Đại học Quốc gia
Thành phố Hồ Chí Minh

Mẫu R01 - cập nhật TT55

Ngày nhận hồ sơ	
Mã số đề tài	
(Do CQ quản lý ghi)	

THUYẾT MINH
ĐỀ TÀI KHOA HỌC VÀ CÔNG NGHỆ

A. THÔNG TIN CHUNG

A1. Tên đề tài

- Tên tiếng Việt: **Xác thực có bảo vệ tính riêng tư cho các thiết bị với tài nguyên giới hạn trong mạng vạn vật**
- Tên tiếng Anh: **Light-weight Privacy Preserving Authentication for the IoTs**

A2. Thuộc ngành/nhóm ngành (N/NN)

N/NN ưu tiên 1: Công nghệ Thông tin và Truyền thông; Hướng nghiên cứu: Bảo mật

A3. Loại hình nghiên cứu: Nghiên cứu cơ bản

A4. Thời gian thực hiện: 24 tháng (kể từ khi được duyệt).

A5. Tổng kinh phí

- Kinh phí từ nguồn huy động (vốn tự có và vốn khác): 0 triệu đồng, trong đó:
  Vốn tự có: 0 triệu đồng (văn bản chứng minh kèm theo).
  Vốn khác: 0 triệu đồng (văn bản chứng minh kèm theo).

A6. Chủ nhiệm

Học hàm, học vị, họ và tên: **PGS.TS Đặng Trần Khánh**

Điện thoại di động: 0975436383; Email: khanh@hcmut.edu.vn

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

Chủ nhiệm đề tài đã có kinh nghiệm nghiên cứu và đào tạo trong lĩnh vực ứng dụng bảo mật dữ liệu, bảo vệ tính riêng tư, và các hệ thống thông tin hơn 10 năm qua, cả ở môi trường giáo dục và công nghiệp trong và ngoài nước. Về mặt nghiên cứu, những chủ đề nghiên cứu của chủ nhiệm đề tài tập trung vào lĩnh vực bảo mật dữ liệu và các hệ thống thông tin như bảo mật cơ sở dữ liệu, bảo mật và bảo vệ tính riêng tư trong các ứng dụng với thiết bị di động khả định vị, bảo vệ tính riêng tư trong khai phá dữ liệu, bảo mật trong thương mại điện tử, bảo mật cho thiết bị di động thông minh dựa trên sinh trắc học, v.v... Chủ nhiệm đề tài cùng các cộng sự ở trong và ngoài nước đã có hơn 180 bài báo khoa học được đăng trong kỷ yếu của các hội nghị và tạp chí chuyên ngành trên thế giới với nhiều kết quả có liên quan đến lĩnh vực ứng dụng bảo mật dữ liệu, bảo vệ tính riêng tư, và các hệ thống thông tin. Ngoài ra, chủ nhiệm đề tài cũng đã chủ trì và tham gia nhiều đề tài nghiên cứu khoa học và chuyển giao công nghệ có liên quan đến lĩnh vực này ở các cấp và với nhiều đối tác khác nhau. Vào đầu năm 2006, chủ nhiệm đề tài đã thành lập nhóm nghiên cứu ứng dụng về bảo mật dữ liệu (D-STAR Lab: Data SecuriTy Applied Research Lab) và đã xây dựng, phát triển nhóm này thành một nhóm nghiên cứu mạnh trong ĐHQG-HCM cũng như ở Việt Nam. Chủ nhiệm đề tài cũng đã chủ trì thành lập và tổ chức thành công hội nghị quốc tế về "Công nghệ bảo mật và dữ liệu tương lai", có kỷ yếu được xuất bản bởi LNCS/Springer từ 2014 và được đánh chỉ số trong các hệ thống uy tín như CPCI, Scopus, và DBLP (*FDSE: International Conference on Future Data and Security Engineering*). Về đào tạo sau

đại học, chủ nhiệm đề tài đã và đang giảng dạy cũng như hướng dẫn nhiều luận văn thạc sỹ, tiến sỹ cho các học viên và nghiên cứu sinh tại ĐHBK-ĐHQG Tp. HCM và một số đơn vị thành viên của ĐHQG-HCM nghiên cứu về các chủ đề có liên quan đến lĩnh vực ứng dụng bảo mật dữ liệu và bảo vệ tính riêng tư. Chi tiết hơn về các hoạt động nghiên cứu và đào tạo sau đại học có liên quan đến đề tài của chủ nhiệm có thể tham khảo tại trang web cá nhân theo địa chỉ sau đây: http://www.cse.hcmut.edu.vn/~khanh.

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

E-mail: khcn@hcmut.edu.vn

Số tài khoản..Tại kho bạc:

A8. Đối tác có đóng góp cho nghiên cứu

Cơ quan 1: Phòng Thí Nghiệm Tính Toán Nâng Cao (*Cơ quan phối hợp thuộc trường*)

Họ và tên thủ trưởng: PGS.TS Đặng Trần Khánh

Điện thoại: (84-8) 97.543.6383. Fax:

Địa chỉ: 268 Lý Thường Kiệt, Quận 10, TPHCM

Khả năng đóng góp cho đề tài của đối tác: Phòng TN Tính toán Nâng cao (Advanced Computing-AC lab) có cơ sở vật chất hiện đại được đầu tư bởi ĐHQG-HCM, tập trung nhiều chuyên gia về bảo mật và bảo vệ tính riêng tư với kinh nghiệm lâu năm. AC lab cũng đã chủ trì nhiều đề tài nghiên cứu các cấp như cấp trường/sở/ĐHQG với kết quả nghiệm thu tốt và xuất sắc. Các thành viên của AC lab cũng có nhiều công trình nghiên cứu liên quan đến chủ đề nghiên cứu của đề tài như xác thực, bảo vệ tính riêng tư, mạng vạn vật.

A9. Nhân lực nghiên cứu

TT	Học hàm, học vị, Họ tên	Đơn vị công tác	Phân công Chỉ ghi số thứ tự của nội dung được phân công
Danh sách thành viên chủ chốt			
1	PGS. TS. Đặng Trần Khánh	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	2,3,4,5,6,7
2	TS. Trương Tuấn Anh	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	1,2,3,4,5,6,7
3	TS. Phan Trọng Nhân	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	1,2,3,4,5,6,7
4	TS. Lê Hồng Trang	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	1,2,3,4,5,6
5	ThS. Lê Thị Kim Tuyến	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	1,2,3,4,5,6
6	ThS. Đặng Trần Trí	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	1,3,4,5,6
7	ThS. Nguyễn Đình Thành	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	3,4,5,6,7
Danh sách nghiên cứu sinh, học viên cao học, sinh viên			
1	NCS. ThS. Trần Thị Quế Nguyệt	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	1,2,3,4,5,6
2	HVCH. Phạm Đức Minh Châu	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	3,4,5,6
3	HVCH. Trần Thị Kim Khánh	Trường Đại học Bách Khoa - ĐHQG Tp.HCM	3,4,5,6

B. MÔ TẢ NGHIÊN CỨU

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

1. Tổng quan về mạng vạn vật (IoTs)

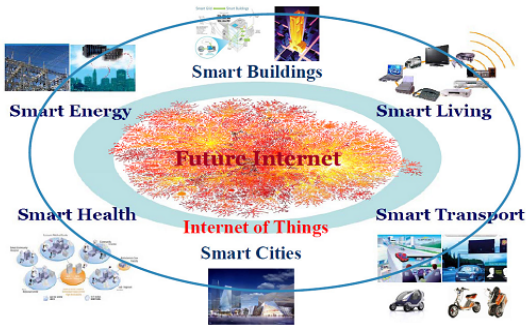
Mạng vạn vật (Internet of Things – IoTs) xuất hiện lần đầu tiên vào năm 2005 nhưng cho đến nay vẫn chưa có một định nghĩa về khái niệm này mà được rộng rãi cộng đồng khoa học chấp nhận. Ta có thể hiểu IoTs là việc kết nối các thiết bị vật lý vào mạng Internet hoặc kết nối giữa các thiết bị này với nhau thông qua các cảm biến, công nghệ dây hoặc không dây, tạo ra một hệ sinh thái tính toán rộng khắp (ubiquitous computing) [7]. "Things" được xét đến trong mạng IoTs có thể là bất kỳ thiết bị nào có thể kết nối vào mạng chứ không chỉ là máy tính hay điện thoại thông minh.

IoTs đang và sẽ trở thành hướng nghiên cứu nổi bật trong và ngoài nước. IoTs hiện được sử dụng trong các hệ thống dành cho ngôi nhà thông minh (smart home), thành phố thông minh (smart city), các hệ thống quản lý nước, môi trường… Tuy nhiên, nhược điểm của các hệ thống IoTs hiện tại là chưa có một chuẩn chung nhất để giao tiếp giữa các thiết bị trong hệ thống. Ngoài ra, vấn đề bảo mật và tính riêng tư cho dữ liệu cũng như các thiết bị trong hệ thống IoTs vẫn chưa được chú trọng [8].

1.1 Đặc tính của IoTs

IoTs có thể được xem là một môi trường mở, kết nối giữa người dùng, thiết bị, dịch vụ và nội dung bằng Internet [1]. Đóng góp quan trọng nhất của IoTs là tăng giá trị thông tin truyền nhận giữa các thiết bị và chuyển đổi thông tin này thành nguồn tri thức có lợi. IoTs cho phép người dùng và thiết bị/dịch vụ kết nối với nhau tại bất kỳ thời gian nào (Anytime), bất cứ đâu (Anyplace), với bất kỳ thiết bị/dịch vụ nào (Anything) và với bất kỳ ai (Anyone), một cách lý tưởng là sử dụng bất kỳ đường kết nối nào (Any path/network) và bất kỳ dịch vụ nào (Any service) [2].

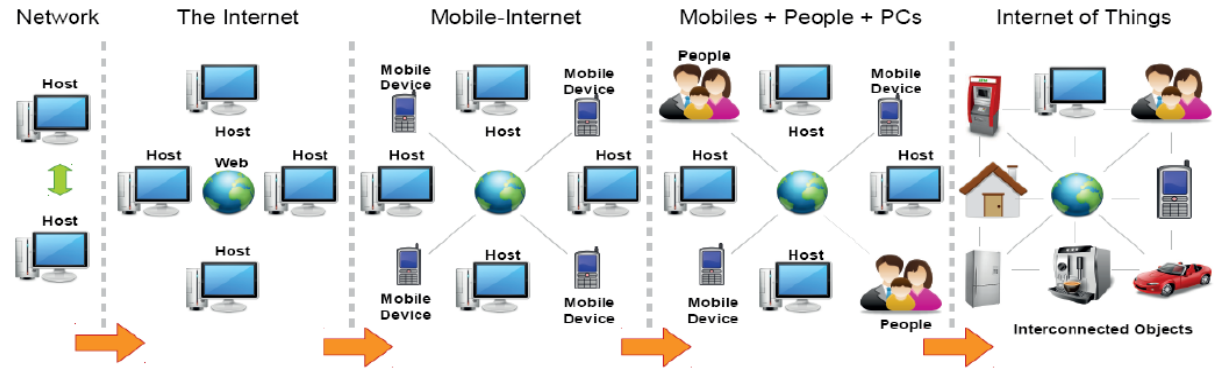
Mục tiêu chính của IoTs là tạo ra một môi trường thông minh trong đó các thiết bị/dịch vụ có khả năng tự vận hành. Ví dụ như giao thông thông minh, thành phố, sản phẩm thông minh, tòa nhà thông minh [5, 6], năng lượng thông minh… cho các ứng dụng trong lĩnh vực thời tiết, cung ứng thức ăn, năng lượng, thiết bị di động, xã hội số, và ứng dụng sức khỏe (Hình 1).



Hình 1. IoTs và việc tạo dựng môi trường thông minh [2]

Để hiểu rõ hơn những đặc trưng của IoTs, ta sẽ đi sơ lược về quá trình phát triển của Internet [3]. Từ những năm cuối của thập niên 1960, kết nối giữa các máy tính được thực hiện thông qua mạng máy tính cục bộ. Đến những năm đầu của thập niên 1980, khái niệm TCP/IP được giới thiệu và sau đó là Internet và World Wide Web (WWW) được chính thức sử dụng vào năm 1991. Tính đến thời điểm này, các máy tính được kết nối với nhau thông qua Internet. Sau đó, các thiết bị di động cũng bắt đầu tham gia vào mạng kết nối này, hình thành nên mạng Mobile-Internet. Ở bước phát triển tiếp theo, người dùng cũng trở thành một thành phần trong mạng với nhu cầu kết nối với nhau qua mạng xã hội, từ đó hình thành kiểu kết nối Mobile + Peoples + PCs. Và sau cùng, ở thời điểm hiện tại, tất cả các đối tượng đều có thể kết nối và trao đổi thông tin lẫn nhau thông qua Internet. Các đối tượng ở đây có thể là người dùng, máy tính, thiết bị di động, hay các thiết bị được sử dụng trong cuộc sống hàng ngày của con người (đồ gia dụng, xe, camera…). Hình 2 tổng hợp lại những những bước phát triển của Internet vừa được đề cập.

IoTs hứa hẹn sẽ là môi trường lý tưởng nơi các đối tượng có thể kết nối Internet và trao đổi thông tin với nhau mà không cần sự can thiệp quá nhiều từ người dùng. Các đối tượng trong mạng có thể biết được nhu cầu cụ thể của người dùng để có những đáp ứng phù hợp mà không cần những hướng dẫn rõ ràng từ phía người dùng.



Hình 2. Sự phát triển của Internet [4]

1.2 Khác biệt của IoTs với các hệ thống IT khác

Không giống như các mạng thông tin khác như enterprise applications, cloud computing hay big data; việc kết hợp một lượng lớn các thiết bị vào trong cùng một mạng khiến IoT có những đặc tính duy nhất, đồng thời cũng là những thách thức cho loại mạng này. Bốn tính chất riêng biệt có thể kể đến là: (1) Môi trường không kiểm soát (uncontrolled environment), (2) tính không đồng nhất (heterogeneity), (3) khả năng đáp ứng (scalability); và (4) ràng buộc tài nguyên (constrained resources) [8]. Ta sẽ lần lượt xem xét từng đặc tính này.

a. Môi trường không kiểm soát (The uncontrolled environment)

Với bản chất là một mạng với rất nhiều loại thiết bị khác biệt tham gia vào, kể cả các thiết bị đáng tin và không đáng tin, IoTs được xem là một môi trường không thể điều khiển. Các đặc tính cụ thể hơn có thể được xét đến là:

- **Mobility**: kết nối mạng ổn định và việc hiện diện liên tục là điều không thể được đảm bảo trong mạng IoT khi mà các thiết bị có khả năng di chuyển với tốc độ và quỹ đạo không xác định trước được.
- **Physical accessibility**: trong mạng IoTs, các thiết bị có thể được truy xuất mà không cần thông qua phân quyền truy cập, ví dụ các camera giao đông hay cảm biến môi trường
- **Trust**: mối quan hệ tin tưởng không thể được thiết lập giữa một lượng lớn các thiết bị có kết nối lẫn nhau và kết nối với người dùng. Do đó, mạng IoTs cần một cơ chế tự động để xác định độ tin tưởng của các thiết bị, dịch vụ và người dùng tham gia vào mạng.

b. Tính không đồng nhất (The heterogeneity)

IoT được xem là một mạng có tính không đồng nhất cao vì sự kết hợp của nhiều thiết bị từ nhiều nhà sản xuất. Do đó, việc phù hợp giữa các phiên bản và giữa các thiết bị với nhau cần phải được xem xét kỹ trong mạng IoTs.

c. Khả năng đáp ứng (scalability)

Với số lượng lớn các thiết bị kết nối lẫn nhau trong mạng, IoTs đòi hỏi các giao thức sử dụng trong mạng phải có khả năng mở rộng cao. Hay nói cách khác, các giao thức bảo mật hiện tại kể cả quản lý tập trung (như Public Key Infrastructures) hay quản lý phân tán (như pairwise symmetric key) đều không đáp ứng được khả năng mở rộng mà mạng IoTs yêu cầu.

d. Ràng buộc tài nguyên (the constrained resources)

Các thiết bị trong mạng IoTs thông thường là bị giới hạn về năng lượng và khả năng tính toán. Do đó các thuật toán phức tạp như tính toán mật mã hóa không thể áp dụng lên các thiết bị này.

2. Vấn đề cần giải quyết

Trong phạm vi của đề tài, chúng tôi nghiên cứu cách thức xác thực có quan tâm đảm bảo tính riêng tư cho các thiết bị bị giới hạn tài nguyên trong mạng IoTs. Cụ thể hơn, đề tài nghiên cứu đi sâu vào làm rõ các vấn đề chính cần giải quyết như sau:

- Nghiên cứu giải pháp xác thực các thiết bị trong mạng IoTs có quan tâm đến tính riêng tư: bởi vì IoTs bao gồm nhiều loại thiết bị với cấu hình khác nhau, nhiều phương thức kết nối với phạm vi khác nhau, cũng như nhiều hướng ứng dụng với những người dùng khác nhau, nên để

bảo mật trong IoTs không chỉ đòi hỏi cần phải bảo mật ở từng công nghệ cụ thể (ví dụ bảo mật trong sensor network hay bảo mật trong RFID) mà còn phải đảm bảo tính an toàn khi có sự giao tiếp hay tương tác giữa các thành phần trong những cơ sở hạ tầng khác nhau. Do đó, mục tiêu của hướng nghiên cứu này là cần xác thực các thông điệp nhận được có phải đến từ các thiết bị hay dịch vụ hợp lệ hay không. Hơn nữa, việc xác thực có thể làm bộc lộ các thông tin nhạy cảm của các thiết bị (được gắn với người sử dụng), do đó, các giải pháp xác thực cũng nên quan tâm đến vấn đề bảo vệ tính riêng tư

- Nghiên cứu giải pháp xác thực dành cho các thiết bị bị giới hạn tài nguyên: các thiết bị trong hệ thống thông thường là các thiết bị di động hoặc các thiết bị nhỏ. Các thiết bị này thường bị giới hạn về tài nguyên như bộ xử lý, bộ nhớ, năng lượng, v....v... Việc áp dụng các phương thức an toàn và bảo mật thông tin truyền thống trên các thiết bị này trở nên không khả thi. Do đó, hướng nghiên cứu này đảm bảo giải pháp xác thực có bảo vệ tính riêng tư có khả năng áp dụng được một cách hiệu quả trên các thiết bị trong mạng IoTs.

3. Các công trình liên quan

Để quản lý sự phức tạp trong bảo mật IoTs, có thể sử dụng sơ đồ phân lớp, trong đó lớp dưới cung cấp những tính năng cần thiết cho lớp bên trên hoạt động. Hình 3 là sơ đồ phần lớp bảo mật cho IoTs đề xuất bởi Jing và các cộng sự [10].

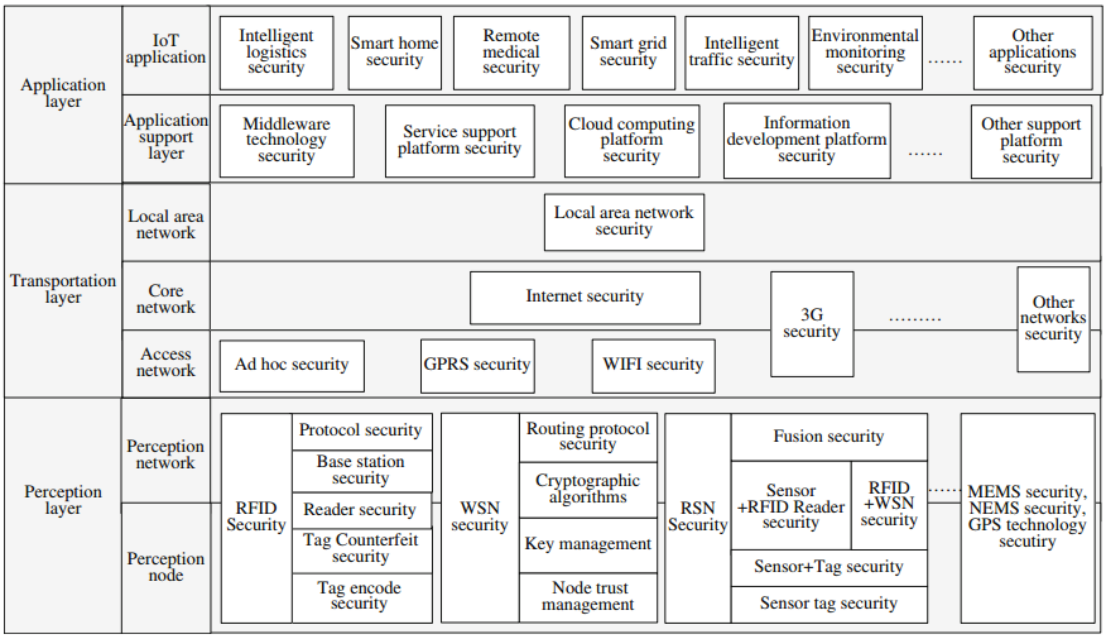
Từ sơ đồ trong Hình 3, có thể nhận ra những vấn đề về xác thực trong IoTs theo cấp độ từ dưới lên bao gồm:

a. Perception layer

- RFID: cần đảm bảo xác thực giữa 2 kênh giao tiếp: giữa RFID tag đến reader, và giữa reader với base station. Phương pháp truyền thống là sử dụng digital signature, nhưng digital signature lại đòi hỏi năng lực tính toán và lưu trữ cao hơn năng lực mà RFID tag có thể cung cấp.
- WSN: symmetric cryptography được sử dụng rộng rãi trong WSN do tính đơn giản và hiệu quả của nó. Nhưng symmetric cryptography lại gặp phải 3 vấn đề: key exchange, đảm bảo tính bí mật của key, và việc áp dụng digital signature không thuận tiện. Do đó, public key cryptography cũng đang được nghiên cứu trong WSN, nhưng public key cryptography lại bị vấn đề về đòi hỏi năng lực tính toán cao, và đặc biệt là tiêu thụ năng lượng trong WSN.
- RSN (RFID sensor network): hệ thống này là sự kết hợp giữa RFID và WSN. Đối với RSN, ngoài các vấn đề về xác thực đã đề cập đối với RFID và WSN, còn có thêm vấn đề về xác thực khi tích hợp 2 hệ thống khác nhau: vì chúng có định dạng khác nhau, yêu cầu bảo mật khác nhau, năng lực xử lý khác nhau, nên cần phải có sự thay đổi cần thiết để 2 thành phần từ 2 công nghệ này có thể giao tiếp (xác thực) lẫn nhau.

b. Transportation layer

c. Application layer



Hình 3. Sơ đồ phân lớp bảo mật trong IoTs

Các lớp Transportation và Application cũng có những vấn đề tương tự về xác thực trong một cơ sở hạ tầng kỹ thuật hoặc xác thực giữa các thành phần từ các cơ sở hạ tầng kỹ thuật khác nhau, nhưng đối với các lớp này khả năng tính toán, lưu trữ và tiết kiệm năng lượng không có yêu cầu quá hạn chế như đối với lớp Perception.

Việc truyền nhận thông điệp giữa các thiết bị trong mạng lưới vạn vật có thể dẫn đến vi phạm tính riêng tư. Tính riêng tư là quyền được pháp luật bảo vệ mà trong đó một cá nhân được quyền giữ bí mật các thông tin riêng tư và nhạy cảm của mình, và không muốn các thông tin cá nhân này bị bộc lộ cho bên thứ ba nào khác. Chính vì vậy, tính riêng tư là tối cần thiết trong các hệ thống thông tin/dịch vụ hiện đại ngày nay. Đôi khi để dịch vụ được cung cấp ở chất lượng cao nhất, người dùng phải cung cấp thông tin chính xác của họ. Tuy nhiên, khi sử dụng các dịch vụ này, người dùng cảm thấy không thoải mái và lo ngại rằng thông tin cá nhân của họ có thể sẽ bị bộc lộ cho bên thứ ba hoặc bị lợi dụng cho những mục đích không tốt đẹp. Ví dụ trong ngữ cảnh xác thực dành cho hệ thống giao thông thông minh, khi một định danh của người dùng X được đính kèm trong thông điệp truyền nhận ở dạng văn bản rõ ràng và có thể đọc được, định danh này có thể được kết hợp với thông tin vị trí của chiếc xe trong hệ thống. Kết quả là thông tin riêng tư của người dùng X bị vi phạm. Hoặc trong ngữ cảnh dịch vụ y tế [11], dữ liệu của bệnh nhân từ một bệnh viện có thể được gửi đến trung tâm phân tích dữ liệu y tế để thực hiện quá trình khai phá dữ liệu nhằm rút trích ra tri thức đằng sau tập dữ liệu này. Như vậy, các thông tin bệnh án nhạy cảm của bệnh nhân có thể sẽ được bộc lộ cho bên thứ ba là trung tâm phân tích dữ liệu y tế, và có khả năng dữ liệu này sẽ được bộc lộ công khai nếu bệnh viện và trung tâm y tế không có các chính sách bảo vệ tính riêng tư cho bệnh nhân. Một bệnh nhân sẽ không hài lòng nếu thông tin bệnh án của mình bị bộc lộ ra cho người khác biết. Thậm chí ngay cả khi định danh của bệnh nhân đã được che giấu, vẫn có khả năng vi phạm tính riêng tư. Ví dụ như ở Hình 4a là dữ liệu y tế của bệnh viện, Hình 4b là dữ liệu bầu cử. Mặc dù dữ liệu y tế của bệnh viện đã che giấu định danh của bệnh nhân, nhưng trung tâm phân tích dữ liệu y tế có thể sử dụng dữ liệu công khai như dữ liệu bầu cử để tái định danh bệnh nhân. Trong trường hợp này, bệnh nhân Doug, là luật sư, 38 tuổi, bị xác định là nhiễm HIV.

(a) Patient table

Job	Sex	Age	Disease
Engineer	Male	35	Hepatitis
Engineer	Male	38	Hepatitis
Lawyer	Male	38	HIV
Writer	Female	30	Flu
Writer	Female	30	HIV
Dancer	Female	30	HIV
Dancer	Female	30	HIV

(b) External table

Name	Job	Sex	Age
Alice	Writer	Female	30
Bob	Engineer	Male	35
Cathy	Writer	Female	30
Doug	Lawyer	Male	38
Emily	Dancer	Female	30
Fred	Engineer	Male	38
Gladys	Dancer	Female	30
Henry	Lawyer	Male	39
Irene	Dancer	Female	32

Hình 4. Ví dụ vi phạm tính riêng tư dữ liệu; (a) Dữ liệu y tế; (b) Dữ liệu bầu cử [11]

Sự e ngại về tính riêng tư trở thành một thách thức cho các hệ thống thông tin hiện đại và góp phần quyết định đến sự tồn tại và phát triển của các dịch vụ được hệ thống cung cấp.

Bên cạnh đó, các cơ chế và giải pháp bảo vệ tính riêng tư cần phải chú trọng đến yếu tố hiệu quả về mặt năng lượng. Thông thường, các thiết bị trong mạng lưới vạn vật có thể là các thiết bị di động, nhỏ, và bị giới hạn về khả năng xử lý cũng như là nguồn năng lượng được cung cấp. Do đó, nếu các phương pháp bảo vệ tính riêng tư đòi hỏi quá trình tính toán phức tạp, khả năng xử lý cao, và tiêu tốn năng lượng nhiều sẽ dẫn đến sự hạn chế khi áp dụng các phương pháp này trong mạng lưới vạn vật.

Trong công trình nghiên cứu [12], Raya and Hubaux đề xuất mạng lưới bảo mật cho phương tiện giao thông thông qua cách xác thực ẩn danh. Cụ thể hơn, các chứng thực (Certificates) được cung cấp bởi thành phần chứng nhận thẩm quyền (Certification Authority-CA) cho từng phương tiện và các phương tiện này sẽ sử dụng các chứng thực được cấp để ký tên lên các thông điệp truyền nhận một cách ẩn danh. Thành phần CA cũng sẽ lưu thông tin về định danh thật của xe, mã số đăng ký, và chứng thực tương ứng. Các chứng thực này có thời gian hợp lệ ngắn và nhanh chóng bị hủy bỏ khi hết thời gian hợp lệ. Mỗi lần một phương tiện yêu cầu một chứng thực mới, phương tiện này phải kết nối đến CA. Tuy nhiên, cách xác thực này yêu cầu CA thực hiện tìm kiếm trong toàn bộ dữ liệu của CA để đối chiếu chứng thực của một định danh được cung cấp. Cách xác thực này gây ra sự hao tốn năng lượng trong quá trình tìm kiếm toàn diện dữ liệu.

Cũng có cùng cách tiếp cận như trên, Liu et at. [13] xây dựng một cơ sở hạ tầng khóa công khai để CA phân phối cặp khóa bí mật-khóa công khai cho người dùng để ký tên lên thông điệp. Tuy nhiên, cách xác thực này gặp phải vấn đề về khả năng mở rộng trong lưu trữ dữ liệu vì các phương tiện phải lưu trữ một số lượng lớn các cặp khóa này. Hơn nữa, cách xác thực này cũng gây ra sự hao tốn năng lượng trong quá trình tìm kiếm toàn diện dữ liệu.

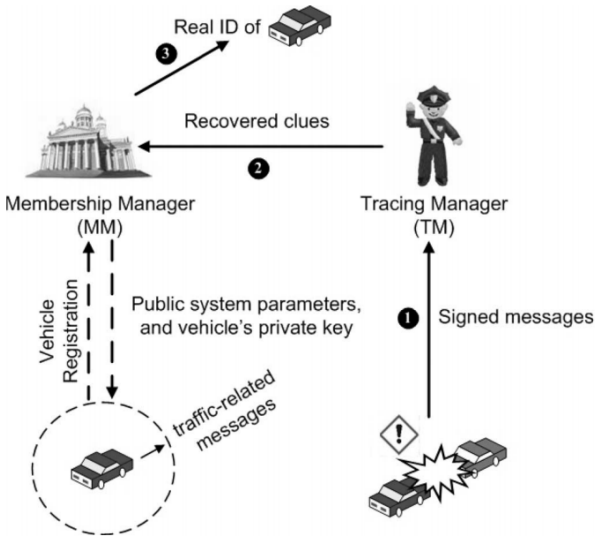
Các tác giả trong công trình nghiên cứu [14, 15, 16] đưa ra cách tiếp cận dựa trên chữ ký nhóm. Sự xác thực của cơ chế chữ ký nhóm cho phép nhiều khóa bí mật kết hợp với một khóa công khai. Bên nhận sẽ có thể xác thực được chữ ký nhóm và liên kết chữ ký này với nhóm phương tiện, nhưng lại không biết chính xác bên gửi là ai. Tuy nhiên, thành phần CA vẫn có thể truy được định danh của người gửi trong cách xác thực này. Để khắc phục vấn đề trên, công trình nghiên cứu [15] đề xuất cơ chế chữ ký nhóm với định danh giả. Tuy nhiên, độ phức tạp tính toán của phương pháp này lại quá cao.

Hình 5 cho thấy mối quan hệ giữa các thực thể trong mạng lưới quản lý các phương tiện giao thông. Trong đó, mỗi phương tiện sẽ phải đăng ký thông tin của mình cho trung tâm quản lý thành viên (MM). Khi lưu thông, các phương tiện này sẽ gửi các thông điệp liên quan đến tình hình giao thông mà phương tiện đang di chuyển. Khi cần có nhu cầu truy vết định danh của một phương tiện (ví dụ xác định phương tiện gây ra tai nạn giao thông), một thông điệp được ký tên sẽ gửi đến cảnh sát TM, sau đó yêu cầu xác định danh tính của phương tiện được gửi đến MM để tìm ra định danh thật của phương tiện gây tai nạn.

Sampigethaya et al. [17] giới thiệu cách thức xác thực cộng tác theo nhóm với độ phức tạp thấp hơn dựa trên kỹ thuật gom cụm. Các nhóm được hình thành sẽ có một trưởng nhóm đại diện trong quá trình giao tiếp với bên ngoài. Tuy nhiên, trưởng nhóm sẽ phải bộc lộ thông tin của mình để bảo vệ thông tin của các thành viên trong nhóm.

Hình 6 minh họa sự truy cập ẩn danh của một phương tiện vehicle i, là thành viên của nhóm Gj, với trưởng nhóm đại diện là GLj. Các thức hoạt động của giao thức truy cập ẩn danh này được mô tả tóm tắt qua 7 bước sau:

- Bước 1: Vehicle i gửi yêu cầu dịch vụ tới trưởng nhóm GLj.
- Bước 2: Trưởng nhóm GLj chuyển tiếp yêu cầu của Vehicle i đến cơ quan đăng ký RA với định danh giả và thông tin vị trí của GLj thông qua RSU.
- Bước 3: RSU chuyển tiếp yêu cầu cho RA.
- Bước 4-7: Cơ quan đăng ký RA xác thực yêu cầu dịch vụ và cung cấp khóa phiên làm việc $k_{x,i}$ cho nhà cung cấp dịch vụ SP_x và vehicle i. Khóa này sẽ được sử dụng để bảo mật kênh truyền giữa vehicle I và nhà cung cấp dịch vụ SP_x.



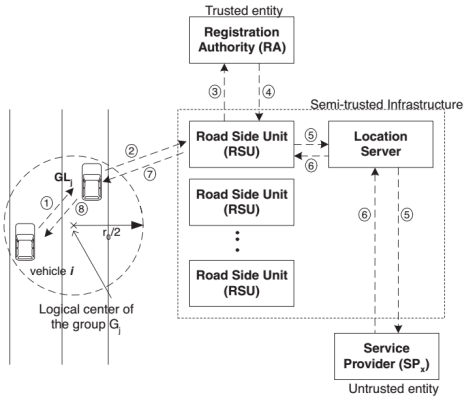
Hình 5. Hệ thống giao tiếp an toàn giữa các phương tiện [14]

Một cách tiếp cận khác đến từ các công trình [9, 18, 19, 20, 21, 22] sử dụng cơ chế xác thực dựa trên định danh giả. Mỗi một phương tiện sẽ được cấp một định danh giả và một khóa bí mật bởi thành phần thứ ba tin cậy (Trusted Authority-TA) để ký tên lên thông điệp truyền nhận. Các thông tin định danh giả này sẽ được chuyển đổi thường xuyên để tránh các tấn công truy vết nhằm xác định ra định danh thật. Do đó, các phương tiện phải thường xuyên liên hệ TA để cập nhật danh sách các định danh giả được cấp.

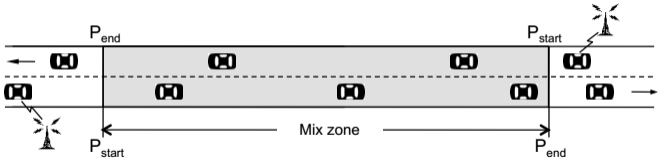
Hình 7 minh họa một ví dụ về vùng pha (Mix zone) bằng cách sử dụng 2 RSU (Road Segment Unit) để cung cấp cùng khóa mã hóa cho phương tiện di chuyển. Khi một phương tiện vào vùng pha, phương tiện này có thể thay đổi định danh của mình, và chọn thời điểm bất kỳ để quay trở lại trạng thái thông thường trước khi ra khỏi vùng pha.

Hình 8 minh họa lược đồ trạng thái biểu diễn quá trình tạo định danh giả với các bước sau:

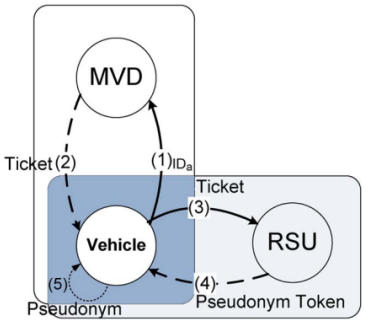
- Bước 1: Phương tiện Va đăng ký thông tin định danh của mình cho bộ phận quản lý MVD (Motor Vehicle Division).
- Bước 2: Bộ phận quản lý MVD cung cấp một thẻ để duy nhất xác định phương tiện Va nhưng không bộc lộ thông tin định danh của Va.
- Bước 3: Khi di chuyển, phương tiện Va sẽ xác thực chính nó với RSU (Road Segment Unit) gần nhất.
- Bước 4: Va nhận token từ RSU để tạo ra định danh giả. Ở bước này, RSU cũng không biết định danh thật của Va.
- Bước 5: Va tự tạo ra định danh giả cho mình.



Hình 6. Phương pháp xác thực cộng tác theo nhóm [17]



Hình 7. Ví dụ về vùng pha [18]



Hình 8. Lược đồ trạng thái biểu diễn quá trình tạo định danh giả [20]

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

*Ý tưởng khoa học:

Ý tưởng khoa học chính của đề tài là nghiên cứu các giải pháp để hỗ trợ việc xác thực các thiết bị tham gia vào hệ thống IoTs. Các giải pháp xác thực được đề nghị trong đề tài phải đáp ứng được những yêu cầu chính: giải pháp phải hỗ trợ xác thực các thông điệp nhận được có phải đến từ các thiết bị/dịch vụ hợp lệ (là các dịch vụ được cấp phép tham gia vào hệ thống) hay không. các giải pháp xác thực này nên quan tâm đến việc bảo vệ các thông tin riêng tư, nhạy cảm của các thiết bị bởi vì các thiết bị tham gia vào hệ thống thường phải gửi các thông tin (ví dụ về định danh, vị trí, ...) của mình cho các thiết bị/dịch vụ khác để phục vụ việc xác thực; Tiếp theo, các giải pháp được đề nghị phải phải tương thích với các thiết bị tham gia vào hệ thống IoTs bởi vì các thiết bị này thường bị giới hạn về tài nguyên như bộ xử lý, bộ nhớ.
Để thực hiện các ý tưởng này, đề tài sẽ tập trung vào các công việc chính sau:

a. Phát triển kiến trúc của mô hình xác thực cho các thiết bị trong IoTs: mô hình này phải tương thích với các hệ thống IoTs hiện có và có tính khả thi trong thực tế.

b. Phát triển các kỹ thuật xác thực hoạt động trên mô hình được đề nghị: các kỹ thuật này phải được thiết kế phù hợp để vừa có thể hoạt động tốt trên mô hình xác thực được đề nghị, vừa có thể hoạt động tốt trên các thiết bị bị giới hạn tài nguyên tham gia vào hệ thống IoTs, vừa quan tâm đến vấn đề bảo vệ tính riêng tư của các thiết bị này.

* Tính cấp thiết:

Ngày nay, các ứng dụng của mạng vạn vật đã thu hút rất nhiều sự chú ý của cả cộng đồng các nhà nghiên cứu và các nhà phát triển sản phẩm. Cùng với sự phát triển ngày càng nhanh của các thiết bị thông minh có khả năng kết nối với nhau, nhiều ứng dụng của mạng vạn vật đã được ứng dụng vào thực tế để hỗ trợ cuộc sống của con người, ví dụ như là hệ thống nhà thông minh đã được sản xuất và áp dụng trong thực tế, hoặc các hệ thống như thành phố thông minh và mạng giao thông thông minh đang được các tổ chức, tập đoàn lớn ưu tiên đầu tư phát triển.

Thông thường, trong các ứng dụng của mạng vạn vật, các thiết bị tham gia vào mạng có khả năng truyền, nhận các thông điệp với nhau. Tuy nhiên, những người tấn công có thể gán ghép các thiết bị của mình vào mạng một cách bất hợp pháp để từ đó lan truyền các thông điệp sai lệch. Do đó, đòi hỏi cấp thiết là phải có một cơ chế xác thực các thiết bị để bảo đảm được rằng các thông điệp truyền nhận đến một thiết bị nào đó phải đến từ một thiết bị hợp lệ trong mạng. Hơn nữa, việc xác thực cũng có nhiều khả năng làm lộ các thông tin riêng tư của người sử dụng. Do đó, việc xác thực phải đồng thời đi kèm với các giải pháp bảo vệ tính riêng tư. Đề tài này sẽ tập trung nghiên cứu các giải pháp vừa hỗ trợ việc xác thực các thiết bị tham gia vào mạng, vừa bảo vệ các thông tin riêng tư của người sử dụng trong quá trình xác thực. Hơn nữa, các giải pháp được đề nghị trong đề tài phải tương thích với các thiết bị đặc thù của mạng IoTs, đó là các thiết bị bị giới hạn bởi các nguồn tài nguyên như bộ xử lý, bộ nhớ, ...

* Tính mới:

Như đã phân tích trong phần các công trình nghiên cứu liên quan, các giải pháp hiện tại vẫn còn tồn tại rất nhiều điểm hạn chế như các giải pháp hiện tại chưa thực sự hiệu quả trong mạng IoTs với các thiết bị giới

hạn tài nguyên cũng như, tính riêng tư chưa được quan tâm. Chính vì vậy, đề tài này sẽ nghiên cứu một framework thống nhất cho việc xác thực các thiết bị tham gia vào mạng đồng thời đề nghị các giải pháp đề vừa để vừa hỗ trợ việc xác thực các thiết bị, vừa quan tâm đến việc bảo vệ các thông tin riêng tư của người sử dụng. Hơn nữa, các giải pháp trong đề tài này cũng phải tương tích với các thiết bị đặc thù của mạng IoTs như các sensor với nguồn tài nguyên bị hạn chế (đây cũng là một điểm mới của các giải pháp trong đề tài so với các giải pháp trước đây).

B3. Kết quả nghiên cứu sơ khởi (nếu có)

Trong đề tài nghiên cứu khoa học cấp ĐHQG-HCM trọng điểm 2012 [22], nhóm các tác giả đã nghiên cứu về bài toán bảo vệ tính riêng tư trong các ứng dụng với thiết bị di động khả định vị. Kết quả của đề tài là phương pháp bảo vệ tính riêng tư cho các thiết bị di động khả định vị thông qua một thành phần trung gian (middleware) hoặc giải pháp bảo vệ tính riêng tư được tích hợp vào cơ sở dữ liệu. Bên cạnh đó, kết quả của đề tài còn đưa ra một framework chẳng những hỗ trợ bảo vệ tính riêng tư cho người sử dụng mà còn hỗ trợ cho sự phát triển của các dịch vụ dựa trên vị trí. Ngoài ra, framework được đề nghị có thể hỗ trợ các kỹ thuật bảo vệ tính riêng tư cũng như vấn đề nhận thức ngữ cảnh.

B4. Tài liệu tham khảo

[1] Park, A. J., Kim, H. Y., & Lim, J. I. (2015). A Framework of Device Authentication Management in IoT Environments. In IT Convergence and Security (ICITCS), pages 1-3, IEEE.

[2] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, pages 9-52.

[3] Kumar, J. S., & Patel, D. R. (2014). A survey on Internet of Things: security and privacy issues. International Journal of Computer Applications, 90(11).

[4] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the internet of things: A survey. Communications Surveys & Tutorials, 16(1), pages 414-454, IEEE.

[5] Lumi Smarthome (2016) http://www.lumi.vn/tin-tuc/chi-tiet/internet-of-things-va-nhung-ung-dung-giai-phap-nha-thong-minh

[6] Bkav Smarthome (2016) http://www.smarthome.com.vn/

[7] Staff, F. T. C. (2015). Internet of Things: Privacy and Security in a Connected World. Technical report, Federal Trade Commission.

[8] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015). On the Security and Privacy of Internet of Things Architectures and Systems. In 2015 International Workshop on Secure Internet of Things (SIoT), pages 49-57, IEEE.

[9] Sucasas, V., Mantas, G., Saghezchi, F. B., Radwan, A., & Rodriguez, J. (2016). An autonomous privacy-preserving authentication scheme for intelligent transportation systems. Computers & Security, pages 193-205.

[10] Jing, Qi, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. (2014). "Security of the Internet of Things: perspectives and challenges." *Wireless Networks* 20, no. 8, pages 2481-2501.

[11] Fung, B. C. M., Wang, K., Chen, R., & Yu, P. S. (2010). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys*, *42*(4), DOI: 10.1145/1749603.1749605

[12] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. (2005). In *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '05, pages 11–21, New York, NY, USA, ACM.

[13] Xiaonan Liu, Zhiyi Fang, and Lijun Shi. Securing vehicular ad hoc networks. (2007). In *Pervasive Computing and Applications, 2007. ICPCA 2007*, pages 424–429.

[14] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. Gsis. (2007). A secure and privacy-preserving protocol for vehicular communications. *Vehicular Technology, IEEE Transactions on*, 56(6): pages 3442–3456.

[15] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. (2008). Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.

[16] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. Efficient and robust pseudonymous authentication in vanet. In *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '07, pages 19–28, New York, NY, USA, 2007. ACM.

[17] K. Sampigethaya, Mingyan Li, Leping Huang, and R. Poovendran. Amoeba: Robust location privacy scheme for vanet. *Selected Areas in Communications, IEEE Journal on*, 25(8):1569–1589, Oct 2007.

[18] Zhendong Ma, F. Kargl, and M. Weber. Pseudonym-on-demand: A new pseudonym refill strategy for vehicular communications. In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pages 1–5, Sept 2008.

[19] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien. Abaka: An anonymous batch authenticated and key agreement scheme for valueadded services in vehicular ad hoc networks. *Vehicular Technology, IEEE Transactions on*, 60(1):248–262, Jan 2011.

[20] Dijiang Huang, S. Misra, M. Verma, and Guoliang Xue. Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets. *Intelligent Transportation Systems, IEEE Transactions on*, 12(3):736–746, Sept 2011.

[21] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin Shen, and Jinshu Su. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *Vehicular Technology, IEEE Transactions on*, 59(7):3589–3603, Sept 2010.

[22] Đặng Trần Khánh (chủ nhiệm) et. al. *Bảo vệ tính riêng tư trong các ứng dụng với thiết bị di động khả định vị*. Đề tài nghiên cứu khoa học cấp ĐHQG-HCM trọng điểm, 2012.

B5. Mục tiêu, nội dung, kế hoạch nghiên cứu

B5.1 Mục tiêu

Đề tài tập trung nghiên cứu các vấn đề liên quan đến việc xác thực các thiết bị tham gia vào mạng IoTs. Từ đó, đề tài sẽ đề xuất các giải pháp để hỗ trợ việc xác thực các thiết bị tham gia vào hệ thống IoTs. Các giải pháp xác thực được đề nghị trong đề tài phải vừa hỗ trợ việc xác thực các thông điệp nhận được có phải đến từ các thiết bị/dịch vụ hợp lệ hay không vừa phải quan tâm việc bảo vệ các thông tin riêng tư, nhạy cảm của các thiết bị. Thêm nữa, đặc điểm của các thiết bị này như bị giới hạn về tài nguyên phải cần được xem xét trong quá trình thiết kế các giải pháp. Các mục tiêu chính của đề tài là:

a. Phát triển kiến trúc của mô hình xác thực cho các thiết bị trong IoTs: mô hình này phải phù hợp với các hệ thống IoTs hiện có.

b. Phát triển các kỹ thuật xác thực hoạt động trên mô hình được đề nghị: các kỹ thuật này phải được thiết kế phù hợp để vừa có thể hoạt động tốt trên mô hình xác thực được đề nghị, vừa có thể hoạt động tốt trên các thiết bị bị giới hạn tài nguyên tham gia vào hệ thống IoTs. Các kỹ thuật này cũng nên quan tâm đến vấn đề tính riêng tư của thiết bị trong quá trình xác thực.

Đề tài thành công sẽ cung cấp một framework thống nhất, hiệu quả để hỗ trợ việc xác thực các thiết bị và có quan tâm đến việc bảo vệ tính riêng tư của người sử dụng (thông quan các thông tin của các thiết bị cần được xác thực) khi tham gia vào mạng để họ có thể yên tâm khi sử dụng vào các ứng dụng của mạng vạn vật. Ngoài ra, thông qua việc thực hiện đề tài, một nhóm nghiên cứu mạnh về các xác thực trong mạng vạn vật cũng sẽ được hình thành và phát triển tại Đại học Quốc gia TPHCM nói riêng và Việt Nam nói chung. Góp phần vào thúc đẩy việc nghiên cứu và phổ biến về về lĩnh vực này cũng như mối liên kết với các nhóm nghiên cứu khác trên thế giới.

B5.2 Nội dung và phương pháp nghiên cứu

Nội dung 1: Nghiên cứu tổng quan về mạng vạn vật.

Mục tiêu nội dung 1: Tìm hiểu tổng quan về cấu trúc của mạng vạn vật nói chung: kiến trúc, các công nghệ, mô hình có thể áp dụng vào mạng vạn vật.

Sản phẩm khoa học dự kiến và chỉ tiêu đánh giá:

• Quyển báo cáo tổng quan về các khái niệm, định nghĩa, cấu trúc của mạng vạn vật: Báo cáo trình bày rõ ràng các khái niệm chính về mạng vạn vật nói chung và kiến trúc của nó.

Kế hoạch thực hiện:

Công việc	Nội dung thực hiện	Người thực hiện	Từ ... đến ...(tháng)
1.1	Nghiên cứu tổng quan về mạng vạn vật.	*Trương Tuấn Anh *Lê Thị Kim Tuyến *Trần Thị Quế Nguyệt *Phan Trọng Nhân *Lê Hồng Trang *Đặng Trần Trí	1-2

Phương pháp:

• Thu thập tài liệu tham khảo qua nhiều nguồn khác nhau như Internet, sách tham khảo, ...

• Tìm hiểu các khái niệm và kiến trúc của mạng vạn vật từ các tài liệu tham khảo.

• Viết báo cáo các khái niệm và kiến trúc cơ bản về mạng vạn vật (một chương trong báo cáo tổng kết đề tài).

Phân tích và diễn giải số liệu thu được:

• Báo cáo các khái niệm và kiến trúc tổng quan của mạng vạn vật.

Nội dung 2: Xác thực trong các hệ thống thông tin và ứng dụng.

Mục tiêu nội dung 2: Tìm hiểu các yêu cầu, các mô hình cho bài toán xác thực và bảo vệ tính riêng tư từ các công trình nghiên cứu liên quan và các giải pháp đã được đề nghị có thể có. Phân tích và đánh giá các giải pháp đã được đề nghị.

Sản phẩm khoa học dự kiến và chỉ tiêu đánh giá:

• Quyển báo cáo nội dung 2: Báo cáo khảo sát, tổng hợp các kỹ thuật và giải pháp liên quan đến việc xác thực trong các hệ thống thông tin và ứng dụng.

Kế hoạch thực hiện:

Công việc	Nội dung thực hiện	Người thực hiện	Từ ... đến ...(tháng)
2.1	Nghiên cứu, tìm hiểu bài toán xác thực trong các hệ thống thông tin và ứng dụng.	*Trương Tuấn Anh *Đặng Trần Khánh *Lê Thị Kim Tuyến *Trần Thị Quế Nguyệt *Phan Trọng Nhân *Lê Hồng Trang	2-4

Phương pháp:

• Thu thập tài liệu tham khảo qua nhiều nguồn khác nhau như Internet, sách tham khảo, ...

• Phân tích các hướng tiếp cận chính trong về xác thực trong các hệ thống thông tin và ứng dụng.

• Viết báo cáo chuyên đề cho nội dung 2.

Phân tích và diễn giải số liệu thu được:

• Quyển báo cáo các phương pháp và kỹ thuật xác thực trong các hệ thống thông tin.

Nội dung 3: Nghiên cứu về xác thực trong mạng vạn vật với các thiết bị có tài nguyên giới hạn.

Mục tiêu nội dung 3: Nghiên cứu, tìm hiểu về bài toán xác thực trong mạng vạn vật cũng như các ràng buộc về tài nguyên đối với các thiết bị trong mạng vạn vật.

Sản phẩm khoa học dự kiến và chỉ tiêu đánh giá:

• Quyển báo cáo nội dung 3: Báo cáo về bài toán cũng như các yêu cầu xác thực trong mạng vạn vật với các thiết bị bị ràng buộc về tài nguyên.

Kế hoạch thực hiện:

Công việc	Nội dung thực hiện	Người thực hiện	Từ ... đến ...(tháng)
3.1	Bài toán xác thực trong mạng vạn vật.	*Lê Hồng Trang *Đặng Trần Khánh *Phan Trọng Nhân *Lê Thị Kim Tuyến *Trần Thị Quế Nguyệt	4-6
3.2	Các ràng buộc về tài nguyên trong xác thực với mạng vạn vật	*Trương Tuấn Anh *Lê Thị Kim Tuyến *Phạm Đức Minh Châu *Trần Thị Kim Khánh *Nguyễn Đình Thành *Đặng Trần Trí	5-7

Phương pháp:

• Thu thập các công trình nghiên cứu về xác thực thiết bị trong mạng vạn vật cũng như các ứng dụng của nó.

• Tìm hiểu, nghiên cứu về bài toán xác thực cũng như các ràng buộc về tài nguyên trong mạng vạn vật.

• Viết báo cáo chuyên đề.

Phân tích và diễn giải số liệu thu được:

• Quyển báo cáo về bài toán xác thực cũng như các ràng buộc về tài nguyên trong mạng vạn vật.

Nội dung 4: Nghiên cứu đề xuất mô hình xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến tính riêng tư trong mạng vạn vật.

Mục tiêu nội dung 4: Đè xuất, thiết kế một mô hình phù hợp với nền tảng IoTs để hỗ trợ việc xác thực các thiết bị bị giới hạn tài nguyên và có quan tâm đến tính riêng tư.

Sản phẩm khoa học dự kiến và chỉ tiêu đánh giá:

• Quyển báo cáo nội dung 4: Báo cáo trình bày về mô hình xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến tính riêng tư trong mạng vạn vật.

Kế hoạch thực hiện:

Công việc	Nội dung thực hiện	Người thực hiện	Từ ... đến ...(tháng)

4.1	Đề xuất mô hình xác thực các thiết bị trong mạng vạn vật.	*Trương Tuấn Anh *Lê Hồng Trang *Lê Thị Kim Tuyến *Trần Thị Quế Nguyệt *Phan Trọng Nhân *Đặng Trần Khánh *Nguyễn Đình Thành	7-10
4.2	Bài toán xác thực với tài nguyên giới hạn.	*Trương Tuấn Anh *Lê Hồng Trang *Nguyễn Đình Thành *Lê Thị Kim Tuyến *Trần Thị Kim Khánh	9-10
4.3	Bài toán xác thực có quan tâm đến bảo vệ tính riêng tư.	*Đặng Trần Khánh *Phan Trọng Nhân *Trần Thị Quế Nguyệt *Đặng Trần Trí *Phạm Đức Minh Châu	10-11

Phương pháp:

• Nghiên cứu, tìm hiểu sâu vào từng kiến trúc mô hình xác thực, phân tích các điểm mạnh, điểm yếu của nó và lựa chọn/đề xuất giải pháp phù hợp.

Phân tích và diễn giải số liệu thu được:

• Quyển báo cáo chuyên đề mô tả chi tiết mô hình xác thực đề nghị.

Nội dung 5: Nghiên cứu đề xuất các kỹ thuật xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến tính riêng tư.

Mục tiêu nội dung 5: Nghiên cứu đề xuất các kỹ thuật xác thực các thiết bị với tài nguyên giới hạn và có quan tâm đến việc bảo vệ tính riêng tư. Các kỹ thuật được đề nghị trong mục này sẽ hoạt động trên mô hình được đề nghị trong nội dung 4.

Sản phẩm khoa học dự kiến và chỉ tiêu đánh giá:

• Quyển báo cáo nội dung 5: mô tả chi tiết các kỹ thuật cũng như các thử nghiệm đánh giá.

Kế hoạch thực hiện:

Công việc	Nội dung thực hiện	Người thực hiện	Từ ... đến ...(tháng)
5.1	Nghiên cứu đề xuất các kỹ thuật xác thực các thiết bị với tài nguyên giới hạn và có quan tâm đến việc bảo vệ tính riêng tư.	*Đặng Trần Khánh *Trương Tuấn Anh *Phan Trọng Nhân *Lê Hồng Trang *Lê Thị Kim Tuyến *Đặng Trần Trí	12-16
5.2	Đánh giá các kỹ thuật đã được đề xuất.	*Trần Thị Quế Nguyệt *Trần Thị Kim Khánh *Phạm Đức Minh Châu *Nguyễn Đình Thành	15-18

Phương pháp:

• Tìm hiểu các kỹ thuật xác thực đã được đề nghị và chọn hướng tiếp cận thích hợp, phù hợp với mạng

vạn vật.
• Đề xuất, thiết kế, hiện thực các kỹ thuật xác thực các thiết bị với tài nguyên giới hạn và có quan tâm đến việc bảo vệ tính riêng tư.
• Đánh giá các kỹ thuật được đề nghị.
Phân tích và diễn giải số liệu thu được:
• • Quyển báo cáo các kỹ thuật xác thực các thiết bị với tài nguyên giới hạn và có quan tâm đến việc bảo vệ tính riêng tư đề nghị.

Nội dung 6: Tích hợp và hiện thực giải pháp xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến tính riêng tư.

Mục tiêu nội dung 6: Xây dựng được một khung sườn thống nhất cho bài toán xác thực các thiết bị với tài nguyên giới hạn và có quan tâm đến tính riêng tư.

Sản phẩm khoa học dự kiến và chỉ tiêu đánh giá:

• Báo cáo chi tiết framework thống nhất giải quyết bài toán xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến bảo vệ tính riêng tư.

Kế hoạch thực hiện:

Công việc	Nội dung thực hiện	Người thực hiện	Từ ... đến ...(tháng)
6.1	Đề xuất một khung sườn framework thống nhất cho bài toán xác thực các thiết bị với tài nguyên giới hạn và có quan tâm đến tính riêng tư.	*Đặng Trần Khánh *Trương Tuấn Anh *Phan Trọng Nhân *Lê Hồng Trang *Lê Thị Kim Tuyến *Đặng Trần Trí	18 – 20
6.2	Hiện thực khung sườn được đề xuất	*Phan Trọng Nhân *Lê Thị Kim Tuyến *Trần Thị Quế Nguyệt *Trần Thị Kim Khánh *Phạm Đức Minh Châu *Nguyễn Đình Thành	19 – 23

Phương pháp:
• Thiết kế kiến trúc framework thống nhất như được thảo luận ở nội dung 4 với các kỹ thuật xác thực các thiết bị với tài nguyên giới hạn và có quan tâm đến tính riêng tư được đề nghị trong nội dung 5.
• Hiện thực framework được đề xuất.
Phân tích và diễn giải số liệu thu được:
• Báo cáo chi tiết về framework giải quyết bài toán xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến bảo vệ tính riêng tư được đề nghị.

Nội dung 7: Viết báo cáo tổng kết

Mục tiêu nội dung 7: Hoàn thành báo cáo nghiệm thu cho đề tài.
Sản phẩm khoa học dự kiến và chỉ tiêu đánh giá:

• Báo cáo nghiệm thu.

Kế hoạch thực hiện:

Công việc	Nội dung thực hiện	Người thực hiện	Từ ... đến ...(tháng)

7.1	Báo cáo nghiệm thu	*Đặng Trần Khánh *Trương Tuấn Anh *Phan Trọng Nhân *Nguyễn Đình Thành	24

Phương pháp:
• Viết báo cáo theo các định dạng có sẵn của ĐHQG.
• Tiến hành theo quy trình cho các thủ tục hành chính và thanh quyết toán.
• Báo cáo nghiệm thu trước hội đồng.
Phân tích và diễn giải số liệu thu được:
• Các tài liệu báo cáo nghiệm thu theo biểu mẫu.
• Các hóa đơn, chứng từ.

B5.3 Tóm tắt công việc và phân công

Nội dung	Kết quả khoa học cần đạt và tiêu chí đánh giá	Nguồn nhân lực
Nội dung 1	• Quyển báo cáo tổng quan về các khái niệm, định nghĩa, cấu trúc của mạng vạn vật: Báo cáo trình bày rõ ràng các khái niệm chính về mạng vạn vật nói chung và kiến trúc của nó.	Chủ trì: **Trương Tuấn Anh**: 10 ngày Tham gia: ***Phan Trọng Nhân**: 10 ngày ***Lê Thị Kim Tuyến**: 9 ngày ***Trần Thị Quế Nguyệt**: 10 ngày ***Lê Hồng Trang**: 5 ngày ***Đặng Trần Trí**: 10 ngày
Nội dung 2	• Quyển báo cáo nội dung 2: Báo cáo khảo sát, tổng hợp các kỹ thuật và giải pháp liên quan đến việc xác thực trong các hệ thống thông tin và ứng dụng.	Chủ trì: **Đặng Trần Khánh**: 7 ngày Tham gia: ***Trương Tuấn Anh**: 12 ngày ***Phan Trọng Nhân**: 12 ngày ***Lê Thị Kim Tuyến**: 12 ngày ***Trần Thị Quế Nguyệt**: 12 ngày ***Lê Hồng Trang**: 7 ngày
Nội dung 3	• Quyển báo cáo nội dung 3: Báo cáo về bài toán cũng như các yêu cầu xác thực trong mạng vạn vật với các thiết bị bị ràng buộc về tài nguyên.	Chủ trì: **Phan Trọng Nhân**: 12 ngày Tham gia: ***Trương Tuấn Anh**: 11 ngày ***Đặng Trần Khánh**: 7 ngày ***Lê Thị Kim Tuyến**: 23 ngày ***Đặng Trần Trí**: 5 ngày ***Trần Thị Quế Nguyệt**: 12 ngày ***Phạm Đức Minh Châu**: 11 ngày ***Trần Thị Kim Khánh**: 11 ngày ***Nguyễn Đình Thành**: 11 ngày ***Lê Hồng Trang**: 12 ngày

Nội dung 4	• Quyển báo cáo nội dung 4: Báo cáo trình bày về mô hình xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến tính riêng tư trong mạng vạn vật.	Chủ trì: **Trương Tuấn Anh**: 26 ngày Tham gia: ***Phan Trọng Nhân**: 26 ngày ***Đặng Trần Khánh**: 10 ngày ***Lê Thị Kim Tuyến**: 26 ngày ***Lê Hồng Trang**: 14 ngày ***Trần Thị Quế Nguyệt**: 26 ngày ***Đặng Trần Trí**: 7 ngày ***Phạm Đức Minh Châu**: 11 ngày ***Trần Thị Kim Khánh**: 11 ngày ***Nguyễn Đình Thành**: 26 ngày
Nội dung 5	• Quyển báo cáo nội dung 5: mô tả chi tiết các kỹ thuật cũng như các thử nghiệm đánh giá.	Chủ trì: **Đặng Trần Khánh**: 5 ngày Tham gia: ***Trương Tuấn Anh**: 17 ngày ***Phan Trọng Nhân**: 17 ngày ***Lê Hồng Trang**: 7 ngày ***Lê Thị Kim Tuyến**: 17 ngày ***Đặng Trần Trí**: 17 ngày ***Trần Thị Quế Nguyệt**: 17 ngày ***Nguyễn Đình Thành**: 17 ngày ***Phạm Đức Minh Châu**: 17 ngày ***Trần Thị Kim Khánh**: 17 ngày
Nội dung 6	• Báo cáo chi tiết framework thống nhất giải quyết bài toán xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến bảo vệ tính riêng tư.	Chủ trì: **Lê Hồng Trang**: 7 ngày Tham gia: ***Trương Tuấn Anh**: 12 ngày ***Đặng Trần Khánh**: 5 ngày ***Lê Thị Kim Tuyến**: 17 ngày ***Phan Trọng Nhân**: 24 ngày ***Đặng Trần Trí**: 12 ngày ***Trần Thị Quế Nguyệt**: 12 ngày ***Nguyễn Đình Thành**: 12 ngày ***Phạm Đức Minh Châu**: 12 ngày ***Trần Thị Kim Khánh**: 12 ngày
Nội dung 7	• Báo cáo nghiệm thu.	Chủ trì: **Đặng Trần Khánh**: 5 ngày Tham gia: ***Trương Tuấn Anh**: 10 ngày

		***Phan Trọng Nhân**: 10 ngày ***Nguyễn Đình Thành**: 10 ngày

B5.4 Tính khả thi

a. **Về nguyên vật liệu, năng lượng**

b. **Về trang thiết bị**

c. **Về lực lượng nghiên cứu**

d. **Mô tả nội dung, nhân sự của các chuyến đi trong quá trình triển khai nghiên cứu để có cơ sở đánh giá công tác phí trong và ngoài nước**

Nhóm nghiên cứu sẽ nộp và tham gia 2 hội thảo khoa học quốc tế. Do đó, sẽ có hai nhân sự tham gia vào 2 chuyến đi này (mỗi chuyến đi một nhân sự). Công tác phí sẽ bao gồm phí hội nghị và các phí ăn ở, đi lại, visa, v.v...

B6. Kết quả nghiên cứu

B6.1 Mô tả sản phẩm/kết quả nghiên cứu (bắt buộc)

Dạng I: Các sản phẩm mềm

TT	Tên sản phẩm	Chỉ tiêu đánh giá *(định lượng)*	Ghi chú
1	Thuyết minh đề tài	Quyển thuyết minh đề tài nghiên cứu.	
2	Báo cáo nội dung 1	Quyển báo cáo chuyên đề tổng quan về các khái niệm, định nghĩa, cấu trúc của mạng vạn vật và các ứng dụng cụ thể, phổ biến của nó.	
3	Báo cáo nội dung 2	Quyển báo cáo chi tiết về về bài toán xác thực và các yêu cầu của nó trong các hệ thống thông tin và ứng dụng nói chung. Báo cáo cũng khảo sát, tổng hợp các kỹ thuật và giải pháp liên quan đến việc xác thực trong các hệ thống thông tin và ứng dụng. Báo cáo cũng nêu rõ các đặc điểm của các kỹ thuật/giải pháp này.	
4	Báo cáo nội dung 3	Quyển báo cáo về bài toán cũng như các yêu cầu xác thực trong mạng vạn vật với các thiết bị bị ràng buộc về tài nguyên.	
5	Tập dữ liệu thu thập được	Tập dữ liệu/case study này dự kiến sẽ phục vụ cho việc kiểm thử các kỹ thuật xác thực có quan tâm đến việc bảo vệ tính riêng tư được đề nghị sau này.	
6	Báo cáo nội dung 4	Quyển báo cáo trình bày về mô hình xác thực các thiết bị với tài nguyên giới hạn có quan tâm đến tính riêng tư trong mạng vạn vật.	
7	Báo cáo nội dung 5	Quyển báo cáo mô tả chi tiết các kỹ thuật cũng như các thử nghiệm đánh giá.	
8	Báo cáo nội dung 6	Quyển báo cáo chi tiết framework thống nhất giải quyết bài toán xác thực các thiết bị với tài	

		nguyên giới hạn có quan tâm đến bảo vệ tính riêng tư.	
9	Ấn phẩm khoa học	1 Bài báo khoa học đăng trên kỷ yếu hội nghị được xuất bản bởi các nhà xuất bản có uy tín.	
10	Ấn phẩm khoa học	1 Bài báo khoa học đăng trên kỷ yếu hội nghị được xuất bản bởi các nhà xuất bản có uy tín.	
11	Ấn phẩm khoa học	1 Bài báo khoa học nộp vào tạp chí quốc tế uy tín (thuộc ISI).	
12	Ấn phẩm khoa học	1 Bài báo khoa học nộp vào tạp chí quốc tế uy tín (thuộc ISI).	
13	Báo cáo nghiệm thu	Báo cáo tổng kết đề tài.	

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

B6.2 Ấn phẩm khoa học

TT	Ấn phẩm dự kiến	Số lượng	Dự kiến nơi công bố *(Nhà xuất bản, tạp chí, hội nghị)*
1.	**Sách**		
1.1	Chuyên khảo tiếng nước ngoài		
1.2	Chuyên khảo tiếng Việt		
2.	**Bài báo đăng tạp chí uy tín**	**2**	
2.1	Tạp chí quốc tế*	**2**	Trong đó: 02 bài ISI thuộc SCI-E/SSCI/SCI.
2.2	Tạp chí trong nước *(thuộc danh mục tính điểm của các hội đồng học hàm)*		*Kết quả của nội dung …*
3.	**Bài báo đăng hội nghị có phản biện**	**2**	
3.1	Hội nghị quốc tế	**2**	Các hội nghị chất lượng được xuất bản bởi các nhà xuất bản có uy tín như Springer, ACM, IEEE,....
3.2	Hội nghị trong nước		*Tên hội nghị:….*

B6.3 Sở hữu trí tuệ

TT	Hình thức đăng ký	Số lượng	Nội dung dự kiến đăng ký

B6.4 Đóng góp cho đào tạo

Bậc đào tạo	Số lượng	Nêu rõ hoàn tất hay tham gia đào tạo tiến sỹ, công việc NCS, HVCH hay SV được giao trong đề tài	Tiền công của NCS, HVCH, SV *(triệu đồng)*
Tiến sỹ	2	Báo cáo xong chuyên đề nghiên cứu sinh hoặc tham gia viết 1 bài báo	
Thạc sỹ	2	Hoàn tất (bảo vệ xong Luận văn trong thời gian thực hiện đề tài)	

B7. Những đóng góp của nghiên cứu

B7.1 Đóng góp mới về tri thức; mức độ giải quyết vấn đề nghiên cứu đặt ra

Ngày nay, các ứng dụng của mạng vạn vật đã thu hút rất nhiều sự chú ý của cả cộng đồng các nhà nghiên cứu và các nhà phát triển sản phẩm. Cùng với sự phát triển ngày càng nhanh của các thiết bị thông minh có khả năng kết nối với nhau, nhiều ứng dụng của mạng vạn vật đã được ứng dụng vào thực tế để hỗ trợ cuộc sống của con người, ví dụ như là hệ thống nhà thông minh đã được sản xuất và áp dụng trong thực tế, hoặc các hệ thống như thành phố thông minh và mạng giao thông thông minh đang được các tổ chức, tập đoàn lớn ưu tiên đầu tư phát triển.

Thông thường, trong các ứng dụng của mạng vạn vật, các thiết bị tham gia vào mạng có khả năng truyền, nhận các thông điệp với nhau. Tuy nhiên, những người tấn công có thể gán ghép các thiết bị của mình vào mạng một cách bất hợp pháp để từ đó lan truyền các thông điệp sai lệch. Do đó, các mạng IoTs này cần thiết phải có một cơ chế xác thực các thiết bị để bảo đảm được rằng các thông điệp truyền nhận đến một thiết bị nào đó phải đến từ một thiết bị hợp lệ trong mạng. Đề tài thành công sẽ góp phần xây dựng một framework thống nhất chịu trách nhiệm xác thực các thiết bị tham gia vào mạng IoTs đồng thời bảo vệ tính riêng tư cho người sử dụng trong quá trình xác thực. Từ đó, góp phần giúp bảo mật các ứng dụng IoTs cũng như tạo niềm tin cho người sử dụng an tâm hơn trong việc sử dụng các dịch vụ của mạng IoTs. Có thể nói, đề tài nghiên cứu này là một trong những công trình nghiên cứu toàn diện đầu tiên về việc xác thực các thiết bị trong mạng IoTs có quan tâm đến việc bảo vệ tính riêng tư của người sử dụng và các đặc điểm riêng của các thiết bị đặc thù tham gia vào mạng IoTs.

B7.2 Đóng góp thực tiễn về chính sách, về khả năng ứng dụng trong thực tế

Với sự phát triển ngày càng mạnh mẽ của mạng vạn vật nói chung và các ứng dụng cụ thể, phổ biến của nó trong cuộc sống hằng ngày cũng như sự phát triển của các thiết bị thông minh và dịch vụ, việc đề ra các giải pháp hỗ trợ việc xác thực và có quan tâm bảo vệ tính riêng tư của người sử dụng có khả năng ứng dụng thực tế rất cao. Rõ ràng, người sử dụng luôn có nhu cầu cấp thiết để bảo vệ tính riêng tư của mình để tránh việc các thông tin cá nhân, nhạy cảm của mình bị tiết lộ trong khi, do yêu cầu bảo mật, các thiết bị (là nơi nắm giữ các thông tin của người sử dụng) tham gia vào mạng vạn vật phải cần được xác thực. Vì vậy, các giải pháp được cung cấp trong đề tài sẽ góp phần bảo mật các hệ thống IoTs cũng như bảo vệ tính riêng tư của người sử dụng tham gia vào hệ thống.

Ngoài ra, đề tài được thực hiện thành công sẽ góp phần định hướng các hướng nghiên cứu về bảo mật trong các hệ thống IoTs, đặc biệt, trong các ứng dụng cụ thể của nó như thành phố thông minh và mạng giao thông thông minh, là các hệ thống mà nhiều thành phố lớn trên thế giới đang quan tâm.

B7.3 Phát triển nhóm nghiên cứu

Các chủ đề về bảo vệ tính riêng tư và bảo mật cho các mạng vạn vật nói chung cũng như các ứng dụng cụ thể, phổ biến nhất của nó nói riêng đang thu hút rất nhiều sự chú ý của cả cộng đồng các nhà nghiên cứu và các nhà phát triển sản phẩm ứng dụng trên thế giới. Thông qua việc thực hiện đề tài, một nhóm nghiên cứu mạnh về các mạng vạn vật cũng như về bảo mật và tính riêng tư của nó sẽ được hình thành và phát triển tại Đại học Quốc gia TPHCM nói riêng và Việt Nam nói chung dựa trên nguồn nhân lực chất lượng sẵn có của nhóm nghiên cứu thực hiện đề tài. Từ đó, bổ sung vào sức mạnh nghiên cứu trong lĩnh vực bảo mật và tính riêng tư của Đại học Quốc gia TPHCM, một trong những lĩnh vực quan trọng mà Đại học Quốc gia TPHCM nói riêng và cả nước nói chung đang quan tâm đầu tư và phát triển. Ngoài ra, đề tài cũng góp phần vào thúc

đẩy việc nghiên cứu và phổ biến về mạng vạn vật cũng như tạo mối liên kết với các nhóm nghiên cứu, trường đại học khác trên thế giới.

B7.4 Khả năng chuyển giao kết quả nghiên cứu

(*Chỉ dành cho loại hình nghiên cứu triển khai)*

B8. Tổng hợp kinh phí đề nghị cấp

Ngày ..... tháng ..... năm	*Ngày ..... tháng ..... năm ....*
Chủ tịch hội đồng thẩm định[1]	**Chủ nhiệm**
(Họ tên, chữ ký)	*(Họ tên và chữ ký)*
Ngày ..... tháng ..... năm....	*Ngày ..... tháng ..... năm ....*
Cơ quan chủ trì[2]	**Cơ quan chủ quản**[3]
(Họ tên, chữ ký, đóng dấu)	*(Họ tên, chữ ký, đóng dấu)*

[1] , [ii], [iii] Chỉ ký tên, đóng dấu khi Đề tài được phê duyệt

[2]

[3]