Kỷ yếu Hội nghị Quốc gia lần thứ X về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), Đà Nẵng, ngày 17-18/08/2017
DOI: 10.15625/vap.2017.00037

INTERNET OF THINGS (IOT) VÀ NHỮNG VẤN ĐỀ THÁCH THỨC AN NINH THÔNG TIN

Nguyễn Văn Tánh[1], Trần Quang Đức[2], Nguyễn Linh Giang[3], Luangoudom Sonxay4

Viện Công nghệ Thông tin và Truyền thông, Trường Đại học Bách khoa Hà Nội

[(1)] tanh.nguyenvan@hust.edu.vn, [(2)]ductq@soict.hust.edu.vn, [(3)]giangnl@soict.hust.edu.vn, [(4)] xay_22@yahoo.com

***TÓM TẮT**: Trong những năm gần đây, sự phát triển mạnh mẽ của Internet of Things (IoT) đã và đang góp phần định hình xã hội thông tin tương lai. IoT thay đổi cách tiếp cận và ứng dụng của công nghệ nhưng đồng thời cũng tạo điều kiện phát sinh các nguy cơ mới về an ninh, an toàn và bảo mật thông tin. Có thể thấy rằng với một môi trường đa dạng, phức tạp, đa vật thể cùng các chuẩn kết nối không đồng nhất, việc đầu tư nghiên cứu xây dựng một hệ thống hoàn thiện về an ninh vẫn chưa thực sự thuyết phục được cộng đồng công nghệ. Trong phạm vi bài viết, chúng tôi sẽ nêu ra một cái nhìn tổng quan về môi trường IoT, các vấn đề liên quan đến giải pháp an ninh hiện thời, những thách thức và khó khăn phía trước trong lĩnh vực này. Cuối bài viết chúng tôi cũng đưa ra những đề xuất về định hướng nghiên cứu góp phần hoàn thiện cơ chế an ninh của hệ thống IoT.*

***Từ khóa**: Internet of Things, An ninh IoT, An toàn bảo mật thông tin IoT, Secure IoT.*

I. GIỚI THIỆU

Trong một vài năm trở lại đây, thuật ngữ Internet of Things (IoT) được nhắc đến khá nhiều và nhận được sự quan tâm mạnh mẽ của cộng đồng công nghệ [1]. IoT là một hệ thống trong đó mỗi đồ vật đều được cung cấp một định danh riêng, có khả năng truyền tải, trao đổi thông tin, dữ liệu qua một mạng duy nhất. Sự bùng nổ của Internet, sự mở rộng về quy mô của thị trường công nghệ di động, thị trường phần mềm và hệ nhúng đã tạo động lực thúc đẩy mạnh mẽ sự phát triển của IoT. Theo dự đoán của các chuyên gia thì đến năm 2020 sẽ có khoảng 50 tỉ thiết bị được kết nối mạng bao gồm cả các thiết bị dân dụng và các thiết bị phục vụ cho các mục đích chuyên biệt như quốc phòng an ninh [2]. Rõ ràng, IoT đã và đang đóng một vai trò quan trọng trong việc thay đổi xã hội thông tin trong tương lai.

Tuy vậy, với một hệ sinh thái phức tạp, IoT tồn tại hàng loạt lỗ hổng an ninh có thể bị khai thác và gây ảnh hưởng trực tiếp đến dữ liệu riêng tư của người sử dụng. Một nghiên cứu gần đây của OWASP (Open Web Application Security Project) [5] đã chỉ ra rằng 75% thiết bị IoT bao gồm cả các thiết bị được tích hợp trong giao thông tự hành, các hệ thống giám sát, nhà thông minh có nguy cơ bị tin tặc tấn công và xâm hại. Các phương pháp bảo mật truyền thống như IPSec, PKI, cơ chế trao đổi khóa Diffie-Hellman đòi hỏi khối lượng tính toán lớn và không phù hợp để tích hợp trong các thiết bị IoT vốn bị hạn chế về hiệu năng, năng lượng và không gian lưu trữ. Bên cạnh đó, sự bất đồng nhất về chuẩn giao thức, cơ sở hạ tầng giữa các nhà sản xuất cũng dẫn đến nhiều khó khăn đối với việc xây dựng một giải pháp hoàn thiện về an ninh cho mạng IoT hiện đại.

Mục tiêu của bài viết này là cung cấp một cái nhìn tổng quan nhất về IoT, những vấn đề an ninh liên quan đến các thành phần hệ thống bao gồm cả thiết bị đầu cuối, định tuyến, chuyển mạch, điện toán đám mây, bài viết cũng tập trung phân tích những thách thức cần phải giải quyết trong tương lai, trên cơ sở đó nâng cao nhận thức của cộng đồng công nghệ đồng thời mở ra những cơ hội hợp tác nghiên cứu giữa các nhà khoa học trong cả nước vì một xã hội an toàn thông tin hướng tới cuộc cách mạng công nghiệp 4.0.

Bài viết này được tổ chức như sau. Phần II giới thiệu về kiến trúc mạng, kiến trúc an ninh của IoT. Phần III đề cập đến cơ chế bảo mật, giải pháp an ninh mạng đang được sử dụng và những vấn đề tồn tại. Phần IV đề xuất một số định hướng nghiên cứu trong môi trường IoT. Phần V đưa ra một số nhận xét đánh giá của nhóm tác giả và kết luận.

II. TỔNG QUAN VỀ INTERNET OF THINGS (IOT)

Đến nay, Internet of Things (IoT) khẳng định được bước tiến của mình nhờ sự hội tụ của nhiều công nghệ, bao gồm truyền tải vô tuyến hiện diện dày đặc, phân tích dữ liệu thời gian thực, học máy, cảm biến hàng hóa và hệ thống nhúng. Điều này có nghĩa là tất cả các dạng thức của hệ thống nhúng cổ điển, như mạng cảm biến không dây, hệ thống điều khiển, tự động hóa (bao gồm nhà thông minh và tự động hóa công trình),…đều đóng góp vào việc vận hành IoT [3].

A. Kiến trúc hệ thống IoT

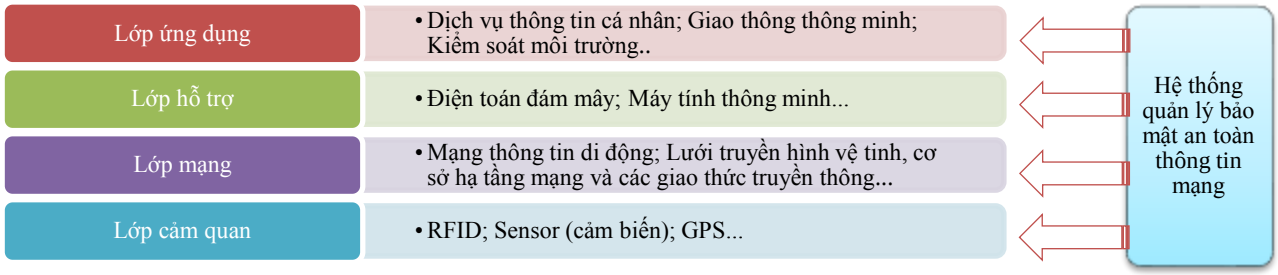
Trong [4], Yashaswini đã mô tả kiến trúc tổng quát của IoT bao gồm 4 thành phần cơ bản như minh họa tại Hình 1.

Các vật thể kết nối Internet (Things) đề cập đến các thiết bị có khả năng kết nối, truyền thông tin và thực hiện nhiệm vụ được xác định của nó như đồng hồ, điện thoại thông minh, đồ gia dụng, đèn chiếu sáng, đo năng lượng hoặc các thiết bị cảm biến để thu thập thông tin khác.

Các Gateway đóng vai trò là một trạm trung gian, tạo ra kết nối giữa các vật thể với điện toán đám mây một cách bảo mật và dễ dàng quản lý. Nói cách khác, Gateway là cửa sổ của hệ thống IoT nội bộ với thế giới bên ngoài. Các công nghệ truyền dữ liệu được sử dụng như GSM, GPRS, cáp quang hoặc các công nghệ internet khác.

Hạ tầng mạng và điện toán đám mây (Network and Cloud): Cơ sở hạ tầng mạng bao gồm thiết bị định tuyến (Router), chuyển mạch (Switch), thiếp bị lặp (Repeater) và nhiều thiết bị khác được dùng để kiểm soát lưu lượng dữ liệu, được kết nối đến mạng lưới viễn thông và triển khai bởi các nhà cung cấp dịch vụ. Trung tâm dữ liệu và hạ tầng điện toán đám mây bao gồm một hệ thống lớn các máy chủ, hệ thống lưu trữ và kết nối các mạng ảo hóa. Công nghệ không dây như Bluetooth, Smart, Zigbee, subGhz, Wi-Fi giúp tạo ra kết nối giữa các thiết bị hoặc giữa thiết bị với mạng Internet. Hệ thống điều khiển được sử dụng để giám sát các mạng IoT thông qua công nghệ không dây, có thể là một thiết bị chuyên dụng như điều khiển từ xa (Remote), điện thoại thông minh (Smartphone) và máy tính bảng (Tablet).

Các lớp tạo và cung cấp dịch vụ (Services-Creation and Solutions Layers) gồm các API (Application Progmraming Interface) hỗ trợ cho công tác quản lý, phân tích dữ liệu và tận dụng hệ thống tài nguyên sẵn có một cách hiệu quả và nhanh chóng.



Hình 1. Mô hình kiến trúc an ninh trong IoT

B. Kiến trúc an ninh trong IoT

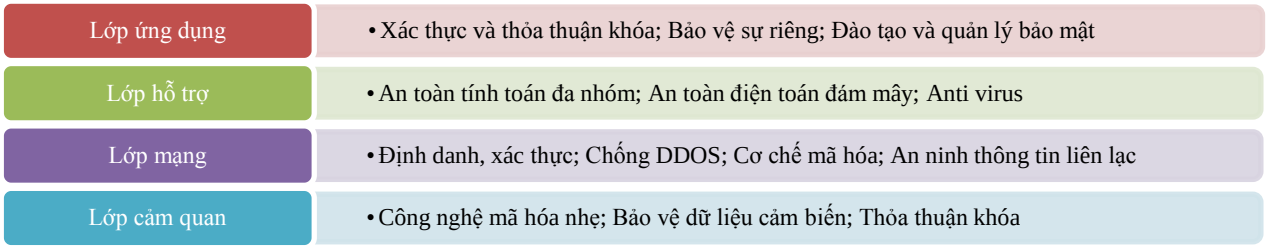
Cũng như các hệ thống truyền thống khác, mục đích cuối cùng của an ninh trong IoT là đảm bảo tính bảo mật, toàn vẹn, tính sẵn sàng, xác thực dữ liệu và thông tin. Trong cơ chế này, kiến trúc an ninh trong IoT có thể chia thành 4 phần chính với các yêu cầu khác nhau như mô hình trong Hình 2 để duy trì tính bảo mật và đảm bảo an toàn thông tin cho người sử dụng.

Tầng cảm quan thực hiện thu thập thông tin về các thuộc tính đối tượng và điều kiện môi trường từ các thiết bị cảm biến. Yêu cầu về an ninh tại tầng này bao gồm (1) Chứng thực (Authentication) giúp ngăn chặn các truy cập bất hợp pháp vào hệ thống IoT; (2) Mã hóa (Encryption) đảm bảo tính bảo mật khi truyền tải thông tin và (3) Thảo thuận khóa (Key agreement) được thực hiện trước khi mã hóa để cung cấp các khả năng an ninh mạng nâng cao. Các khóa hạng nhẹ có thể được sử dụng để tối ưu hóa việc sử dụng tài nguyên và nâng cao hiệu năng của hệ thống.

Tầng mạng truyền tải thông tin dựa trên cơ sở hạ tầng mạng cơ bản như mạng Internet, mạng truyền thông di động, vệ tinh, mạng không dây và các giao thức truyền thông. Các cơ chế bảo mật hiện tại khó có thể áp dụng đối với tầng này. Nguyên nhân chính là do các thiết bị IoT có nguồn năng lượng thấp, dễ tổn hao, khả năng tính toán hạn chế dẫn đến khó khăn trong việc xử lý các thuật toán với độ phức tạp cao [6].

Tầng hỗ trợ được tổ chức theo nhiều cách thức khác nhau, phù hợp với dịch vụ cung cấp như phân tải và xử lý dữ liệu. Tầng hỗ trợ có thể bao gồm phần sụn (Middleware), M2M (Machine to Machine) hoặc nền tảng điện toán đám mây. Hầu hết các giao thức mã hóa, kỹ thuật bảo mật, phân tích mã độc đều được triển khai tại tầng này [7].

Tầng ứng dụng tạo ra các ứng dụng người dùng. Để giải quyết vấn đề an toàn tại tầng này, cần quan tâm hai vấn đề: (1) Chứng thực và thỏa thuận khóa bất đối xứng qua mạng; (2) Bảo vệ quyền riêng tư của người dùng. Ngoài ra, công tác quản lý như quản lý mật khẩu cũng cần nhận được sự quan tâm đặc biệt.



Hình 2. Mô hình kiến trúc an ninh trong IoT

Như đã thảo luận, việc phát triển các giải pháp IoT an toàn đầu cuối đòi hỏi một cách tiếp cận toàn diện bao gồm nhiều cấp độ và kết hợp các tính năng bảo mật quan trọng giữa bốn lớp: Thiết bị, Truyền thông, Hỗ trợ và Ứng dụng. Có thể thấy rằng, đảm bảo an toàn an ninh trong IoT là một vấn đề phức tạp và nhiều thách thức. Các cơ chế và kỹ thuật hiện có sẽ được đề cập chi tiết hơn ở phần sau.

III. CƠ CHẾ BẢO MẬT VÀ NHỮNG THÁCH THỨC AN NINH TRONG IOT

Bên cạnh sự phát triển mạnh mẽ của IoT, vấn đề an ninh ngày càng đóng vai trò quan trọng, nhằm đảm bảo an toàn cho thông tin khách hàng cũng như ngăn chặn việc truy cập điều khiển trái phép thiết bị, dựa trên mô hình kiến trúc của IoT, phần này của bài viết giới thiệu các giải pháp an ninh đang được sử dụng hiện nay, đồng thời cũng nêu ra những vấn đề còn tồn tại, những thách thức để cảnh báo nhằm nâng cao tối đa hiệu quả an ninh và tiện lợi cho cả nhà sản xuất cũng như người sử dụng.

A. Phương pháp mã hóa

Yêu cầu cơ bản của một hệ thống an ninh là đảm bảo thông tin được mã hóa một cách an toàn và không dễ dàng bị khai thác. Thực hiện được việc này cần các thuật toán có độ phức tạp cao, nhưng cũng cần đáp ứng các vấn đề về hiệu suất xử lý của thiết bị [8]. Trong đó mã hóa đối xứng và mã hóa bất đối xứng là hai thuật toán phổ biến nhất. Một số hệ thống bảo mật hiện đại sử dụng kết hợp cả hai thuật toán nhằm tận dụng các ưu điểm của chúng.

Mã hóa đối xứng (Symmetric Encryption) [8] [9] như AES (Advanced Encryption Standard) [10], Triple DES (Triple Data Encryption Algorithm) [11] hoặc IDEA (International Data Encryption Algorithm) [12] là những kỹ thuật sử dụng chung một khóa bí mật. Ưu điểm của nó là khối lượng tính toán ít phù hợp cho các thiết bị cấu hình thấp. Tuy nhiên mã hóa đối xứng có tính bảo mật không cao [13].

Mã hóa bất đối xứng (Asymmetric Encryption) [14] là thuật toán sử dụng một cặp khóa, khóa công khai và khóa cá nhân. Khóa công khai được dùng mã hóa còn khóa bí mật được dùng giải mã. Mã hóa bất đối xứng phổ biến như RSA có độ phức tạp và khối lượng tính toán lớn hơn nhiều lần so với mã hóa đối xứng [9] [15]. Thuật toán trao đổi khóa Diffie-Hellman cho phép thiết lập một khóa bí mật chung để mã hóa dữ liệu trên kênh truyền thông không an toàn [16].

Bảng 1. So sánh mã hóa đối xứng và bất đối xứng

	Mã hóa đối xứng	**Mã hóa bất đối xứng**
Đặc điểm khóa	Dùng chung 1 chìa khóa cho quá trình mã hóa và giải mã.	Nếu dùng public key để mã hóa thì private key sẽ dùng để giải mã và ngược lại.
Ưu điểm	Tốc độ mã hóa và giải mã nhanh. Sử dụng khóa đơn giản.	Khả năng an toàn cao hơn khóa đối xứng.
Hạn chế	Khó khăn trong việc lựa chọn, phân phối và lưu trữ khóa tin cậy. Giải pháp "thỏa thuận" secret key chưa an toàn. Không dùng để xác thực hay mục đích chống thoái thác được.	Khối lượng tính toán lớn trong quá trình mã hóa và giải mã. Tốc độ mã hóa chậm, tốn nhiều chi phí. Dễ bị lợi dụng tấn công vào khóa công khai

Bảng 2. So sánh một số thuật toán mã hóa đối xứng và bất đối xứng cơ bản

	Ưu điểm	**Hạn chế**
AES [17] (Advanced Encryption Standard): AES là một thuật toán "mã hóa khối" (block cipher) đối xứng với độ dài khóa là 128 bít, 192 bít và 256 bít.	Tốc độ thực hiện cao, chiếm ít tài nguyên AES có mô tả toán học đơn giản, cấu trúc rõ ràng. Được xếp vào nhóm Tiêu chuẩn về an toàn thông tin	AES không đủ an toàn đối với dạng tấn công kênh bên (side channel attack). Cấu trúc toán học của AES có mô tả toán học khá đơn giản.
Triple DES [18] (Triple Data Encryption Algorithm): DES là một thuật toán khối đối xứng với khối 64 bít và khóa 56 bít, 3DES dùng khóa gồm 3 khóa DES.	Triple DES được áp dụng phổ biến hơn với việc thực hiện 3 lần DES làm tăng độ phức tạp và tổng kích thước của khóa hơn. Do đó, chiều dài mã khóa sẽ lớn hơn và an toàn sẽ cao hơn.	Thuật toán được tin tưởng là an toàn trong thực tiễn mặc dù trên lý thuyết phương pháp này vẫn có thể bị phá.
IDEA [19] (International Data Encryption Algorithm): Phương pháp mã khối đối xứng sử dụng 128 bit khoá để mã khối dữ liệu 64 bit.	IDEA đạt được 3 yêu cầu cơ bản của các thuật toán an toàn: (1) Độ an toàn của khối; (2) Độ dài khóa; và (3) Độ phức tạp	Thuật toán vẫn có thể bị khai phá theo lý thuyết.
RSA [20] (Rivest-Shamir-Adleman): RSA là một thuật toán mật mã bất đối xứng, mã hóa khóa công khai. Thuật toán RSA có hai khóa: khóa công khai và khóa bí mật.	Trong các kết nối VPN RSA thường được dùng để mã hóa các "session key" giúp quá trình trao đổi các secret keys được đơn giản và dễ dàng, bảo đảm được tính xác thực cũng như tính toàn vẹn dữ liệu.	Tốc độ mã dịch không nhanh lắm. Chính nhược điểm này làm cho các hệ mật mã khoá công khai khó được dùng một cách độc lập.
Diffie-Hellman [21]: Là thuật toán bất đối xứng, thiết lập bí mật chung để trao đổi dữ liệu an toàn trên một kênh truyền thông, bằng cách tạo ra shared private key.	Nếu quản trị khóa một cách hợp lý có thể chống lại các mối đe dọa như: lộ khóa bí mật; những thao tác không được phép trên khóa công khai và khóa bí mật.	Có khả năng tìm ra được khóa bí mật. Mối quan hệ giữa 2 khóa hay điểm yếu của thuật toán cho phép giải mã không cần khóa.

Trong các hệ thống hiện đại, bảo mật thông tin được thực hiện dựa trên hai cơ chế End-to-End (E2E) và By-Hop. Trong cơ chế E2E (thường được áp dụng ở tầng ứng dụng), việc mã hóa và giải mã chỉ được tiến hành bởi bên gửi và bên nhận. Với cơ chế By-Hop (thường được áp dụng ở tầng mạng), việc mã hóa và giải mã sẽ được thực hiện theo từng chặng

[22]. Đối với môi trường IoT, tầng mạng và tầng ứng dụng có quan hệ mật thiết với nhau. Thông thường, E2E được sử dụng với các yêu cầu bảo mật cao và By-Hop có thể đáp ứng các yêu cầu bảo mật ở mức thấp hơn [22].

B. An ninh thông tin truyền thông

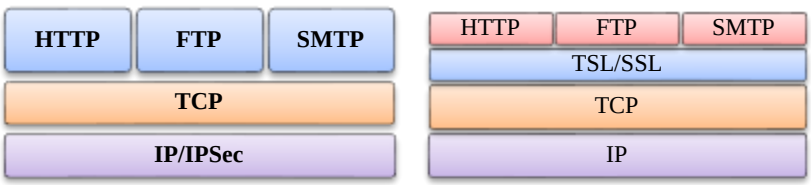
Lớp truyền thông kết nối đảm bảo dữ liệu được truyền/nhận an toàn dù tại lớp vật lý (Wifi, 802.15.4 hoặc Ethernet), lớp mạng (IPv6, Modbus hoặc OPC-UA) hoặc lớp ứng dụng (MQTT, CoAP, web-sockets). Các giải pháp an ninh đã được sử dụng trong lớp này có thể được kể đến như (1) Giải pháp bảo mật tập trung vào dữ liệu (data-centric) đảm bảo dữ liệu được mã hóa an toàn trong khi chuyển tiếp cũng như ở trạng thái nghỉ sao cho ngay cả khi bị chặn, dữ liệu cũng chỉ có ý nghĩa với đối tượng sử dụng là những người có khóa mã hóa chính xác để giải mã; (2) Giải pháp sử dụng tường lửa và các hệ thống ngăn chặn xâm nhập được thiết kế để kiểm tra các luồng lưu lượng cụ thể tại đầu cuối thiết bị. Một số vấn đề an ninh cần lưu ý trên lớp này:

Thiết lập kết nối với đám mây: Việc mở cổng tường lửa chỉ cần thiết khi kết nối đến một dịch vụ nào đó. Thiết bị được điều khiển từ xa thông qua thiết lập kênh truyền 2 chiều giữa chúng và đám mây, có thể xem xét sử dụng mạng riêng ảo (VPN) để truy cập vào thiết bị IoT, điều đó cũng đồng nghĩa với việc cho phép các dịch vụ, cá nhân hoặc một mạng khác tác động vào các tài nguyên bên trong mạng.

Bảo mật thông điệp: Các giao thức bậc thấp dựa trên thông điệp là lựa chọn tốt cho các thiết bị IoT với các tùy chọn cho việc mã hóa hai lần (Double Encrypt), xếp hàng, lọc và thậm chí chia sẻ với bên thứ ba. Với việc đánh nhãn chính xác, mỗi thông điệp có thể được xử lý theo chế độ bảo mật thích hợp. Truyền thông điệp cùng với các quyền kiểm soát truy cập, khả năng bảo mật của thông điệp là giải pháp an ninh cần thiết trên lớp truyền thông của IoT.

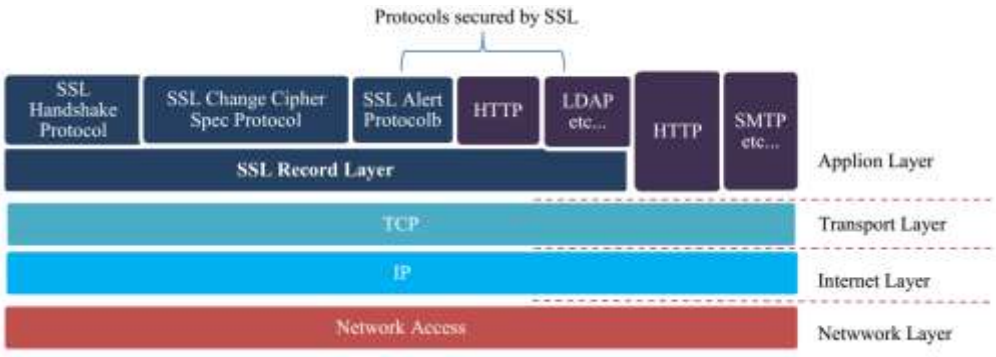
Để chống lại các thách thức của an ninh IoT, việc tuân thủ các nguyên tắc chính này ở cả lớp thiết bị cảm biến và lớp truyền thông sẽ giúp giảm nguy cơ trong tương lai đối với các cấu trúc cơ bản về hệ thống an ninh IoT như hiện nay.

TLS/SSL và IPSec là hai giao thức được sử dụng phổ biến nhất để đáp ứng các yêu cầu về an toàn an ninh như tính toàn vẹn (thông tin không bị thay đổi trong quá trình truyền), tính xác thực (người nhận có thể chứng thực được nguồn gốc của thông tin) và tính bảo mật (dữ liệu được mã hóa để đảm bảo không bị nghe trộm trên đường truyền). Trong mô hình TCP/IP, TSL/SSL được thiết kế nằm ở giữa tầng vận chuyển và tầng ứng dụng. Trong khi đó, IPSec là cơ chế bảo mật ở tầng Internet.



Hình 3. Mô hình bảo mật IPsec và TSL/SSL

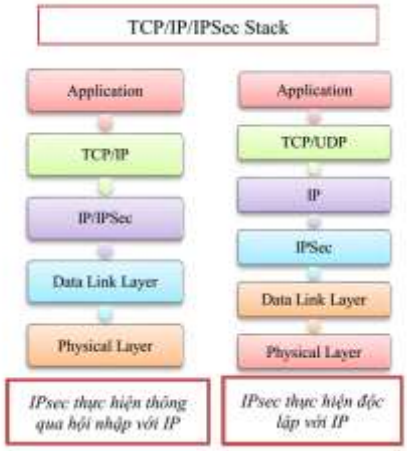
TLS/SSL [23] không phải là một giao thức đơn lẻ, mà là một tập các thủ tục đã được chuẩn hoá để thực hiện các nhiệm vụ như kiểm tra tính hợp lệ của các chứng chỉ được cấp phát và bảo mật thông tin trong quá trình trao đổi giữa máy chủ và khách. Bên cạnh đó, các thuật toán băm (hash algorithm) cũng được áp dụng để đảm bảo tính toàn vẹn của dữ liệu. Một số phương pháp mã hóa và xác thực của SSL như DES, Triple DES, DSA (Digital Signature Algorithm), KEA (Key Exchange Algorithm), MD5 (Message Digest Algorithm), RSA (thuật toán được phát triển bởi Rivest, Shamir và Adleman), RC2, RC4 và SHA-1 (Secure Hash Algorithm). Việc xác định thuật toán mã hóa phù hợp cho phiên giao dịch SSL sẽ được thực hiện trong quá trình bắt tay giữa máy chủ và khách. Các ứng dụng sử dụng TSL/SSL bao gồm NSIIOP, HTTP, FTP, Telnet, IMAP, IRC và POP3 như minh họa trong hình 4.



Hình 4. Mô hình cấu trúc TLS/SSL

IP Security (IPSec) [24] là một giao thức được chuẩn hoá bởi IETF (Internet Engineering Task Force) từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hoá và xác thực cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Như

minh họa trong Hình 5, IPSec có thể coi như phần mở rộng của giao thức IP và được thực hiện thống nhất trong cả hai phiên bản IPv4 và IPv6. Đối với IPv4, việc áp dụng IPSec là một tuỳ chọn, nhưng đối với IPv6, giao thức bảo mật này được triển khai bắt buộc [25]. IPSec chủ yếu dựa vào các thuật toán mã hoá đối xứng. Một yêu cầu không thể thiếu với IPSec bên cạnh các yêu cầu chung là bảo đảm tính đơn nhất của mỗi gói tin nhận và gửi.



Hình 5. Mô hình ứng dụng IPSec trong TCP/IP

C. An ninh dữ liệu cảm biến

Nhiệm vụ quan trọng nhất của tầng cảm biến là đảm bảo tính riêng tư của người sử dụng. Tính riêng tư được thực hiện dựa trên một số nguyên tắc cơ bản như người dùng phải biết rằng dữ liệu liên quan đến họ đang được thu nhận bởi các thiết bị cảm biến, người dùng có quyền quyết định dừng hoặc tiếp tục quá trình thu nhận, thông tin cá nhân của người dùng phải được giữ kín [48]. Đảm bảo các nguyên tắc trên đòi hỏi kỹ thuật lập trình nhúng phù hợp. Bên cạnh các giao thức bảo mật hiện có như đề cập ở phần trước, công tác đào tạo người dùng về các quy trình và cơ chế an toàn an ninh thông tin cũng cần nhận được sự quan tâm đặc biệt nhằm hạn chế việc xâm nhập bất hợp pháp hoặc đánh cắp thông tin cá nhân của tội phạm mạng [49]. Sau đây là một số vấn đề an ninh trên lớp thiết bị cảm biến trong IoT:

Thiết bị "thông minh": Kết nối hiệu quả và an toàn phải được cung cấp bởi một thiết bị "thông minh" có khả năng xử lý bảo mật, mã hóa, xác thực, bộ đếm thời gian, bộ nhớ đệm, proxy, tường lửa,… Do đó, thiết bị phải đủ mạnh để có thể hoạt động trong môi trường IoT.

Xử lý ở biên: Thiết bị thông minh cung cấp sức mạnh, khả năng phát triển, sự tiện dụng, hữu ích theo thời gian, có thể xử lý dữ liệu cục bộ trước khi nó được gửi tới đám mây, hạn chế đưa trực tiếp dữ liệu lớn vào đám mây, thông tin nhạy cảm không cần phải được gửi tới đám mây mà dữ liệu sẽ được xử lý, đóng gói thành các thông điệp rời rạc và được gửi an toàn đến các đối tượng khác nhau. Việc xử lý tốt ở lớp thiết bị sẽ giúp tăng cường an ninh mạng lưới tổng thể.

D. An ninh lớp hỗ trợ, điện toán đám mây

Lớp hỗ trợ đề cập đến phần mềm và công nghệ phụ trợ cho các giải pháp IoT, nơi mà dữ liệu từ thiết bị được thu thập, phân tích, xử lý và hiển thị theo những tiêu chuẩn, định dạng được định nghĩa từ trước. Lớp hỗ trợ và đặc biệt điện toán đám mây được coi là những yếu tố then chốt cho việc áp dụng và phổ biến rộng rãi của IoT.

Các vấn đề cần lưu ý về an ninh IoT trên lớp hỗ trợ và dịch vụ đám mây gồm định danh, chứng thực và mã hóa cho thiết bị, máy móc. Người dùng truy cập các dịch vụ đám mây thường sử dụng hai phương thức xác thực như mật khẩu kết hợp với cơ chế tạo mật khẩu một lần, còn đối với thiết bị máy móc thì xử lý các chứng thư số chắc chắn đem lại hiệu quả cao hơn. Chứng thư số sử dụng hệ thống xác thực bất đối xứng, không chỉ xác thực một giao dịch mà còn mã hóa kênh từ thiết bị tới đám mây trước khi xác thực. Ngoài ra, nó còn cung cấp mã hoá định danh mà rất khó đạt được với user-id/password thông thường.

E. An ninh lớp ứng dụng

Nhu cầu bảo mật của các ứng dụng sẽ khác nhau. Do đó, việc chia sẻ dữ liệu giữa các nền tảng công nghệ cần có sự thống nhất. Đây là một điểm quan trọng phục vụ cho việc xử lý dữ liệu lớn và kiểm soát các hoạt động nhằm đảm bảo an ninh và độ tin cậy cho mạng IoT như bảo vệ sự riêng tư, kiểm soát truy cập dữ liệu, bảo vệ thiết bị điện tử, rò rỉ theo dõi thông tin và bản quyền của phần mềm. Một số nguy cơ thường gặp đối với lớp ứng dụng như khai thác lỗ hổng tràn bộ nhớ đệm, cross-site scripting, SQL injection, các lỗi mật khẩu đơn giản hay lỗ hổng leo thang đặc quyền và tấn công DoS.

Các giải pháp đã được đề xuất để đảm bảo vấn đề an ninh ở lớp ứng dụng như sau: Thứ nhất, ứng dụng cần phải sử dụng công nghệ lập trình an toàn với các phần mềm kiểm tra, chống virus nhằm xác định lỗ hổng dịch vụ và tất cả các loại mã độc có thể tấn công. Thứ hai, dữ liệu cần được xác thực, phát triển bộ nhớ đệm để ngăn chặn tấn công tới dữ liệu. Thứ

ba, thiết lập một cơ chế kiểm tra phiên cho hai hoặc nhiều yêu cầu từ cùng một nguồn để hạn chế tấn công phát lại thông điệp. Thứ tư, kiểm tra ranh giới dữ liệu, mã hóa dữ liệu, kiểm soát truy cập và các biện pháp tương tự được sử dụng để tránh rò rỉ thông tin trong dữ liệu người dùng. Bên cạnh đó, tính sẵn sàng của thiết bị, dữ liệu và dịch vụ là một khía cạnh quan trọng của ứng dụng IoT. Cơ chế kiểm soát của cấu trúc chiều dọc có thể bảo vệ các hệ thống khỏi tấn công từ chối dịch vụ và tấn công từ chối dịch vụ phân tán.

F. An ninh hệ thống IoT trên nền tảng IP

An toàn an ninh thông tin là một lĩnh vực rộng lớn. Đối với IoT, nhiều công nghệ đã được phát triển, trong đó tiêu biểu là ZigBee [26] được xây dựng dựa trên tiêu chuẩn 802.15.4 của tổ chức IEEE (Institute of Electrical and Electronics Engineers). Công nghệ ZigBee sử dụng sóng ngắn và có hai tầng gồm tầng vật lý và tầng MAC (Medicum Access Control) [50]. Nhờ chức năng điều khiển từ xa không dây, truyền dữ liệu ổn định và tiêu thụ năng lượng cực thấp, ZigBee ngày càng trở nên phổ biến và được dùng trong nhiều ứng dụng khác nhau, đặc biệt là các ứng dụng nhà thông minh.

Ngoài ra, nhiều giao thức mới cũng được nghiên cứu để đáp ứng nhu cầu truyền tải, bảo mật thông tin trong hệ thống IoT như RPL (Routing Protocol for Low-Power and Lossy Networks), UDP (User Datagram Protocol) và CoAP (Constrained Application Protocol). CoAP [27] là giao thức ở lớp ứng dụng cho phép các thiết bị IoT có thể giao tiếp với nhau thông qua mạng Internet. Để đảm bảo việc truyền tải dữ liệu an toàn, CoAP sử dụng gói tin bảo mật Datagram Transport Layer Security (DTLS). DTLS hỗ trợ các phương pháp mã hóa nguyên thủy với khối lượng tính toán lớn. Hơn nữa, nó được thiết kế để dùng cho những giao thức mạng với kích thước của thông điệp không phải là tiêu chí quan trọng [28]. Vì thế khi áp dụng kết hợp với 6LoWPAN (IPv6 Protocol over Low-Power Wireless PAN), phần tiêu đề của DTLS cần được nén bằng các cơ chế phù hợp để đảm bảo hiệu năng của hệ thống IoT như đề xuất [29].

Có thể thấy rằng, các giải pháp bảo mật đều được xây dựng theo một kịch bản cụ thể, không tính tới khả năng tương thích với những chuẩn Internet hiện có. Các nhà nghiên cứu đã phát hiện ra một loại lỗ hổng liên quan đến IoT có ảnh hưởng nghiêm trọng như Ghost, VENOM (Virtual Environment Neglected Operations Manipulation). Ghost cho phép tin tặc thực thi các lệnh từ xa nhằm chiếm quyền điều khiển của máy chủ Linux. VENOM tạo ra những ảnh hưởng trực tiếp đến chương trình điều khiển đĩa mềm trong QEMU [33], một bộ giả lập máy tính mã nguồn mở được sử dụng để quản lý máy ảo. Tin tặc có thể khai thác để gửi các lệnh đặc biệt gây tràn bộ nhớ đệm và thực thi các mã tùy ý trong tiến trình Hypervisor của thiết bị đầu cuối.

Những năm trở lại đây, rất nhiều cuộc tấn công mạng với quy mô lớn đã xảy ra trên thế giới. Theo như phân tích của iot-analytics.com, cuối năm 2016, các cuộc tấn công DDoS quy mô lớn vào các máy chủ của DYN (nhà cung cấp dịch vụ DNS lớn của Mỹ) đã làm suy giảm nhiều dịch vụ trực tuyến phổ biến ở Mỹ, cho thấy các thiết bị IoT có thể trở thành công cụ cho các tin tặc thực hiện tấn công mạng [30]. Tại Việt Nam, cuối năm 2014, thông tin của hơn 1.000 camera đã bị đánh cắp và công bố rộng rãi [31]. Nguyên nhân là do người dùng chưa quan tâm đúng mức đến cơ chế bảo mật và an ninh, không thay đổi mật khẩu mặc định của hệ thống trước khi kết nối Internet. Theo thống kê của hãng Kaspersky và Symantec [32], tổng số mẫu phần mềm độc hại nhắm mục tiêu đến các thiết bị thông minh đã lên tới hơn 7.000, trong đó hơn một nửa số này xuất hiện vào năm 2017 và Việt Nam nằm trong số các nước có số người dùng di động bị mã độc tấn công nhiều nhất thế giới. Thời gian vừa qua, tập đoàn VNPT cũng ghi nhận nhiều cuộc tấn công từ chối dịch vụ phân tán (DDoS) từ thiết bị IoT vào các trang thương mại điện tử, tài chính, ngân hàng hoặc thậm chí là nhà cung cấp dịch vụ ISP [33]. Theo thống kế của VNPT, số máy chủ C&C (command and control) điều khiển mạng bonet đã lên tới hơn 100 và có khả năng tăng cao trong các năm tiếp theo.

Rõ ràng, IoT là lĩnh vực nghiên cứu tiềm năng nhưng cũng ẩn chứa nhiều thách thức cần giải quyết cụ thể như sau: (1) *Kiến trúc an ninh IoT*: Mặc dù vẫn được duy trì một cách ổn định nhưng việc xây dựng một kiến trúc an toàn với các cơ chế bảo mật theo chiều sâu của hệ thống vẫn là nhiệm vụ quan trọng mà các nhà nghiên cứu cần phải giải quyết. (2) *Cơ chế trao đổi và quản lý khóa*: Đây là cơ sở quan trọng để nâng cao khả năng bảo mật nhưng cũng là khía cạnh khó khăn nhất của an ninh mật mã. Thuật toán hạng nhẹ hoặc các thiết bị cảm biết có hiệu năng cao vẫn chưa được triển khai trong thực tế tạo ra thách thức thực sự với cộng đồng phát triển IoT. (3) *Luật an ninh và các quy định:* Hiện tại luật pháp vẫn chưa quan tâm đúng mức đến các vấn đề kỹ thuật của các hệ thống IoT, đặc biệt là các vấn đề liên quan đến thông tin quốc gia, bí mật doanh nghiệp và sự riêng tư cá nhân. Đưa ra các quy định thúc đẩy sự phát triển IoT đúng hướng, mạnh mẽ và hiệu quả là một trong những đòi hỏi cấp thiết hiện nay. (4) *Yêu cầu đối với các ứng dụng đang phát triển*: với sự phát triển của mạng cảm biến không dây, công nghệ điện toán đám mây, công nghệ truyền thông mạng, lý thuyết điều khiển phối hợp thời gian thực và RFID, IoT đã và đang phát triển mạnh mẽ. Các ứng dụng cũng được tập trung đầu tư nhưng việc thiếu quy trình kiểm định và đánh giá tính an toàn của ứng dụng đã làm phát sinh các lỗ hổng bảo mật mới. (5) *Công tác quản lý IoT* chưa được thực hiện đúng cách. Bên cạnh đó những vấn đề về bảo mật cũng trở nên phức tạp và khó khăn hơn khi liên quan đến các thiết bị vốn có ràng buộc chặt chẽ về tài nguyên và năng lượng. Thiết kế giao thức bảo mật cần chú ý các vấn đề như hiệu năng, giao tiếp, xử lý dữ liệu và cách thức phân mảnh các gói tin để hạn chế tấn công DoS.

IV. ĐỀ XUẤT CÁC HƯỚNG NGHIÊN CỨU AN NINH CHO NỀN TẢNG IOT

An ninh IoT luôn là một yếu tố vô cùng quan trọng quyết định sự phát triển của hệ sinh thái của vạn vật kết nối Internet. Trên thế giới đã và đang xuất hiện ngày càng nhiều nhà khoa học, các nhóm nghiên cứu, các công ty, tập đoàn

tiến hành đầu tư xây dựng phát triển hệ thống an ninh cho IoT, một số công trình về an ninh IoT tiêu biểu hiện nay đang được nghiên cứu trên thế giới có thể kể đến như là: "*A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications"* của nhóm tác giả Xuanxia Yao và các cộng sự nói về xây dựng cơ chế xác thực nhẹ cho các ứng dụng hệ thống IoT quy mô nhỏ [34]. "*Access Control and the Internet of Things"* của Vinton G. Cerf trình bày về các cơ chế điều khiển truy cập trong hệ thống IoT [35]. "*Middleware for Internet of Things: A Survey"* của tác giả Mohammad Abdur Razzaque cùng các đồng nghiệp đưa ra một đánh giá khá toàn diện về các giải pháp trung gian hiện có đối với những yêu cầu với hệ thống mạng IoT [36]. "*Lithe: Lightweight Secure CoAP for the Internet of Things"* của Shahid Raza cùng các cộng sự đề cập tích hợp DTLS vào giao thức CoAP và cải tiến các thuật toán mã hóa thành mã hóa nhẹ [37]. Đề tài "*Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things"* của tác giả Fagen Li cùng các cộng sự nói đến thiết lập an toàn giao tiếp giữa các thiết bị cảm biến [38]. Ngoài ra, một số công trình khác tập trung vào các khía cạnh an ninh và các vấn đề đặc trưng của IoT, tuy nhiên đều chưa tạo ra được một mô hình nhất quán, giải pháp hoàn thiện cho hệ thống IoT do yêu cầu cân đối giữa các yếu tố "*Năng lượng - Chi phí - Hiệu quả - An toàn*".

Trên cơ sở những hạn chế còn tồn tại với các giải pháp truyền thống đã trình bày phần trước cùng với các hướng nghiên cứu đã và đang được triển khai trên phạm vi toàn cầu, chúng tôi mạnh dạn đề xuất một số định hướng nghiên cứu bổ sung thêm nhằm giải quyết các thách thức về an ninh bảo mật trong hệ thống mạng IoT hiện nay.

Thứ nhất, tích hợp thuật toán mã hóa hạng nhẹ (Lightweight Encryption) vào các giao thức bảo mật của IoT đối với thiết bị mạng. Thuật toán này có hạn chế là tính bảo mật không quá cao nhưng đảm bảo được các yêu cầu về hiệu năng, tính sẵn sàng cũng như chi phí sản xuất thiết bị [34] [50]. Mật mã hạng nhẹ hướng tới một giải pháp thỏa hiệp, một số tác giả đề xuất cơ chế nén DTLS để tận dụng ưu điểm của phương pháp bảo mật này khi áp dụng cùng tiêu chuẩn 6LoWPAN [40]. Tuy nhiên, các thành phần như cấu trúc mã, bộ tham số S-box [44], tầng tuyến tính (linear layer) [54] hay việc tối ưu hóa quá trình tích hợp mã hóa hạng nhẹ trên các thiết bị IoT vẫn cần phải quan tâm và tập trung đầu tư nghiên cứu [53].

Thứ hai, các giao thức bảo mật truyền thống không phù hợp với sự đa dạng về hình thái và khả năng giao tiếp giữa các vật thể trong IoT. Chúng có thể được thay thế bởi một số giao thức mới như MQTT (Message Queuing Telemetry Transport) [41], CoAP (Constrained Application Protocol) và 6LoWPAN/CoRE (Constrained RESTful Environments) [52]. MQTT sử dụng TSL/SSL, CoAP như đã trình bày sử dụng DTLS để bảo mật dữ liệu trong quá trình kết nối. DTLS hỗ trợ RSA và AES hoặc ECC và AES, nghiên cứu và chuẩn hóa các giao thức và kỹ thuật trên, bên cạnh đó việc nghiên cứu thêm các giải pháp mã hóa nhẹ như CurveCP để tích hợp có thể sẽ là tương lai của hệ thống IoT bền vững [51].

Thứ ba, phát triển các thuật toán tìm đường đi ngắn nhất như RPL [47] để áp dụng cho việc định tuyến mạng trong môi trường IoT, kết hợp với các kỹ thuật mã hóa và xác thực phù hợp nhằm nâng cao hiệu năng mạng. Chúng tôi đề xuất hướng nghiên cứu liên quan đến các thuật toán tối ưu như thuật toán di truyền [45] [46] để tăng cường khả năng định tuyến của RPL trong mạng cảm biến không dây hỗ trợ 6LoWPAN [40].

Thứ tư, nghiên cứu về các cơ chế nén trong giao thức IPv6 nhằm tận dụng khả năng định danh của IPv6 đồng thời tiết kiệm chi phí về năng lượng, thời gian và tài nguyên của hệ thống. Bên cạnh đó giải pháp này có thể giúp hạn chế việc gói tin bị phân mảnh, thường xảy ra khi kích thước của chúng lớn hơn so với MTU (Max Transmission Unit). Chúng tôi đề xuất cơ chế nén phần tiêu đề của IPv6 [52], tuy nhiên công trình này vẫn đang trong quá trình nghiên cứu phát triển và cần nhiều hơn sự quan tâm nghiên cứu.

Thứ năm, nghiên cứu một giải pháp về điện toán đám mây toàn diện, kết hợp các giải pháp an ninh phù hợp và thông minh đối với từng dạng thức khác nhau của vật thể kết nối. Điện toán đám mây đóng vai trò quan trọng trong mô hình phát triển hệ thống IoT bền vững. Nghiên cứu về điện toán đám mây bao gồm các vấn đề chính sách, công nghệ, các thuật toán mã hóa để bảo vệ dữ liệu và quyền riêng tư của người dùng, các lỗ hổng bảo mật và kiến trúc của điện toán đám mây. Đa phần các quy trình quản lý khóa hiện nay đều tiềm ẩn những rủi ro liên quan đến lưu trữ và bảo vệ khóa. Những hệ thống có số lượng máy ảo lớn đòi hỏi cơ chế phân quyền phù hợp, có thể bao gồm cả việc kết hợp cơ chế phân quyền theo vai với phân quyền theo đối tượng.

Thứ sáu, nghiên cứu mô hình an ninh nhiều lớp để hạn chế thiệt hại do tấn công mạng gây ra. Trong mô hình này, MAC (Mandatory Access Control) [42] đóng vai trò như điểm nút kiểm soát quyền truy cập dựa trên qua trình gán nhãn cho đối tượng hoặc chủ thể trong hệ thống. Nhãn thuộc đối tượng phản ánh mức độ nhạy cảm của thông tin. Nhãn thuộc chủ thể được định nghĩa bằng mức độ tin cậy dành cho người dùng liên quan đến khả năng tiết lộ thông tin nhạy cảm. MAC dựa trên hai nguyên tắc cơ bản (1) Đọc từ trên xuống (Read down) và (2) Viết từ dưới lên (Write up) giúp ngăn chặn người dùng thực thi những chương trình không có cùng mức độ tin cậy. MAC khi được kết hợp với FLASK và GFAC (Generalized Framework for Access Control) [43] có thể tạo thành cơ chế bảo mật đa lớp với khả năng bảo mật cao. Tuy nhiên cơ chế này vẫn cần phải nghiên cứu và chỉnh sửa để phù hợp hơn khi áp dụng vào hệ thống IoT.

V. KẾT LUẬN

An toàn và an ninh thông tin là một lĩnh vực vô cùng rộng lớn, các giải pháp công nghệ bảo mật chỉ luôn mang tính tương đối, khó có thể giải quyết một các triệt để các yêu cầu toàn vẹn dữ liệu, bảo đảm tính riêng tư của người sử

dụng. Đối với IoT, vấn đề trên càng trở nên phức tạp bởi sự tham gia kết nối của hàng tỉ thiết bị với số lượng lớn người dùng khác nhau. Viễn cảnh thế giới công nghệ đầy tiềm năng nhưng cũng ẩn chứa nhiều nguy cơ, khó khăn đã và đang đặt ra nhiều thách thức đối với tất cả các nhà khoa học trong nước và quốc tế. bài viết này cung cấp một cái nhìn chung nhất về IoT, tập trung phân tích những vấn đề, lỗ hổng bảo mật còn tồn tại. Chúng tôi hy vọng bài viết là tiền đề thúc đẩy khả năng và cơ hội hợp tác giữa các nhà nghiên cứu với mục tiêu phát triển một giải pháp hoàn thiện về an ninh cho hệ thống IoT hiện đại và an toàn.

LỜI CẢM ƠN

Bài báo này được tài trợ từ đề tài Nghị định thư với Đài Loan "Xây dựng kiến trúc hạ tầng an toàn thông tin cho mạng vạn vật trên nền điện toán đám mây", Mã số **NĐT.14.TW/16**.

TÀI LIỆU THAM KHẢO

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey" Computer Networks, vol. 54, no.15, 2010.

[2] "Gartner", Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717.

[3] "Internet of things", at https://en.wikipedia.org/wiki/Internet_of_things.

[4] Yashaswini J, "A Review on IoT Security Issues and Countermeasures", Orient.J. Comp. Sci. and Technol, May 17, 2017

[5] "OWASP Board Votes" at: https://www.owasp.org/index.php/OWASP_Board_Votes.

[6] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, "A Multilayer Security Model for Internet of Things", in Communications in Computer and Information Science, 2012, Volume 312, pp 388-393.

[7] Rafiullah Khan, Sarmad Ullah Khan, R. Zaheer, S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", in 10th International Conference on Frontiers of Information Technology (FIT 2012).

[8] Ramesh. A., Suruliandi. A., "Performance Analysis of Encryption for Information Security", IEEE, 2013.

[9] William Stallings, "Cryptography and network security".

[10] Joan Daemen,Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard".

[11] Dr. Manoj Kumar. "Cryptography and Network Security". Section 3.4: The Simplified Version of DES (S-DES). p. 96.

[12] Harivans Pratap Singh, Shweta Verma, Shailendra Mishra, "Secure-International Data Encryption Algorithm" in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 2, February 2013.

[13] Leo Reyzin, "Symmetric Cryptography", Notes for BU CAS CS 538.

[14] Thorsteinson.book, "Asymmetric Cryptography".

[15] "RSA Asymmetric Encryption" - EECS at UC Berkeley.

[16] Ayan Mahalanobis, "Diffie-Hellman Key Exchange Protocol".

[17] "AES Crypt", https://www.aescrypt.com.

[18] "Triple Data Encryption Standard (Triple-DES)", http://www.vocal.com/cryptography/tdes/

[19] "IDEA (International Data Encryption Algorithm)", http://www.quadibloc.com/crypto/co040302.htm

[20] "RSA" , https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[21] "Diffie–Hellman key exchange", https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[22] Jianhua He, Xiaoming Fu, Zuoyin Tang, "End-to-End Versus Hop-by-Hop Soft State Refresh for Multi-hop Signaling Systems".

[23] "Secure Socket Layer (SSL) Secure Socket Layer (SSL) and Transport Layer Security (TLS)", Raj Jain, Washington University in Saint Louis, MO 63130,

[24] SANOG 6: ISP/NSP Security, 16-23 July, 2006, Merike Kaeo, "IPsec Technology Details".

[25] IPSec & IPv6 - Securing the NextGen Internet, http://ipv6.com/articles/security/IPsec.htm

[26] Overview for ZigBee® (IEEE 802.15.4) , http://www.ti.com/lsds/ti/wireless_connectivity/zigbee/overview.page

[27] CoAP RFC 7252 Constrained Application Protocol, http://coap.technology/

[28] Xi Chen, chen857 (at) wustl.edu, "Constrained Application Protocol for Internet of Things".

[29] "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[30] "Understanding IoT Security - IoT Security Architecture on the Device and Communication Layers", iot-analytics.com.

[31] "Thiết bị IoT bị tấn công như thế nào", http://www.pcworld.com.vn/

[32] "Tình hình tấn công mạng năm 2015", http://stttt.laocai.gov.vn/

[33] "QEMU", https://wiki.debian.org/QEMU

[34] Xuanxia Yao, Xiaoguang Han, Xiaojiang Du, "A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications", IEEE Sensors Journal (Volume: 13, Issue: 10, Oct. 2013).

[35] Vinton G. Cerf , "Access Control for the Internet of Things" Published in: Secure IoT (SIoT), 2016 International Workshop on.

[36] Mohammad Abdur Razzaque, "Middleware for Internet of Things: A Survey", Published in: IEEE Internet of Things Journal (Volume: 3, Issue: 1, Feb. 2016)

[37] Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt "Lithe: Lightweight Secure CoAP for the Internet of Things", Published in: IEEE Sensors Journal (Volume: 13, Issue: 10, Oct. 2013).

[38] Fagen Li and Pan Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things", Published in: IEEE Sensors Journal (Volume: 13, Issue: 10, Oct. 2013).

[39] Sandeep Sadanandan, Rajyalakshmi Mahalingam, "Light Weight Cryptography and Applications".

[40] Ralph Droms , The Document Shepherd is 6LoWPAN WG co-chair Carsten Bormann , "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks".

[41] Andy Stanford-Clark and Hong Linh Truong, "MQTT For Sensor Networks (MQTT-SN) Protocol Specification".

[42] Ray Spencer Secure Computing Corporation, Stephen Smalley, Peter Loscocco National Security Agency, Mike Hibler, David Andersen, Jay Lepreau University of Utah, "The Flask Security Architecture: System Support for Diverse Security Policies".

[43] YIN Cai-yan,WANG Lei(School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048), "Generalized Framework for Access Control Based on Immune Mechanism".

[44] Lauren De Meyer, Begul Bilgin, and Bart Preneel, "Extended Analysis of DES S-boxes".

[45] "Giới thiệu thuật toán Di truyền", http://laptrinh.vn/

[46] Nguyễn Hữu Mùi, Vũ Đình Hòa, "một thuật toán di truyền hiệu quả cho bài toán lập lịch".

[47] Tsvetko Tsvetkov, Betreuer: Alexander Klein, "RPL: IPv6 Routing Protocol for Low Power and Lossy Networks".

[48] M. Langheinrich, "Privacy by design-principles of privacy-aware ubiquitous systems," In Proc. of Ubicomp, Oct. 2001.

[49] C. P. Mayer, "Security and privacy challenges in the internet of things," Electronic Communications of the EASST, vol. 17, 2009.

[50] Xuanxia Yao, Xiaoguang Han, Xiaojiang Du, Senior Member IEEE, and Xianwei Zhou, "A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications".

[51] J¨urgen Sch¨onw¨alder, "Internet of Things: 802.15.4, 6LoWPAN, RPL, COAP", Presented on October 14, 2010.

[52] Prof. Dr.-Ing. Carsten Bormann, "6LoWPAN and CoRE: How to get the next billion nodes on the net and into the web".

[53] Shahid Raza, Hossein Shafagh, "Lithe: Lightweight Secure CoAP for the Internet of Things".

[54] Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun "Block Ciphers - Focus On The Linear Layer"

INTERNET OF THINGS AND ISSUES CHALLENGES INFORMATION SECURITY

Nguyen Van Tanh, Tran Quang Duc, Nguyen Linh Giang, Luangoudom Sonxay

***ABSTRACT**: In the recent time, the development of IoT (Internet of Things) has been shaped the future. IoT changes the approach and application of technologies as well as creates new threads of security, integrity and confidentiality. We can see that with a heterogeneous, complex, multi-material environment and heterogeneous connectivity standards, investment in building a complete security system has not really convinced the community. technology. Within the scope of this article, we will provide an overview of the IoT environment, issues related to current security solutions, challenges and constraints ahead in this area. At the end of the article, we also offer recommendations on research orientation to improve the security mechanism of the IoT system.*

***Keywords**: Internet of Things, Secure for IoT, Security challenge in Internet of Things.*