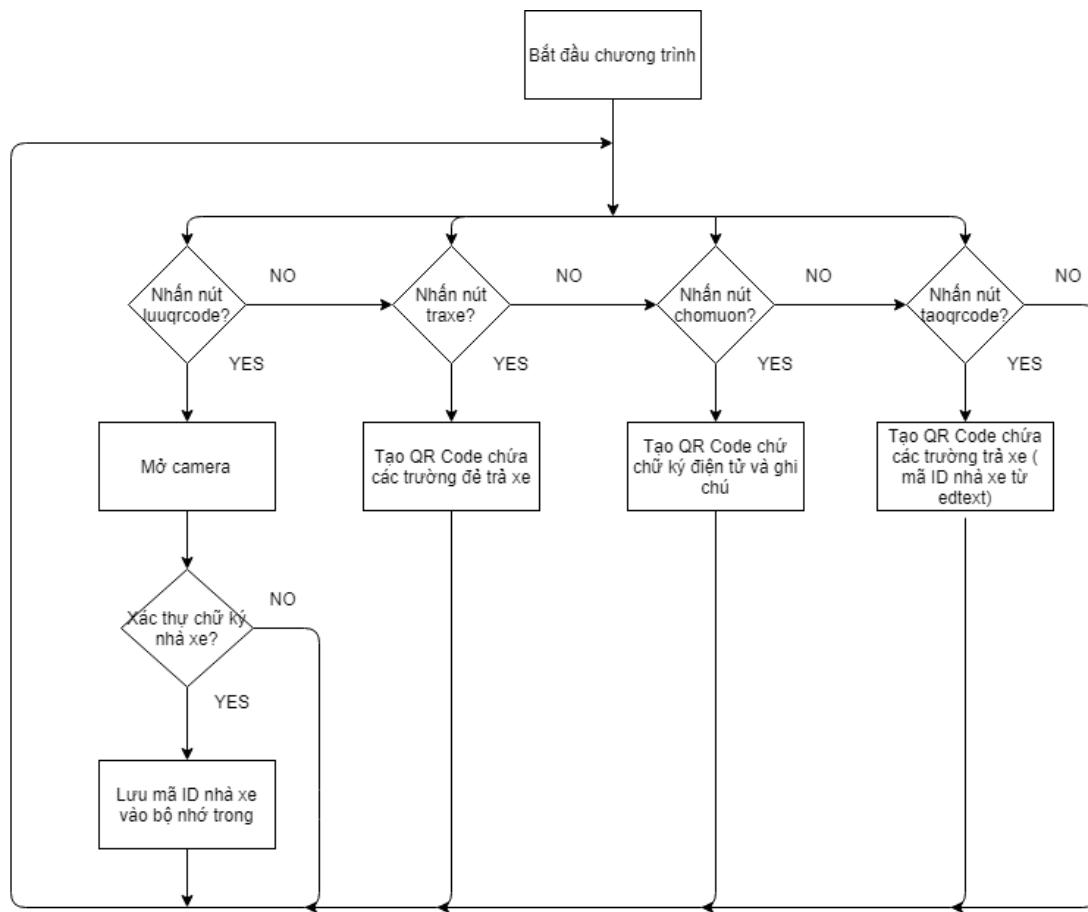
Như vậy chúng ta đã có được ứng dụng đầu tiên dùng để gửi xe



Hình 4.4: Nội dung của QR Code khi scan vào raspberry

Hình 37 phần chữ nhật đỏ cho thấy nội dung QR Code được tạo khi sacan vào raspberry gồm các trường đã nêu trên

4.3 Phần mềm Trả xe và Cho mượn trên Android



Hình 4.5: Lưu đồ giải thuật ứng dụng trả xe và cho mượn

4.3.1 Trả xe

Như vậy theo nguyên lý thiết kế thì khi raspberry giải mã , xác thực xong thì trên LCD sẽ xuất hiện QR Code chứa mã ID nhà xe và văn bản mã hóa id nhà xe. Khi đó chúng ta mở phần mềm TRA_CHOMUON nhấn nút luuqrcode khi đó hệ thống sẽ xác thực chữ ký điện tử của nhà xe . Đầu tiên chúng ta sẽ mở camera lên:

```

public void onClick(View v)
intentIntegrator.initiateScan();
```

Như vậy trong phần mềm chúng ta sẽ đưa public key vào dưới dạng biến BigInteger . Quá trình xác thực cũng tương tự như các phần trên đầu tiên chúng ta sẽ giải mã văn bản mã hóa mà nhà xe gửi cho chúng ta:

```

public synchronized String decrypt(String message) { return new String ((new BigInteger(message)).modInverse().toByteArray()); }
```

Hàm decrypt sẽ trả lại thằng giá trị string là giá trị băm . Sau khi giải mã chúng ta sẽ có được 1 giá trị băm . và từ ID nhà xe chúng ta sẽ băm nó . Quá trình băm chúng ta thực hiện như

phần trên dùng hàm GETMD5 và hàm HexToBytes . Sau đó chúng ta sẽ so sánh hai giá trị bấm này . Nếu đúng thì điện thoại sẽ lưu lại mã ID nhà xe vào bộ nhớ trong:

```
fos = openFileOutput(FILE_NME, MODE_PRIVATE);
fos.write(text.getBytes())
Toast.makeText(this, "savedto" + getFilesDir() + "/" + FILE_NME,
Toast.LENGTH_LONG).show();
```

Đoạn code trên sẽ lưu mã ID nhà xe vào bộ nhớ trong của điện thoại.

Khi trả xe khách hàng sẽ mở lại ứng dụng và nhấn nút traxe .Lúc này điện thoại sẽ tạo ra 1 QR Code chứa các trường sau:

- **idkhachhang** : Dạng string chứa id khách hàng . ID khách là khác nhau cho mỗi người
- **rsaidkhachhang** : Dạng string chứa văn bản mã hóa RSA cho ID khách hàng
- **timestamp**: Dạng string chứa time stamp có thời hạn 10s
- **type** : Dạng string khi gửi xe thì type là 1
- **idnhaxe** :Dạng string là mã id nhà xe đã lưu vào ô nhớ trong

Như vậy khi tạo ra QR Code này chúng ta sẽ scan nó vào camera của raspberry và hệ thống xác thực sẽ làm việc còn lại

4.3.2 Cho mượn xe

Với ứng dụng này chúng ta sẽ làm tiếp việc cho mượn . Như vậy khi muốn cho mượn xe .Chúng ta phải đưa cho người muôn mượn các trường ID chính mình , văn bản mã hóa ID của chính mình , ID nhà xe và cuối cùng là ghi chú của mình . Như vậy chúng ta cần nhập vào 1 editext trên android ghi chú của mình có thể nhập hoặc không nhập như và chúng ta bấm nút chomuon . Lúc này QR Code chứa các trường cần thiết sẽ được tạo ra . Đầu tiên nó sẽ lấy trường mã ID nhà xe lưu trong bộ nhớ trong mà đã lưu lúc gửi xe:

```
fis=openFileInput(FILE_NME);
InputStreamReader isr = new InputStreamReader(fis);
BufferedReader br = new BufferedReader(isr);
StringBuilder sb = new StringBuilder();
```

Sau đó tiếp tục lấy chữ ký điện tử của mình . Sau đó lấy trường từ mục nhập từ editext

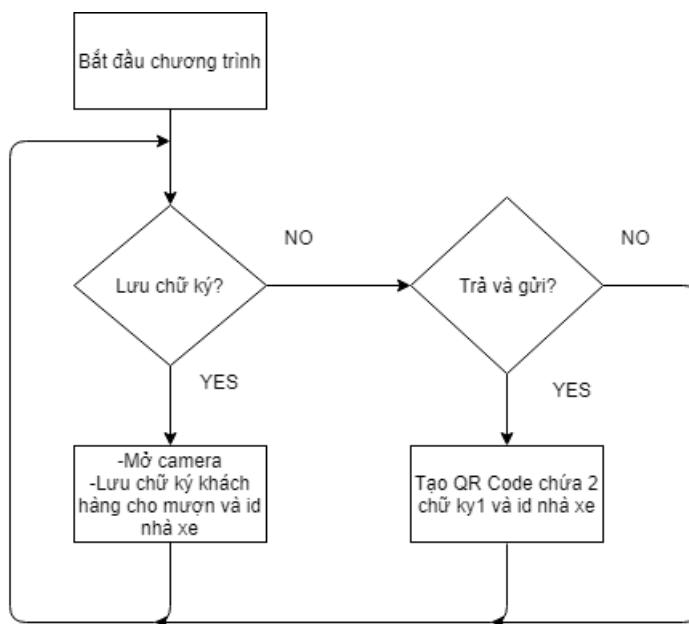
```
jsonObject.put("ghichu",edt3.getText());
```

Khi đã có đủ các trường chúng ta sẽ tạo QR Code trên màn hình android

4.4 Phần mềm mượn xe

Như vậy cũng tương tự như những phần mềm trước . Phần mềm này sẽ có hai nút LUU CHU KY và TRA VA GUI. Nút lưu chữ ký sẽ tạo lưu lại chữ ký điện tử và id xe của khách hàng cho mượn . Còn nút trả và gửi sẽ tạo ra 1 QR Code chứa:

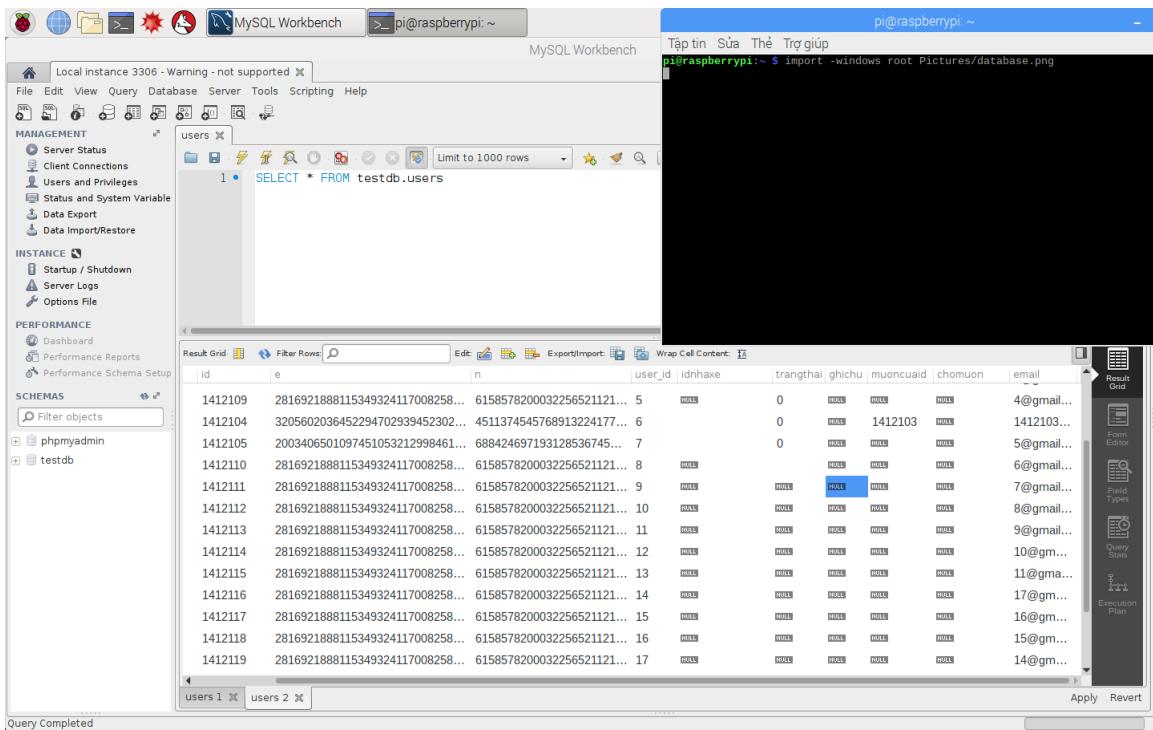
- **idkhachhang** : Dạng string chưa id khách hàng . ID khách là khác nhau cho mỗi người
- **rsaidkhachhang** : Dạng string chứa văn bản mã hóa RSA cho ID khách hàng
- **timestamp**: Dạng string chứa time stamp có thời hạn 10s
- **type** : Dạng string khi gửi xe thì type là 1
- **idnhaxe** :Dạng string là mã id nhà xe đã lưu vào ô nhớ trong
- **idkhmuon** :Dạng string là mã id khách hàng mượn
- **rsaidkhmuon** :Dạng string là mã hóa RSA của id khách hàng mượn
- **ghichu** :Dạng string là ghi chú của khách hàng cho mượn



Hình 4.6: Lưu đồ giải thuật của ứng dụng mượn xe

4.5 Cơ sở dữ liệu trên raspberry

Như vậy trong cơ sở dữ liệu của raspberry chung ta cần có các trường để có thẻ truy vấn và truy xuất . Ngoài ra còn có trường trạng thái để biết được có xe hay không có xe tai nhà giữ . Ngoài ra còn các trường ID khách hàng , private key uca khách hàng , id nhà xe của khách hàng , ghi chú , email



Hình 4.7: Cơ sở dữ liệu của Raspberry

4.6 Hệ thống xác thực trên Raspberry

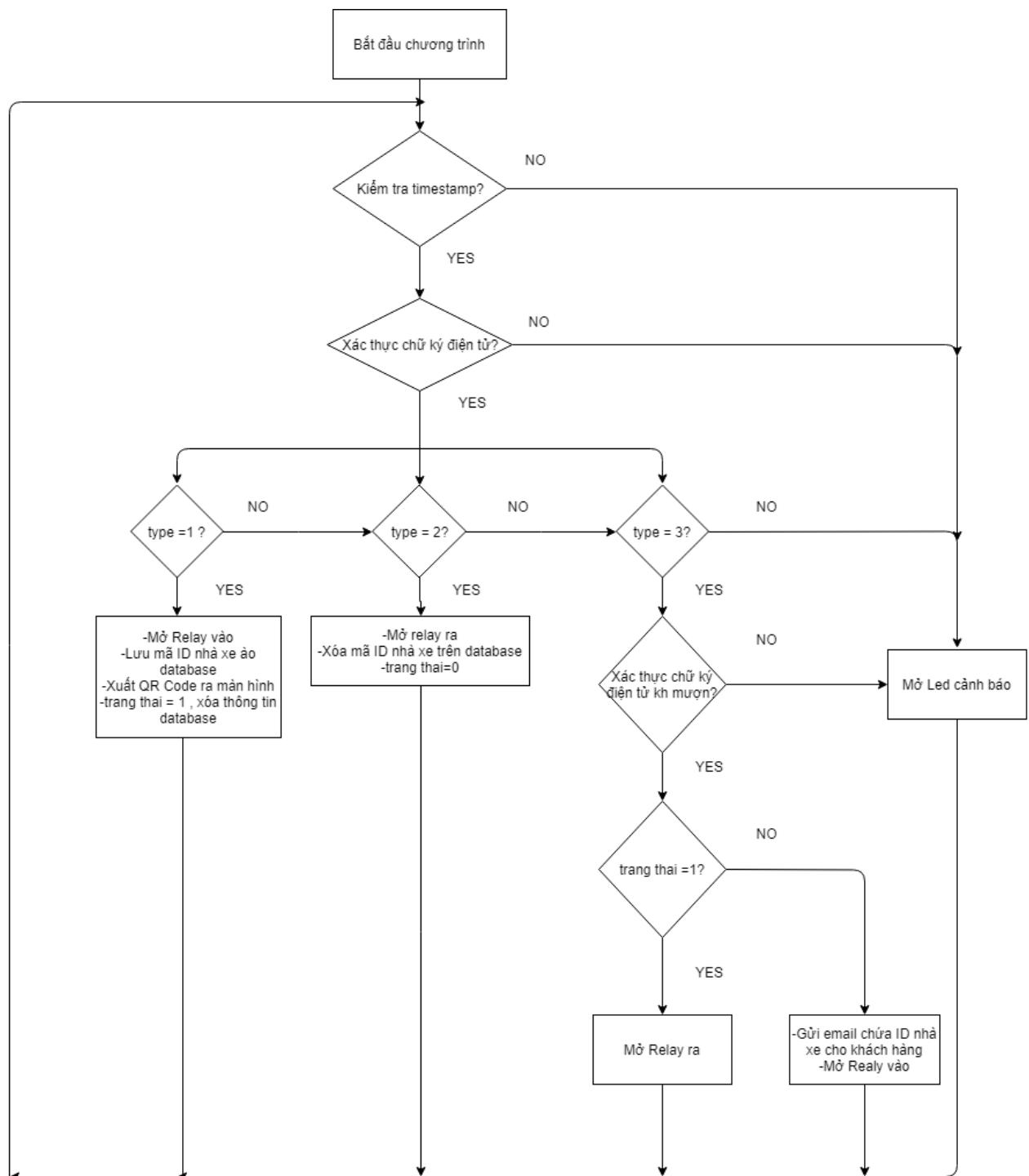
Đầu tiên chúng ta sẽ nhận diện QR Code thông qua Camera . Chúng ta sử dụng thư viện pyzbar trong thư viện này chúng ta sẽ lấy nội dung QR Code bằng lệnh decode(image) với image là frame nhận được từ camera .

```
image=frame.array
barcodes=pyzbar.decode(image)
```

Khi nhận được nội dung , lúc này raspberry sẽ biết được các trường của QR Code Như vậy khi đến hệ thống xác thực . Điều đầu tiên là đang nhập vào cơ sở dữ liệu

```
mydb=mysql.connector.connect(
host="localhost",
user="root",
passwd="test",
database="testdb",
)
```

Sau đó chúng ta sẽ kiểm tra timestamp.Thời gian này được tạo từ time epoch tương tự như trong thiết bị android . Nếu kết quả trả về trị int chênh lệch nhau trong khoảng 10 thì timestamp ko quá hạn.Tiếp tục từ ID khách hàng chúng ta truy xuất vào database để lấy các dữ liệu cần thiết , đầu tiên là khóa công khai của khách hàng tương ứng với ID



Hình 4.8: Lưu đồ giải thuật hệ thống xác thực

```

sql_select_query="""select * FROM users WHERE id = %s"""
my_cursor.execute(sql_select_query (barcodeData_string['idkhachhang'],))
result = my_cursor.fetchall()
for row in result:
    break
n=int(row[3])
e=int(row[2])

```

Như vậy lệnh SELECT sẽ truy xuất cơ sở dữ liệu tương ứng mã ID khách hàng và raspberry nhân biết được mã ID khách hàng dựa vào chuỗi JSON . Từ mã ID này chúng ta có giá trị của cột thứ 2 và cột thứ 3 trong database chính là public key . Sau đó chúng ta dùng khóa này này để xác thực chữ ký điện tử .

```

s1=hashlib.md5(barcodeDatastring['idkhachhang'].encode('us-ascii')).hexdigest()
k=bin(int(binascii.hexlify(s1.encode('utf-8')),16))
k2=int(k,2)
c1=int(barcodeDatastring['rsaidkhachhang'])
k1=pow(c1,e,n)

```

Quá trình xác thực gồm 2 bước bước đầu chúng ta sẽ giải mã RSA k1=pow(c1,e,n) . Sau đó ta sẽ dùng ID khách hàng và băm MD5 chuỗi đó là s1 . Ngược lại với quá trình mã hóa ở phần trước thì từ mã băm s1 ta chuyển lại sang mã ascii , và từ mã ascii chúng ta lại chuyển sang dạng nhị phân bằng lệnh bin() . Sau khi đã có mã nhị phân ta chuyển lại dạng int bằng lệnh int(k,2) . Như vậy cuối cùng chúng ta có chuỗi sau khi băm là k2. Như vậy việc xác thực diễn ra chính xác khi và chỉ khi k1 = k2 .

Đến đây raspberry sẽ tiếp tục kiểm tra type Nếu type bằng 1 , thì Relay bên cổng vào sẽ mở .Lúc này raspberry sẽ tạo ra mã ID nhà xe bằng thời gian epoch tương tự như trong android . Rraspberry sẽ xuất ra màn hình mã ID nhà xe và văn bản mã hóa RSA của mã ID đó . Trong mỗi nhà xe cũng sẽ có 1 cặp khóa điện tử tương ứng . Để in ra màn hình mã QR Code chúng ta sẽ dụng thư viện matplotlib để thực hiện việc này:

```

imgplot=plt.imshow(mpimg.imread("myQR"))
plt.ion()
plt.show()

```

Đồng thời mã ID nhà xe được tạo ra cũng sẽ được lưu trên database của raspberry .Chúng ta dùng lệnh UPDATE sẽ ghi mã ID nhà xe lên database tương ứng với ID nhà xe

```

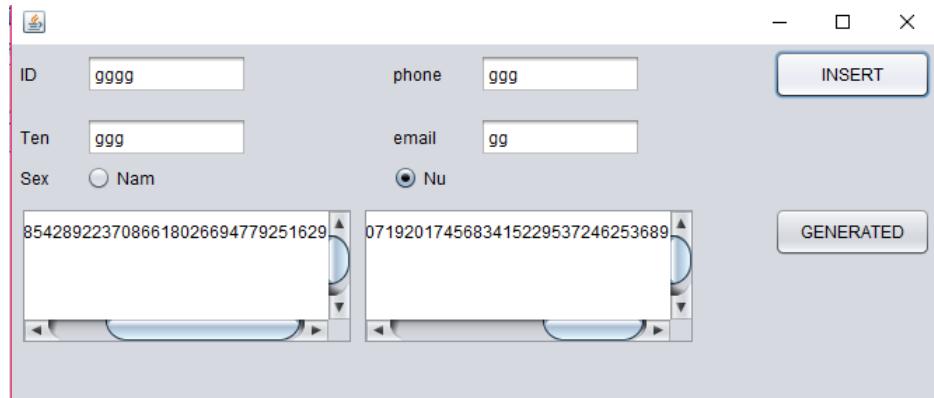
my_sql = """UPDATE users SET idnhaxe = %s WHERE id = % s"""
my_cursor.execute(my_sql,(ticksguixe2,barcodeData_string['idkhachhang'],))

```

Trường hợp khi type bằng 2 , lúc này thì raspberry sẽ chỉ mở Relay ra và xóa mã ID nhà xe trên database . Lưu ý khi bắt cứ trường hợp nào xe vào biến trạng thái trên database cũng sẽ được cập nhật . Khi có xe ở trong bãi thì bằng 1 , không có xe ở trong bãi thì bằng 0 Cuối cùng với type loại 3 . Với mã QR Code này có tới 8 trường . Sau khi xác thực chữ ký điện tử khách hàng xong thì raspberry tiếp tục xác thực chữ ký điện tử của khách hàng mượn . Nếu xác thực đúng tiếp thì sẽ xét đến biến trạng thái lưu trên database . Nếu biến trạng thái bằng 1 tức là lúc này xe đang ở trong bãi và khách hàng mượn muốn lấy xe ra như vậy Relay bên vào sẽ mở . Còn nếu biến trạng thái bằng 0 tức lúc này xe đã ở ngoài nên sẽ mở Relay bên vào vì khách hàng mượn muốn gửi xe trở lại

4.7 Ứng dụng CA Server trên Java-Netbeans

Như vậy cuối cùng chúng ta cần có 1 chổ tạo khóa và lưu khóa lại . Chúng ta sẽ làm theo mô hình PKI X.509.



Hình 4.9: PKI trong luận văn

Ứng dụng sẽ tạo thông tin của khách hàng .như ID , tên điện thoại , email ... Đầu tiên chắc chắn chúng ta sẽ tạo 1 cặp key cho khách hàng

```
public void KeyRSA(int bits){ SecureRandom r = new SecureRandom();
BigInteger p = new BigInteger(bits , 100, r);
BigInteger q = new BigInteger(bits , 100, r);
n = p.multiply(q);
BigInteger m = (p.subtract(BigInteger.ONE)).multiply(q .subtract(BigInteger.ONE));
boolean found = false;
do {
e = new BigInteger(bits , 50, r);
if (m.gcd(e).equals(BigInteger.ONE) & & e.compareTo(m) < 0) {
found = true;
}
} while (found);
d = e.modInverse(m); }
```

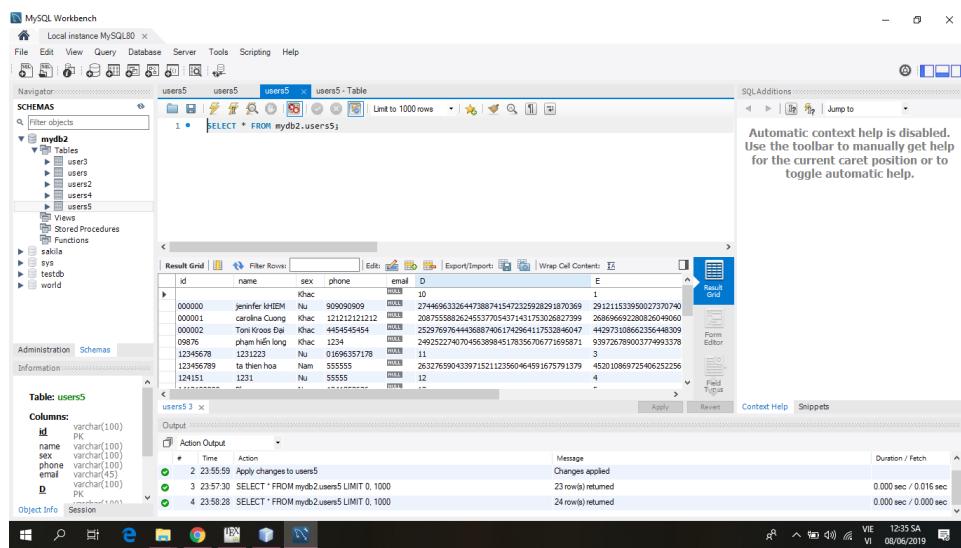
Hàm KeyRSA trên tao cặp key cho khách hàng với bits là giá trị int . Trong luận năn chúng ta chọn 128 bits . Chúng ta sẽ chọn random hai số BigInteger .sau đó thực hiện thuật toán như phần 2.3.5 đã trình bày .

Như vậy sau khi tạo xong khóa . Chúng ta sẽ điền các thông tin của khách hàng và lưu vào trong database

```
PreparedStatement stmt = con.prepareStatement
("INSERT INTO USERS5 VALUES(?,?,?,?,?,?)");
stmt.setString(1, id);
stmt.setString(2, name);
stmt.setString(3, sex);
stmt.setString(4, phone);
```

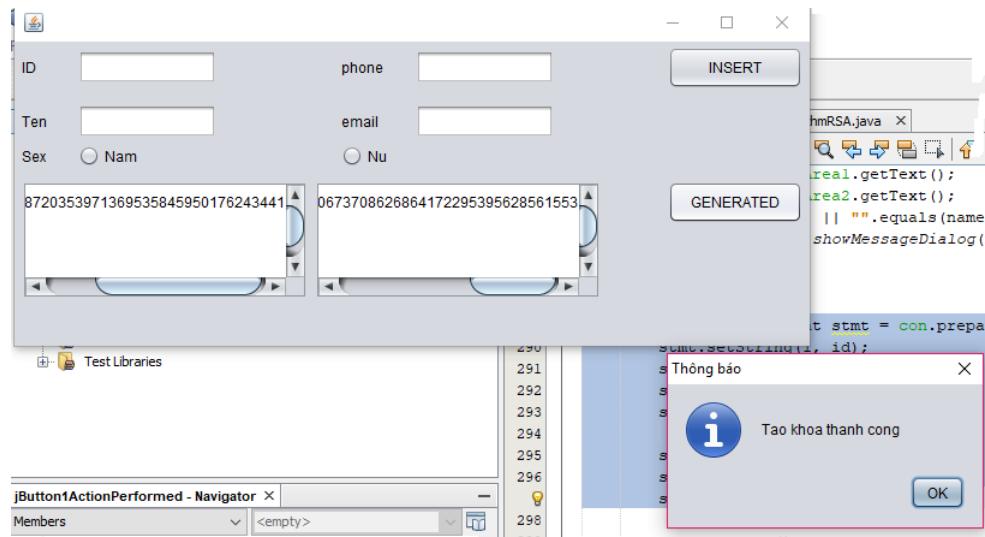
```
stmt.setString(5, email);
stmt.setString(6, dd);
stmt.setString(7, ee);
stmt.setString(8, n);
```

Chúng ta dùng lệnh INSERT INTO để thêm dữ liệu vào database của máy tính. Hình 4.10 cho thấy cơ sở dữ liệu trên máy tính

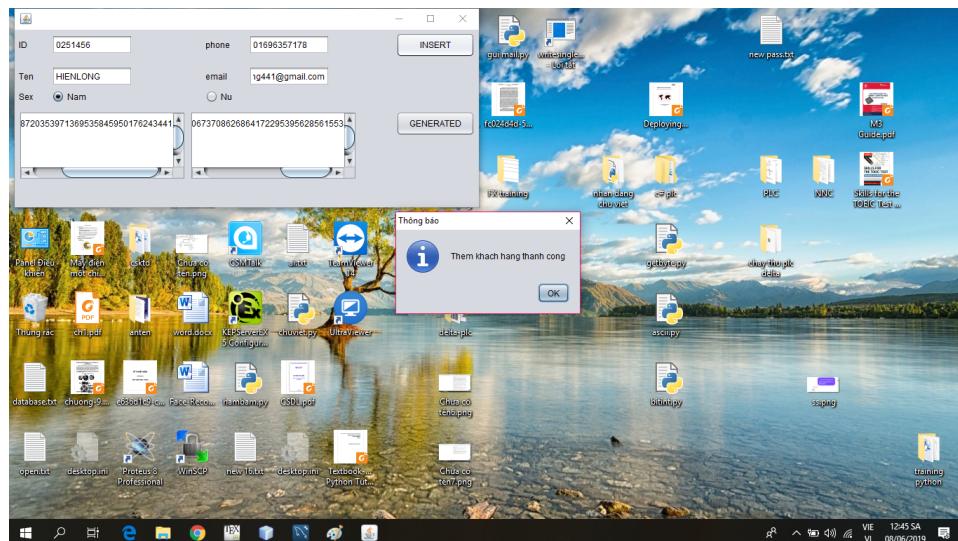


Hình 4.10: Database cho khách hàng trong PKI

Khi ứng dụng được thực hiện đầu tiên chúng ta phải nhấn tạo key . Khi tạo key xong tiếp tục chúng ta mới tạo thông tin và insert vào database



Hình 4.11: Hệ thống thông báo khi tạo khóa thành công



Hình 4.12: Hệ thống thông báo khi thêm khách hàng thành công

4.8 Tổng Kết

Như vậy chúng ta đã hoàn thành được hệ thống phần xác thực hoàn toàn đạt yêu cầu . Tuy nhiên hệ thống vẫn còn một số yếu điểm cần cải thiện

Chương 5

HOẠT ĐỘNG , ĐÁNH GIÁ

Sau khi thực hiện xong được hệ thống chúng ta quay lại đánh giá các tiêu chí ban đầu đặt ra , đồng thời tìm cách cải thiện các điểm yếu của nó và mở rộng nó hơn nữa

5.1 Mức độ hoàn thành trong luận văn

Bảng 5.1 trình bày những mục tiêu đặt ra và mức độ hoàn thành trong luận văn
Như vậy trong luận văn chúng ta đã làm được tạo QR Code chứa chữ ký điện tử trên thiết bị Android thông qua ứng dụng Gửi xe . Tạo QR Code chứa chữ ký điện tử trên python trong reaspberry và giải mã RSA từ các trường trong QR Code và xác thực chữ ký điện tử trên raspberry thông qua hệ thống xác thực . Giải mã RSA từ các trường QR Code và xác thực chữ ký điện tử thông qua ứng dụng trả và cho mượn xe . Giao tiếp với cơ sở dữ liệu (MySQL) và các chân GPIO trên chân raspberry thông qua hệ thống xác thực .Cuối cùng có thể tạo 1 ứng dụng trên Netbean (Java) để có thể tạo key (public key và private key), thông tin khách hàng và lưu nó trong cơ sở dữ liệu

Mục tiêu đặt ra	Làm được	Hoàn thành 50%	Chưa làm được
Tạo QR chứa chứa ký điện tử trên thiết bị Android	*		
Tạo QR Code chứa chữ ký điện tử trên Raspberry	*		
Giải mã RSA và xác thực chữ ký điện tử trên thiết bị Android	*		
Giải mã RSA và xác thực chữ ký điện tử trên Raspberry	*		
Lưu và truy xuất dữ liệu khách hàng trên MySQL	*		
Hệ thống xác thực hoạt động như sơ đồ và điều khiển các Relay , Led bằng các chân GPIO trên Raspberry	*		
Tạo CA Server để quản lý Key		*	

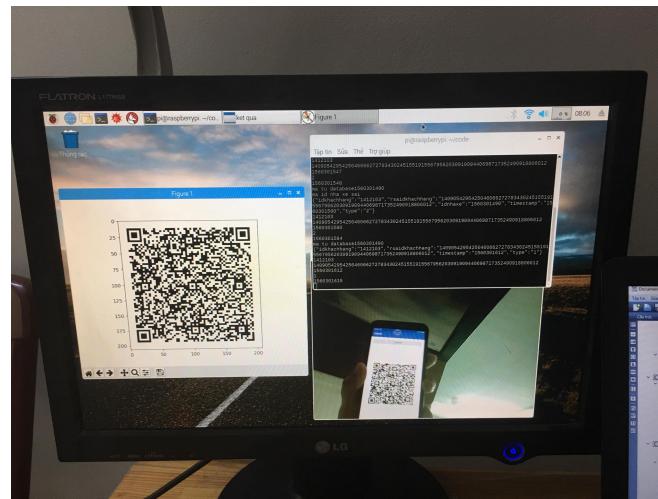
Bảng 5.1: Các mục tiêu đặt ra và mức độ hoàn thành

Các vấn đề hiện tại chưa thể làm được trong luận văn

- Chưa thể kết nối từ raspberry đến CA Server . Hệ thống raspberry chưa thể download dữ liệu người dùng
- Chưa mở rộng được hệ thống để có thể kết hợp các trạm giữ xe ở các toàn nhà khác nhau và khác quyền admin

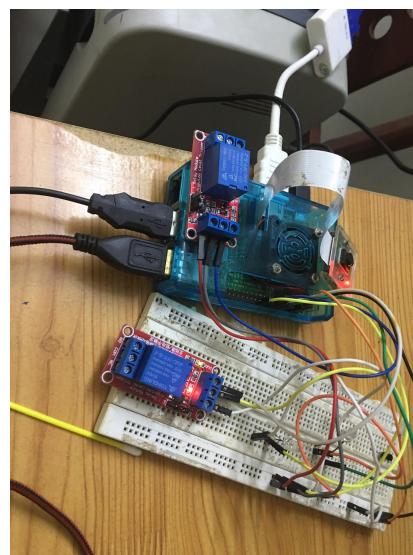
5.2 Kịch bản sử dụng

Bước 1 : Gửi xe khách hàng đang ký sử dụng dịch vụ . CA Server sẽ tạo 1 cặp key gồm Public key và Private key và 1 ID tương ứng với mỗi người . Đồng thời trong thiết bị Android của khách hàng sẽ được cài 3 ứng dụng GUIXE , TRACHOMUON , MUONXE.



Hình 5.1: Khách hàng gửi xe thành công

Bước 2 khách hàng đem xe gửi vào bãi , sau đó sẽ mở ứng dụng GUIXE tạo 1 QR Code có chứa chữ ký điện tử được mã hóa bắt đầu bằng phương thức RSA . Chữ ký điện tử sẽ dùng Private Key để mã hóa . Khách hàng scan QR Code vào Raspberry pi . Lúc này Raspberry sẽ kiểm tra trong Database nếu có khách hàng tương ứng với trường ID trong QR Code thì sẽ lấy dữ liệu public key từ Database sau đó tiến hành xác thực chữ ký điện tử và điều khiển Relay thích hợp .Nếu không có khách hàng (lần đầu gửi xe) thì Raspberry sẽ download Public key từ FTP Server và sẽ lưu Public key vào Database . Kể từ lần thứ 2 nó sẽ không download nữa mà lấy từ Database . Đồng thời khi xác thực chữ ký điện tử trên Raspberry , nếu kết quả đúng Raspberry sẽ lấy thời gian mà khách hàng scan vào chuyển thành chuỗi text và mã hóa nó bằng Private key của nhà xe (chữ ký điện tử của nhà xe) sau đó nén 2 trường thành QR Code và xuất ra màn hình LCD . Đồng thời cũng lưu chuỗi text đó vào Database Raspberry tương ứng với khách hàng.

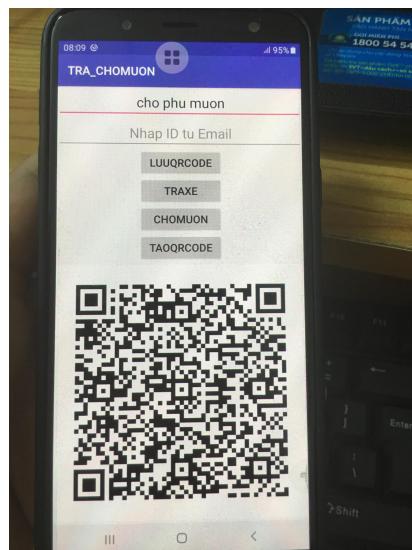


Hình 5.2: Relay hệ thống bật

Bước 3 lúc này khách hàng sẽ mở ứng dụng TRACHOMUON và quét QR Code trên màn hình Raspberry . Thiết bị Android lúc đầu đã được lưu Public key của nhà xe sẽ giải mã và xác thực chữ ký điện tử của nhà xe nếu đúng ứng dụng TRAXE sẽ lưu chuỗi text vào bộ nhớ trong.

Bước 4 : Trả xe khi khách hàng trả xe , sẽ mở ứng dụng TRACHOMUON và tạo QR Code chứa chữ ký điện tử của khách hàng và thêm 1 trường chuỗi text đã lưu ở bước 3 . Lúc này khách hàng sẽ scan QR Code đó vào Raspberry . Hệ thống sẽ tiếp tục xác thực chữ ký điện tử , và kiểm tra chuỗi text đã được lưu . Nếu đúng tất cả thì mở Relay thích hợp

Bước 5 : Mượn xe khi 1 khách hàng A muốn mượn xe của khách hàng B thì khách hàng B sẽ mở ứng dụng TRACHOMUON và tạo QR Code , khách hàng B sẽ mở ứng dụng MUONXE và scan QR Code của khách hàng A . Khi đó khách hàng B đã có chữ ký của khách hàng A đồng thời có lươn chuỗi text mà nhà xe đưa cho khách hàng A ở Bước 3 . Khi đó khách hàng ra nhà xe và tạo QR Code trong ứng dụng MUONXE để scan vào Raspberry . Raspberry sẽ tiến hành giải mã chữ ký điện tử của khách hàng B , sau đó giải mã chữ ký điện tử của khách hàng A , sau đó kiểm tra chuỗi text của khách hàng B trên database . Nếu việc kiểm tra chính xác , hệ thống sẽ mở Relay thích hợp . Khi gửi lại xe thì khách hàng sẽ tạo lại QR Code từ ứng dụng MUONXE và chụp hình QR Code mà nhà xe xuất ra để đưa thông tin cho chủ sở hữu (người cho mượn)

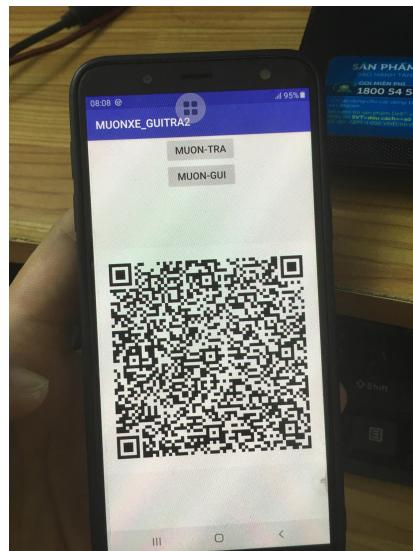


Hình 5.3: Khách hàng cho mượn xe

Lưu ý để chống lại replay attack (tấn công phát lại) mỗi mã QR Code đều có thời gian hiệu lực là 30s. Mỗi QR Code đều có đính 1 trường timestamp . Mỗi lần khách hàng tạo lại mã QR Code tạo lại 1 timestamp nhưng không tạo lại chữ ký điện tử

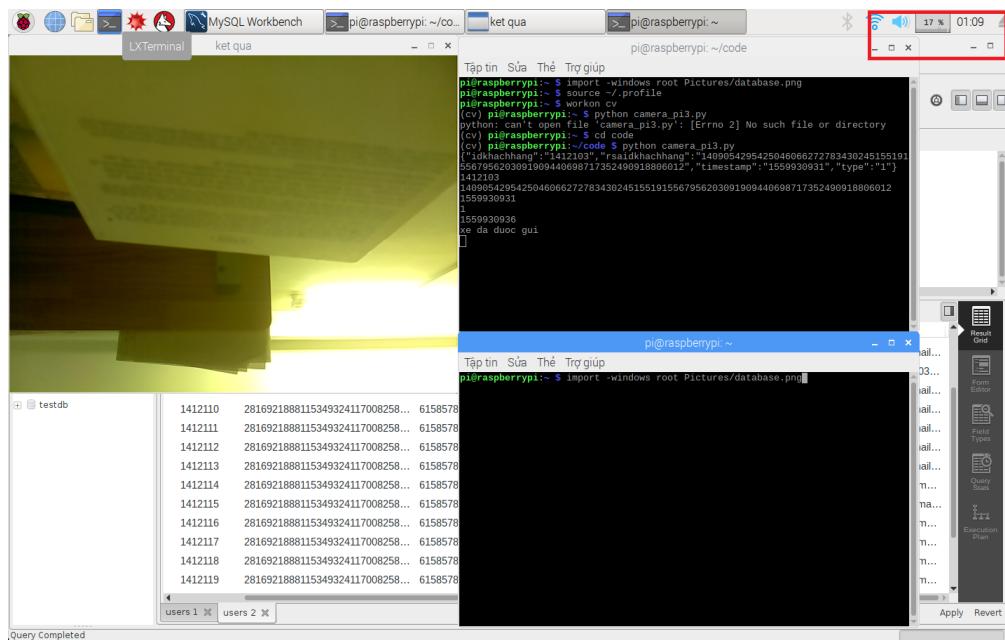
5.3 Hoạt Động , Đánh Giá

Chúng ta thử kiểm tra hoạt động .Đầu tiên chúng ta thử sử dụng với database có 20 người . Như hình chúng ta thấy rằng CPU của raspberry làm việc trong khoảng từ 16-25%.Chúng ta



Hình 5.4: Khách hàng lưu QR Code cho mượn

thử tăng thêm khoảng 40 người trong database . Lúc này hệ thống CPU cũng chỉ hoạt động từ 17-25% . như vậy từ đ1o chúng ta có thể đánh giá hệ thống sử dụng cho 100-200 người hoặc nhiều hơn thì vẫn có thể chấp nhận được

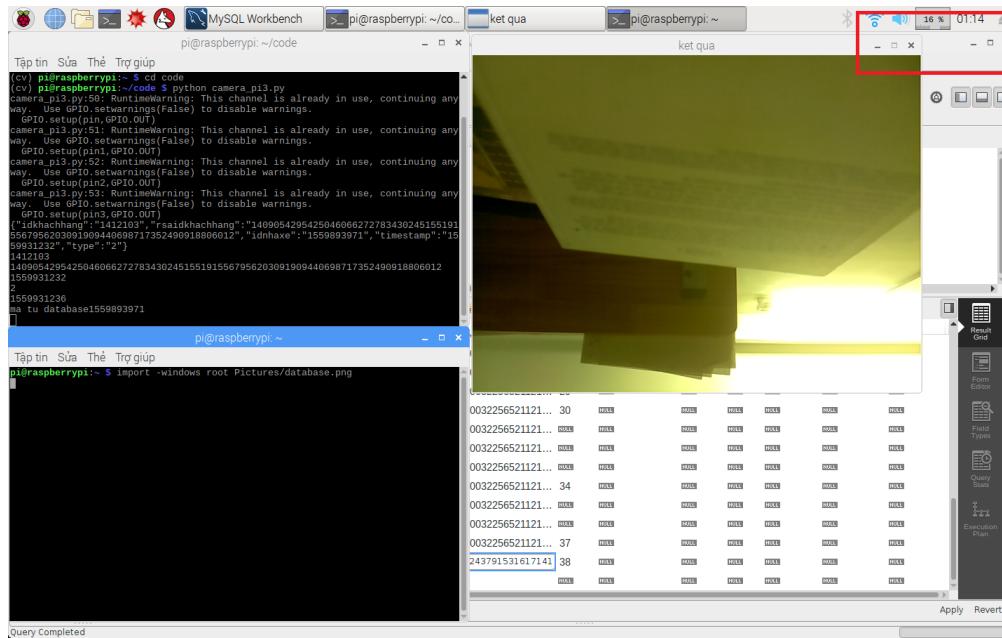


Hình 5.5: Hệ thống hoạt động với 20 người

Lúc này hệ thống CPU cũng chỉ hoạt động từ 17-25% . như vậy từ đó chúng ta có thể đánh giá hệ thống sử dụng cho 100-200 người hoặc nhiều hơn thì vẫn có thể chấp nhận được

Như vậy sau khi hoàn thành được hệ thống . Chúng ta nhận thấy hệ thống tuy chưa hoàn hảo nhưng cũng có thể giải quyết được tối thiểu các yêu cầu đặt ra ban đầu :

- Đảm bảo tính chính xác bằng mã hóa RSA



Hình 5.6: Hệ thống hoạt động với 40 người

- Giải quyết được tính tự động tức là việc xác thực kiểm tra sẽ do máy tính không còn thông qua mắt con người
- Không cần các loại thẻ từ
- Giải quyết được tối thiểu một vài trường hợp mượn xe mà nhà xe vẫn quản lý được người mượn và người cho mượn
- Giá cả hợp lý Raspberry và camera cùng với các dụng cụ có giá khoảng 1,7 triệu VND
- Hệ thống hoàn toàn có thể mở rộng lớn hơn nữa

Nhưng với hệ thống thiết kế chúng ta gấp 1 điểm yếu đó là trong 1 phút chúng ta chỉ có thể giải quyết được khoảng 5 xe . Như vậy là quá thấp so với các giải pháp khác .Chúng ta cần giải quyết vấn đề này thì hệ thống sẽ tốt hơn

Các giải pháp	Thời gian TB 1 khách hàng	Lưu lượng trong 1 phút
Hệ thống sử dụng sinh trắc học	3	20
Hệ thống sử dụng RFID cài tiến	5	12
Hệ thống sử dụng cách nhập mật khẩu	10	6
Hệ thống dùng mã hào RSA	12	5

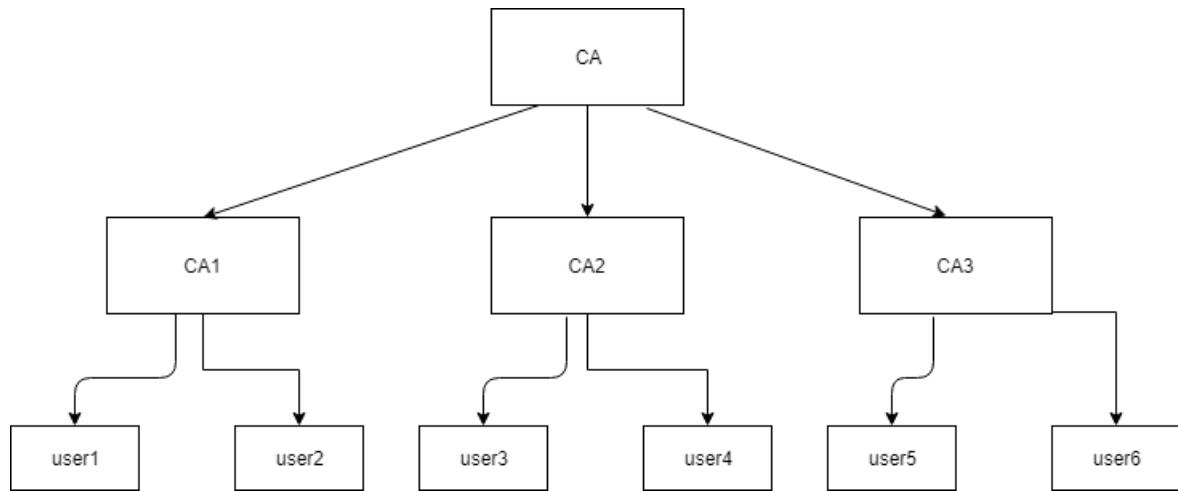
Bảng 5.2: So sánh lưu lưu lượng xe của các giải pháp

5.4 Mở rộng , hướng phát triển

Như vậy hệ thống nhìn chung ổn định nhưng có 1 vấn đề nữa xảy ra đó là tình trạng khách vãng lai . Bất kỳ một bãi giữ xe cho dù dùng cách thứ nào đi nữa thì luôn phải có khách vãng lai . Và một trường hợp gần hơn nữa đó là khi khách hàng ở tòa nhà thứ 2 qua toàn nhà thứ 1 gửi xe thì đương nhiên trong database của tòa nhà thứ 1 không có dữ liệu của khách hàng đó .Trong lúc này chúng ta sẽ giải quyết vấn đề bằng cách mở rộng hệ thống lên

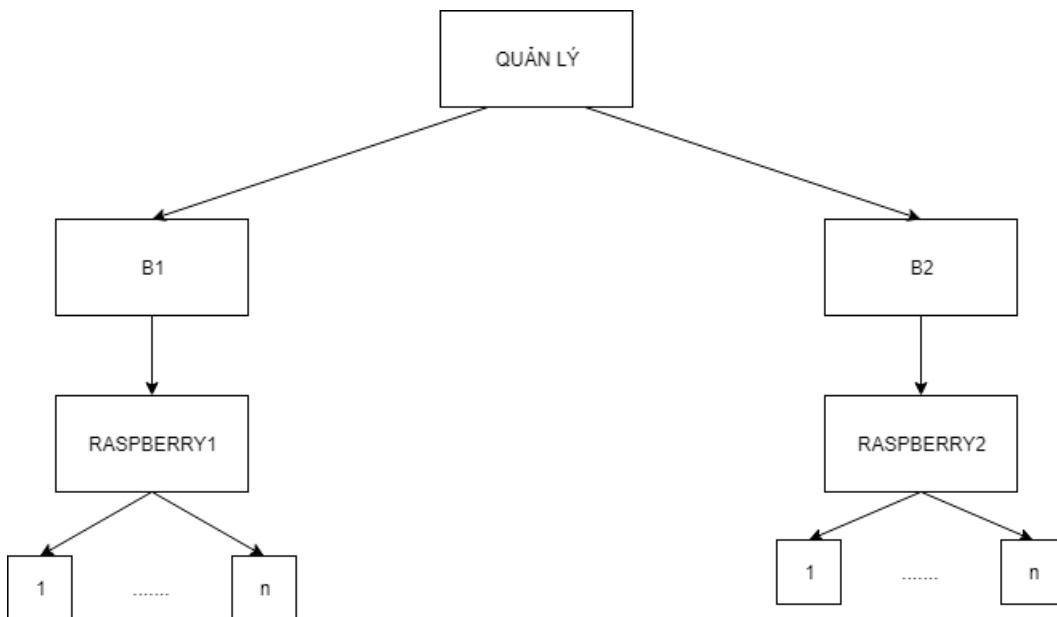
5.4.1 Hierarchical Model

Hierarchical model là một hệ thống hình cây với root là một CA . Hệ thống CA tổng này có thể chứng nhận các CA khác . CA root này cần được tin tưởng bởi các CA khác trong 1 hệ thống.Hình 5.8 cho thấy hình dạng của hệ thống này .Như vậy CA sẽ xác nhận cho CA1 ,CA2 và CA3 . và CA1 , CA2 , CA3 sẽ chứng nhận cho các user .Như vậy ví dụ user1 muốn biết public key của user2 thì lúc này user2 sẽ gửi 1 chuỗi chứng thực CA«CA1» và CA1«user2» cho user1. Lúc này user1 sẽ phê chuẩn CA«CA1» bằng publickey của CA .Sau đó user1 giải nén public key của CA từ CA«CA1» .User1 tiếp tục phê chuẩn CA1«User2» thông qua public key của CA1 . User1 giải nén public key của user2 từ CA1«User2»



Hình 5.7: Mô hình PKI Hierarchical

5.4.2 Ứng dụng mô hình Hierarchical vào hệ thống



Hình 5.8: Mô hình PKI Hierarchical

Như vậy khi ứng dụng mô hình này vào luận văn , giả sử có hai trạm B1 và B1 tương ứng cho hai toàn nhà khác nhau có thể cùng admin(chủ tòa nhà) hoặc khác admin .Giả sử khách hàng ở trạm B2 , ví dụ là A, muốn gửi xe ở trạm B1 dù cho hai trạm này có thể là chủ khách nhau . Lúc này trong database của raspberry ở trạm B1 không có thông tin về khách hàng A này để xác thực , thông tin này chính là public key dùng để xác thực chữ ký điện tử . Như vậy lúc này raspberry ở trạm B1 muôn biết public key của khách hàng này. Lúc này khi khách hàng scan mã QR Code gửi xe thì đã cung cấp cho trạm B1 ID và trạm mình đăng ký thông qua các trường trong QR Code .Lúc này trạm B1 sẽ yêu cầu lên cấp cao hơn là trạm QUANLY thông tin yêu cầu là ID và trạm của khách hàng. Và trạm QUANLY sẽ gửi yêu cầu xuống cho trạm B2 . Trạm B2 sẽ gửi public key khách hàng , kèm theo bản mã hóa ID khách hàng bằng

private key của trạm B2 cho trạm QUANLY .Do trạm quản lý sẽ xác thực các trạm B1,B2 nên QUANLY sẽ dùng public key của trạm B2(đã biết) , để giải mã và so sánh ID nếu đúng thì trạm QUANLY sẽ tin tưởng đây là thông tin của trạm B2 . Lúc này trạm QUANLY GỬI tiếp tục thông tin khách hàng đó và văn bản mã hóa ID khách hàng bằng private key của trạm QUANLY và public key và văn bản mã hóa của trạm B2 cho trạm B1. Lúc này trạm B1 sẽ dùng public key của trạm QUANLY (đã biết) xác thực chuỗi ID .Tiếp tục xác thực mã ID mã hóa của trạm B2. NẾU xác thực đúng hết thì raspberry sẽ lưu mọi hông tin cẩu kahch1 hàng đó vào database của mình. Lần sau sẽ không cần truy cập vào nhà mạng.Tóm lại nếu muốn gửi 1 public key và xác minh public key khách hàng chính xác thì phải gửi public key của khách hàng đó kèm theo văn bản mã hóa bằng private key của trạm thì khi đó xác nhận chính xác thì public key khách hàng mới có giá trị
Như vậy nếu có thể mở rộng lên được thì hệ thống sẽ lớn và phát triển hơn rất nhiều so với các phương thức giữ xe khác .Đồng thời khi hệ thống này lớn hơn , mỗi người đều có một chữ ký điện tử thì lúc này sẽ có các CA cấp quận , huyện ,...Tình trạng khách vãng lai sẽ được giải quyết

5.5 Tổng Kết

Hệ thống hoạt động ổn định , các đánh giá phù hợp với tiêu chuẩn đặt ra lúc đầu . Tuy nhiên hệ thống này cần mở rộng lên nhiều tầng và lớp hơn và cách thức sử dụng phải được đơn giản hơn nữa

Chương 6

KẾT LUẬN

Cách mạng công nghiệp 4.0 đang diễn ra mạnh mẽ, trong cuộc cách mạng này điện thoại thông minh (smart phone) đóng một vai trò vô cùng quan trọng, chúng ngày càng nhanh hơn, mạnh mẽ hơn, tiện lợi hơn và gần như mỗi người đều có cho mình một chiếc điện thoại thông minh. Bên cạnh đó, trong thời đại số hóa, thông tin được xem là một nguồn tài nguyên quý giá vì vậy việc mã hóa, xác thực, kiểm soát truy cập, đảm bảo an toàn thông tin cũng là một yêu cầu thiết yếu. Đối với các hệ thống xác thực truy cập (access control) trên thị trường hiện nay có thể chia thành 3 hình thức xác thực như sau:

- Xác thực thuần thục chẳng hạn như cắp định danh – mật khẩu (username – password)...
- Xác thực bằng các loại thẻ từ (ví dụ RFID tag),...
- Nhận dạng bằng sinh trắc học (biometric identifier): chẳng hạn như dấu vân tay, mẫu võng mạc mắt, giọng nói, gương mặt...

Tuy nhiên, cả ba hình thức trên đều có những lỗ hổng nhất định như sau: Các hệ thống xác thực dùng phương pháp truyền thống: sử dụng mật khẩu do người dùng nhập vào do đó rất dễ suy ra từ các thông tin của chủ sở hữu như tên, ngày sinh, số điện thoại,... hơn nữa, các hệ thống này đòi hỏi người dùng phải ghi nhớ mật khẩu do đó, độ dài và độ phức tạp của mật khẩu không cao

Các hệ thống dùng thẻ từ (RFID tag...): các hệ thống này dùng sóng RF để truyền tải thông tin giữa đầu đọc và thẻ . Ngoài ra hệ thống còn có yếu điểm là tính tiện dụng, đòi hỏi người dùng phải mang theo thẻ để truy cập mặc khác bên cạnh thẻ RFID này còn phải mang theo các thẻ ngân hàng, thẻ thành viên siêu thị,...rất bất tiện.

Các hệ thống dùng sinh trắc học: dù tiện dụng không cần dùng thẻ, không cần nhớ mật khẩu nhưng rất dễ ảnh hưởng khi các yếu tố sinh trắc như vân tay, mống mắt bị thay đổi, hơn nữa khi đã biết chủ sở hữu có thể làm giả đặc điểm sinh trắc học

Từ các vấn đề nêu trên, luận văn đề xuất ý tưởng xây dựng một hệ thống bãi giữ xe thông minh . Hệ thống này sẽ được xây dựng với phần mềm phía người dùng được triển khai trên điện thoại thông minh, loại bỏ các thẻ từ RFID nhằm đem lại sự tiện dụng tối đa cho người dùng, giảm chi phí đầu tư lương lớn thẻ từ cho công sở. Cuối cùng hệ thống này có khả năng mở rộng rất lớn.

Hệ thống này sử dụng kỹ thuật:

- Chữ ký điện tử sử dụng mã hóa bắt đối xứng RSA
- QR code để truyền tải thông tin chữ ký giữa điện thoại thông minh và hệ thống xử lý.

Hệ thống xác thực bãi giữ xe mới áp dụng những công nghệ mạnh mẽ cung cấp mức độ an toàn cao hơn so với các hệ thống hiện có trên thị trường. Hệ thống mới được triển khai với phần mềm trên smart phone của người dùng, loại bỏ các thẻ RFID mang lại sự tiện dụng cao hơn, giảm chi phí đầu tư so với các hệ thống hiện tại.

Tài liệu tham khảo

- [1] Alexander Mordvintsev & Abid K OpenCV-Python Tutorials Documentation , Release 1, Addison-Wesley (2014).
- [2] Behrouz Forouzan Cryptography & Network Security,frist edition ,McGraw-Hill Education (February 28, 2007)
- [3] <https://stackoverflow.com/questions/1207457/convert-a-unicode-string-to-a-string-in-python-containing-extra-symbols>
- [4] <https://stackoverflow.com/questions/8928240/convert-base-2-binary-number-string-to-int>
- [5] <https://stackoverflow.com/questions/5618878/how-to-convert-list-to-string>
- [6] <https://viblo.asia/p/java-ma-hoa-va-giai-ma-voi-thuat-toan-rsa-bJzKmW3Xl9N>
- [7] <https://www.learnopencv.com/barcode-and-qr-code-scanner-using-zbar-and-opencv/>
- [8] <https://nguyendangkhiemit.wordpress.com/2014/10/19/chu-ky-so-su-dung-giai-thuat-rsa/>
- [9] <https://stackjava.com/demo/sha-la-gi-code-vi-du-sha1-sha2-voi-java.html>
- [10] <https://stackjava.com/demo/md5-la-gi-code-vi-du-md5-voi-java.html>