Đại học Quốc gia
Thành phố Hồ Chí Minh

Ngày nhận hồ sơ	
Mã số đề tài	

THUYẾT MINH
ĐỀ TÀI KHOA HỌC VÀ CÔNG NGHỆ

A1. THÔNG TIN CHUNG

Tên đề tài

- Tên tiếng Việt: Tăng cường cơ chế bảo mật cho hệ thống cửa tự động trong nhà thông minh
- Tên tiếng Anh: Advanced security mechanism for door-locking system in smart homes

A2. Thuộc ngành/nhóm ngành

Cơ khí, Tự động hóa, Kỹ thuật Giao thông;

A3. Loại hình nghiên cứu: Nghiên cứu ứng dụng

A4. Thời gian thực hiện: 10 tháng (kể từ khi được duyệt)

A5. Tổng kinh phí

Tổng kinh phí: 23.000.000 đồng (Bằng chữ: Hai mươi ba triệu đồng) , gồm
- Kinh phí từ ĐHQG-HCM: 23.000.000 đồng (Bằng chữ: Hai mươi ba triệu đồng)
- Kinh phí từ nguồn huy động: 0 đồng (Bằng chữ: Không đồng), trong đó:
  Vốn tự có: 0 đồng (Bằng chữ: Không đồng)
  Vốn khác: 0 đồng (Bằng chữ: Không đồng)

A6. Chủ nhiệm

Học hàm, học vị, họ và tên: TS. Trần Việt Hồng
Ngày, tháng, năm sinh: 03/05/1979, Phái: Nam
Số CMND: 001079010047, Ngày cấp: 25/02/2016, Nơi cấp: Tp. Hồ Chí Minh
Mã số thuế cá nhân: 8113021414
Số tài khoản: 0004100001782001 Tại ngân hàng: OCB
Địa chỉ cơ quan: 268 Lý Thường Kiệt, Quận 10, Tp Hồ Chí Minh
Điện thoại: 0902424148, Email: tvhong@hcmut.edu.vn

Tóm tắt hoạt động nghiên cứu và đào tạo sau đại học có liên quan đến đề tài của chủ nhiệm:

Đồng chủ nhiệm

Học hàm, học vị, họ và tên: Trần Bảo Ân
Ngày, tháng, năm sinh: 22/10/1993, Phái: Nam
Số CMND: 024805620, Ngày cấp: 02/11/2007, Nơi cấp: Tp. Hồ Chí Minh
Mã số thuế cá nhân: 8381190915
Số tài khoản: 0004100005952009 Tại ngân hàng: OCB - PGD Sài Gòn;
Địa chỉ cơ quan: 364 Cộng Hòa, p. 13, q. Tân Bình, TPHCM
Điện thoại: 01652323312, Email: hitmanhostline@gmail.com

A7. Cơ quan chủ trì

Tên cơ quan: Trường Đại học Bách Khoa - ĐHQG Tp. Hồ Chí Minh
Họ và tên thủ trưởng: GS.TS Vũ Đình Thành
Điện thoại: (84-8) 38.636.856 Fax: (84-8) 38.636.984
Email: khcn@hcmut.edu.vn
Số tài khoản: Tại kho bạc:

A8. Cơ quan phối hợp thực hiện

A9. Nhân lực nghiên cứu

TT	Học hàm, học vị, Họ và tên	SHCC/MSSV	Đơn vị công tác	Số tháng làm việc quy đổi
Thành viên chủ chốt				
1	TS. Trần Việt Hồng	002342	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	3
Nghiên cứu sinh, học viên cao học, sinh viên				
1	Trần Bảo Ân (1670543)	1670543	Công ty TNHH Robert Bosch Engineering and Business Solutions Việt Nam	3

B. MÔ TẢ NGHIÊN CỨU

B1. Tổng quan tình hình nghiên cứu trong, ngoài nước

Internet vạn vật (Internet of Things, IoT) là thuật ngữ dùng để chỉ các đối tượng có thể được nhận biết (identifiable) cũng như chỉ sự tồn tại của chúng trong một kiến trúc mang tính kết nối. Gần đây thuật ngữ này xuất hiện khá nhiều và thu hút không ít sự quan tâm chú ý của thế giới công nghệ vì sự bùng nổ của IoT trong tương lai sẽ có tác động mãnh mẽ tới cuộc sống, công việc và xã hội loài người. Việc trang bị những công nghệ theo dõi, nhận biết vào những vật thông dụng trong đời sống sẽ làm thay đổi rất nhiều cách chúng ta tương tác với đồ vật cũng như cách tương tác giữa người với người.

Hiện tại, IoT thường được nghĩ ngay tới các vấn đề liên quan đến nhà thông minh (smart homes) [1] làm tăng chất lượng cuộc sống. Tuy nhiên, ở cấp cao hơn là thành phố thông minh (smart cities), có thể giúp cho việc quản lý thành phố trở nên linh hoạt hơn, đáp ứng nhanh với các vấn đề xảy ra trong toàn thành phố. Như vậy, có thể thấy, và ta cũng thường được nghe, việc cần làm chỉ là chuẩn bị tinh thần kết nối, tuy nhiên việc kết nối này hiện nay chưa được thông suốt [2, 3] do chưa có một chuẩn kết nối chung [4]. Và một vấn đề cũng lớn không kém và gây ra nhiều lo ngại trong việc phát triển IoT là vấn đề bảo mật [5, 6].

Chủ nhiệm đề tài và nhóm nghiên cứu có kinh nghiệm và quan tâm đến vấn đề bảo mật nên đã chủ động nghiên cứu về vấn đề bảo mật trong nhà thông minh. Nhóm nghiên cứu đã chọn lựa cụ thể một bộ phận liên quan rất lớn đến nhiều vấn đề bảo mật, kể cả các cách tiếp cận trực tiếp và qua mạng đó là ổ khóa nhà để nghiên cứu, nhằm đề xuất các giải pháp góp phần vào việc đảm bảo an ninh cho các hệ thống smart homes nói riêng và hệ thống IoTs nói chung. Theo thống kê, trong năm 2015 có khoảng 4500 bài báo và 3000 bằng sáng chế, năm 2016 có khoảng 5200 bài báo và 3500 bằng sáng chế, 9 tháng đầu năm năm 2017 có khoảng 3300 bài báo và 900 bằng sáng chế liên quan đến ổ khóa trong nhà thông minh cho thấy số lượng lớn và sự ổn định qua các năm, chứng tỏ rằng đây là vấn đề đang nóng hổi. Bản thân chủ nhiệm đề tài và nhóm nghiên cứu đã hoàn thành một đề tài nghiên cứu khoa học cấp Trường vào năm 2016, đã có đóng góp một phải pháp bảo mật tại chỗ cho khóa cửa và đã có một bài báo khoa học được báo cáo tại một trong những hội nghị hàng đầu thế giới về bảo mật là FDSE. Thành viên chủ chốt của đề tài đó hiện tại đang là học viên cao học vẫn tiếp tục hướng nghiên cứu này, nhưng mở rộng hơn lên tầm mức toàn hệ thống nhà thông minh. Hiện tại, cấu trúc hệ thống khóa trong hệ thống nhà thông minh có thể hình dung như sau:

Hình 1. Cấu trúc thông thường của hệ thống khóa trong nhà thông minh

Như thể hiện trong Hình 1, có 2 đối tượng trực tiếp giao tiếp với khóa là Người sử dụng (mang nghĩa là chủ nhà) và khách khứa, bạn bè, hàng xóm láng giềng, người giao hàng, người đưa thư, ... (mang nghĩa là khách). Người sử dụng thì có thể giao tiếp hai chiều và giao tiếp trực tiếp tới hệ thống mạng điều khiển. Còn đối tượng khách thì chỉ giao tiếp trực tiếp với ổ khóa. Các ổ khóa trong một hệ thống được điều khiển bằng một hệ thống mạng. Hệ thống điều khiển qua mạng này có 2 công việc chính:
- Thứ nhất, điều khiển đóng/mở khóa tùy theo tình trạng yêu cầu từ những người giao tiếp với khóa và phân quyền, thực hiện qui trình thay đổi mật mã.

- Thứ hai, lưu trữ các thông tin về tình trạng khóa và cung cấp các thông báo trở lại khóa.

Mỗi đường kết nối như vậy trong hệ thống đều co thể là chỗ yếu về bảo mật để các đối tượng xấu khai thác.

Việc giải quyết được vấn đề bảo mật trong liên kết trực tiếp giữa chủ nhà hoặc khách với khóa cửa trong đề tài cấp Trường như đã nêu trên, ngoài việc đảm bảo an toàn cho một kết nối trong chuỗi kết nối của hệ thống khóa trong nhà thông minh, còn giúp nhóm nghiên cứu phát triển được một giải pháp tăng cường bảo mật cho toàn bộ hệ thống.

B2. Ý tưởng khoa học, tính cấp thiết và tính mới

**** Ý tưởng khoa học***

Với việc đảm bảo gần như tuyệt đối cho mối liên kết giữa người (chủ nhà hay khách) với khóa cửa bằng mã hóa Rolling code kết hợp RSA (trong đề tài cấp Trường T-CK-2016-02), hệ thống khóa cửa cho nhà thông minh có thể được cấu trúc lại như sau:

Hình 2. Cấu trúc của hệ thống khóa trong nhà thông minh được đề xuất mới

Điểm khác biệt lớn nhất trong mô hình đề xuất này so với hệ thống thông thường là tăng khả năng kiểm soát cho người sử dụng (chủ nhà). Lưu ý rằng có thể có nhiều chủ nhà. Trước hết, kết nối giữa khách và khóa là 2 chiều theo tính năng của mã Rolling code kết hợp RSA, nhưng vẫn đảm bảo an toàn. Thứ hai, các kết nối trong mạng điều khiển cũng là nơi có tỉ lệ tấn công cao thì sẽ được tăng thêm một tầng bảo mật bằng cách giới hạn việc điều khiển khóa từ người sử dụng thông qua mạng. Giao tiếp giữa người sử dụng và mạng chủ yếu chỉ là thay đổi password, một việc mà lâu lâu xảy ra một lần và xuất hiện tại một thời điểm không biết trước, sẽ làm giảm khả năng kẻ xấu trích lọc ra được password. Như vậy, cần có thêm một đường kết nối trực tiếp từ người sử dụng đến khách để thay thế, và con đường này có thể được thực hiện bằng tin nhắn SMS như cách các ngân hàng hiện giờ đang làm với mã OTP, giúp bảo mật mà vẫn tiện lợi, và người sử dụng còn thêm tính chủ động và kiểm soát. Các chức năng khác trong mạng vẫn giữ nguyên, nhưng lưu ý rằng các kết nối này yêu cầu phải biết password. Do đó, kẻ xấu sẽ chỉ còn một con đường là tấn công trực tiếp vào mạng, có thể thông qua internet chứ khó lòng tấn công gián tiếp qua con người. Hiện giờ, việc tấn công trực tiếp qua internet này thì nằm ngoài khả năng của bất kỳ nhóm nghiên cứu nhỏ lẻ nào mà hiện nay vẫn là vấn đề của toàn ngành bảo mật trên toàn thế giới.

**** Tính cấp thiết***

Với tốc độ phát triển nhanh chóng của nhà thông minh và các hệ thống IoTs như hiện nay, đặc biệt là vấn đề bảo mật trong hệ thống IoTs, vấn đề mà đề tài giải quyết mang tính thời sự, rất cần thiết hiện nay.

**** Tính mới***

Nhờ dựa trên nền tảng là mối liên kết trực tiếp giữa người và khóa có độ bảo mật rất cao, qui trình và cấu trúc hệ thống khóa cửa cho nhà thông minh được đề xuất là hoàn toàn mới, chưa được công bố trước đây.

B4. Tài liệu tham khảo

[1] Seana Moran. Ethical Ripples of Creativity and Innovation. 978-1-349-70059-2, 2016

[2] BBC Technology Staff. Internet of Things starter kit unveiled by ARM and IBM. British Broadcasting Corporation, 24/2/2015.

[3] Palmer, M. Expect the spectacular – but just not yet. The Financial Times, 28/1/2015, p. 1-2

[4] Yu, A. Tech companies take step toward the “Internet of Things.” National Public Radio. 13/12/2013

[5] Behar, M. Invasion of the body hackers. The New York Times, 25/5/2014, p. MM36.

[6] Belton, P. Is your toaster a silent recruit in a “thingbot” army? British Broadcasting Corporation, 17/2/2015.

B5. Kế hoạch và phương pháp nghiên cứu

B5.1 Mục tiêu

Đề xuất một cấu trúc bảo mật cho hệ thống khóa cửa trong nhà thông minh để tăng cường độ an toàn cho

hệ thống.

B5.2 Nội dung

Liệt kê và mô tả chi tiết nội dung nghiên cứu

Nội dung 1: Tìm hiểu tổng quan

Mục tiêu nội dung 1

- Tìm hiểu tổng quan về các hệ thống khóa trong nhà thông minh, tập trung vào phần bảo mật

Chỉ tiêu đánh giá

- 01 bản báo cáo tổng quan về các hệ thống khóa trong nhà thông minh

Kế hoạch thực hiện

- 01 tháng

Phương pháp

- Nghiên cứu tài liệu

Phân tích và diễn giải số liệu thu được

- Tổng hợp cấu trúc hệ thống khóa thông minh hiện tại, những nơi có nguy cơ bị tấn công

Nội dung 2: Đề xuất cấu trúc hệ thống và qui trình bảo mật mới

Mục tiêu nội dung 2

- Xây dựng cấu trúc và qui trình bảo mật mới để giảm số điểm có nguy cơ tấn công cao trong hệ thống

Chỉ tiêu đánh giá

- 01 bản báo cáo chuyên đề về cấu trúc hệ thống và qui trình bảo mật mới cho hệ thống khóa trong nhà thông minh

Kế hoạch thực hiện

- 04 tháng

Phương pháp

- Tiếp cận theo hướng giảm số lượng kết nối dễ bị tấn công hoặc có tỉ lệ tấn công cao
- Tận dụng phương pháp bảo mật kết hợp Rolling code và RSA cho ổ khóa điện tử

Phân tích và diễn giải số liệu thu được

Nội dung 3: Xây dựng mô hình và mô phỏng khả năng bảo mật

Mục tiêu nội dung 3

- Xây dựng được mô hình hệ thống khóa trong nhà thông minh với một server và một số ổ khóa điện tử và mô phỏng chứng minh khả năng phòng vệ trước các cách tiếp cận của đối tượng xấu.

Chỉ tiêu đánh giá

- Cấu trúc hệ thống như đề xuất
- Hoạt động đúng theo qui trình đề xuất

Kế hoạch thực hiện

- 04 tháng

Phương pháp

- Xây dựng giả lập server, các nút mạng, thiết lập các kết nối và thu nhận dữ liệu

Phân tích và diễn giải số liệu thu được

Nội dung 4: Báo cáo

Mục tiêu nội dung 4

- Hoàn thành các bản báo cáo cần thiết và viết đơn đăng ký Sáng chế/Giải pháp hữu ích.

Chỉ tiêu đánh giá

- Các bản báo cáo: báo cáo giữa kỳ, báo cáo chuyên đề, báo cáo tổng kết đề tài, ...
- 01 hồ sơ đăng ký Sáng chế/Giải pháp hữu ích

Kế hoạch thực hiện

- Hoàn chỉnh các bản báo cáo - 01 tháng

- Hoàn chỉnh hồ sơ đăng ký Sáng chế/Giải pháp hữu ích - 01 tháng

Phương pháp

Phân tích và diễn giải số liệu thu được

B6 Kết quả nghiên cứu

B6.1 Ấn phẩm khoa học

TT	Tên sách/bài báo dự kiến	Số lượng	Dự kiến nơi công bố (tên Tạp chí, Nhà xuất bản)	Ghi chú

B6.2 Đăng ký sở hữu trí tuệ

TT	Hình thức đăng ký	Số lượng	Nội dung dự kiến đăng ký	Ghi chú
1	Giải pháp hữu ích	1	Cơ chế tăng cường bảo mật cho hệ thống cửa tự động trong nhà thông minh	

Mô tả sản phẩm/kết quả nghiên cứu

Dạng I: Các sản phẩm mềm

TT	Tên sản phẩm	Chỉ tiêu đánh giá (định lượng)	Ghi chú
1	Cơ chế tăng cường bảo mật cho hệ thống cửa tự động trong nhà thông minh	01 cấu trúc hệ thống và qui trình bảo mật	

Dạng II: Các sản phẩm cứng

TT	Tên sản phẩm cụ thể và chỉ tiêu chất lượng chủ yếu của sản phẩm	Đơn vị đo	Mức chất lượng			Dự kiến số lượng/quy mô sản phẩm tạo ra
			Chỉ tiêu đánh giá (định lượng)	Mẫu tương tự (theo các tiêu chuẩn mới nhất)		
				Trong nước	Thế giới	

Mức chất lượng các sản phẩm dạng II so với các sản phẩm tương tự trong nước và thế giới

B6.3 Kết quả đào tạo

TT	Cấp đào tạo	Số lượng	Nhiệm vụ được giao trong đề tài	Dự kiến kinh phí (Triệu đồng)
1	Thạc sĩ	1	Đồng chủ nhiệm đề tài	11.5

B7. Khả năng ứng dụng kết quả nghiên cứu

B7.1 Khả năng ứng dụng trong lĩnh vực đào tạo, nghiên cứu khoa học & công nghệ, chính sách, quản lý...

Kết quả nghiên cứu từ đề tài có thể được ứng dụng trong nhiều môn học của chương trình ngành Cơ điện tử hoặc Kỹ thuật máy tính. Qua liên hệ bước đầu với công ty chuyên sản xuất khóa thông minh GLock thì công ty sẵn sàng nhận chuyển giao nếu đề tài đạt được các kết quả khả quan.

B7.2 Khả năng về ứng dụng các kết quả nghiên cứu vào sản xuất kinh doanh, về liên doanh liên kết với các doanh nghiệp, về thị trường

B7.3 Phương thức chuyển giao kết quả nghiên cứu

B8. Tổng hợp kinh phí đề nghị ĐHQG-HCM cấp

Đơn vị tính: triệu đồng

TT	Các khoản chi phí	Đề nghị ĐHQG-HCM cấp		
		Kinh phí	Trong đó khoán chi (*)	%
1	Khoản 1: Trả công lao động	23,00	23,00	100,00%
2	Khoản 2: Nguyên vật liệu, năng lượng	0,00	0,00	0,00%
3	Khoản 3: Thiết bị, máy móc	0,00	0,00	0,00%
4	Khoản 4: Xây dựng, sửa chữa nhỏ	0,00	0,00	0,00%
5	Khoản 5: Chi khác	0,00	0,00	0,00%
	Cộng:	23,00		100%

(*) Theo quy định tại Thông tư số 93/2006/TTLT/BTC-BKHCN của liên Bộ Tài chính - Bộ Khoa học và Công nghệ ban hành ngày 04/10/2006 và Thông tư số 44/2007/TTLT/BTC-BKHCN của liên Bộ Tài chính - Bộ Khoa học và Công nghệ ban hành ngày 07/5/2007.

Ngày ..... tháng ..... năm .....
Chủ tịch hội đồng thẩm định [i]

Ngày 30 tháng 06 năm 2025
Chủ nhiệm **Đồng chủ nhiệm**

TS. Trần Việt Hồng **Trân Bảo Ân**

Ngày ..... tháng ..... năm .....
Cơ quan chủ trì [ii]

Ngày ..... tháng ..... năm .....
Cơ quan chủ quản [iii]