# Giới thiệu

Trong một vài năm trở lại đây, thuật ngữ Internet of Things (IoT) được nhắc đến rất nhiều và nhận được sự quan tâm mạnh mẽ của cộng đồng công nghệ. 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. Tính đến năm 2025, số lượng thiết bị kết nối Internet trên toàn cầu đã đạt mức 75,44 tỷ thiết bị, theo dự báo của Statista . Sự gia tăng này chủ yếu đến từ sự phát triển của Internet vạn vật (IoT), với các thiết bị như cảm biến, thiết bị gia dụng thông minh, phương tiện giao thông và thiết bị công nghiệp. Trong đó, các thiết bị IoT chiếm tỷ trọng lớn trong tổng số thiết bị kết nối. Rõ ràng, IoT đã và đang đóng một vai trò quan trọng trong việc thay đổi xã hội thông tin trong hiện tại và 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) 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.

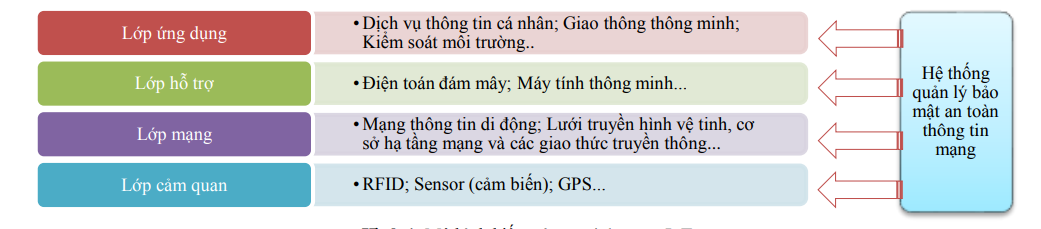
Mục tiêu của bài tiểu luận này là cung cấp một cái nhìn tổng quan nhất về IoT, những vấn đề an ninh liên quan đến các thành phần hệ thống bao gồm cả thiết bị đầu cuối, định tuyến, chuyển mạch, điện toán đám mây, bài viết cũng tập trung phân tích những thách thức cần phải giải quyết trong tương lai, trên cơ sở đó nâng cao nhận thức của cộng đồng công nghệ.

# Tổng quan về Internet of Thing (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

## Kiến trúc hệ thống IoT

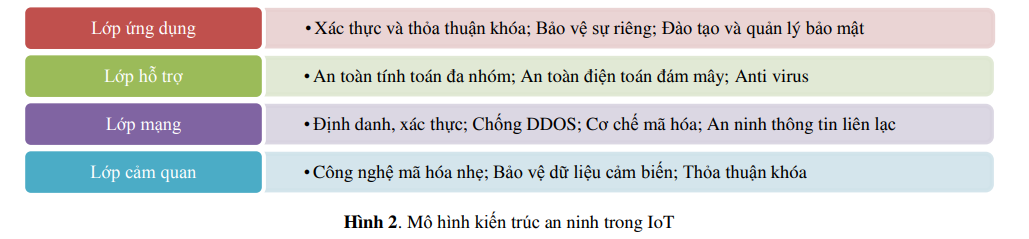
Kiến trúc tổng quát của IoT bao gồm 4 thành phần cơ bản như minh họa tại Hình 1. Các vật thể kết nối Internet (Things) đề cập đến các thiết bị có khả năng kết nối, truyền thông tin và thực hiện nhiệm vụ được xác định của nó như đồng hồ, điện thoại thông minh, đồ gia dụng, đèn chiếu sáng, đo năng lượng 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

## 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 Chứng thực (Authentication) giúp ngăn chặn các truy cập bất hợp pháp vào hệ thống IoT; Mã hóa (Encryption) đảm bảo tính bảo mật khi truyền tải thông tin và Thỏa 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. 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. 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: Chứng thực và thỏa thuận khóa bất đối xứng qua mạng; 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.



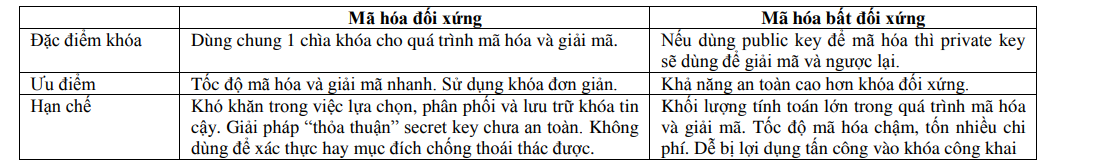
# Cơ chế bảo mật và những thách thức an ninh trong IoT

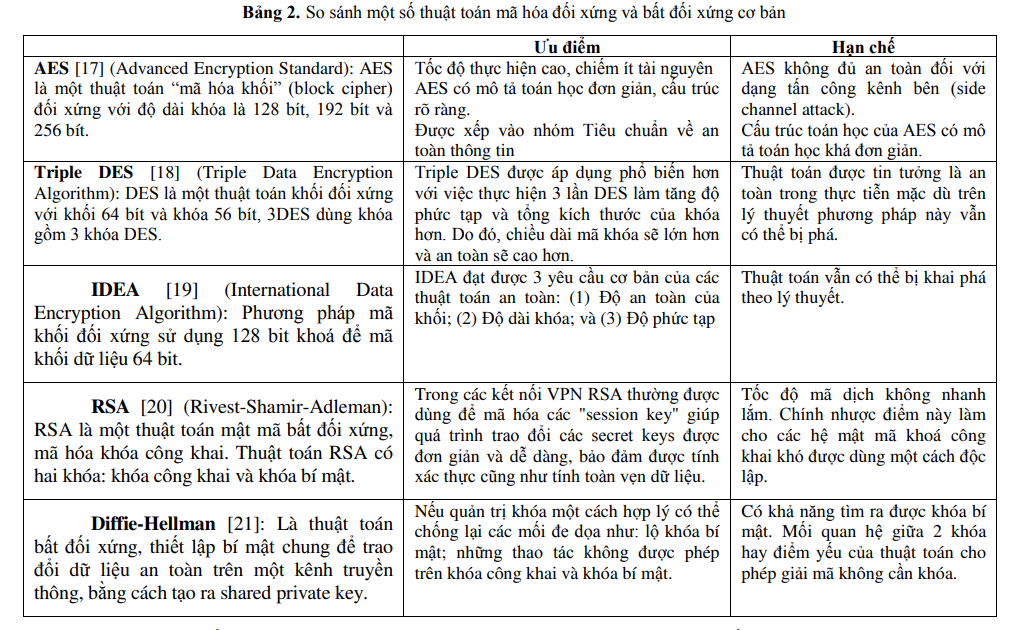
Bên cạnh sự phát triển mạnh mẽ của IoT, vấn đề an ninh ngày càng đóng vai trò quan trọng, nhằm đảm bảo an toàn cho thông tin khách hàng cũng như ngăn chặn việc truy cập điều khiển trái phép thiết bị, dựa trên mô hình kiến trúc của IoT, phần này của bài viết giới thiệu các giải pháp an ninh đang được 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.

## 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. 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) như AES (Advanced Encryption Standard), Triple DES (Triple Data Encryption Algorithm) hoặc IDEA (International Data Encryption Algorithm) 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. Mã hóa bất đối xứng (Asymmetric Encryption) 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. 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.

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





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. 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.

## An ninh thông tin truyền thông

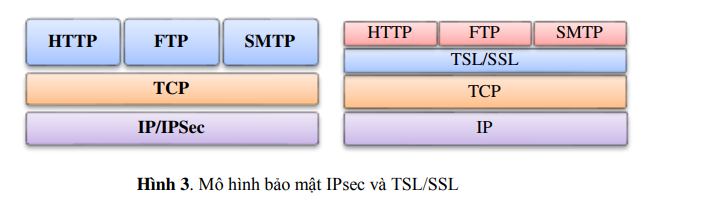
Lớp truyền thông kết nối đảm bảo dữ liệu được truyền/nhận an toàn dù tại lớp vật lý (Wifi, 802.15.4 hoặc Ethernet), lớp mạng (IPv6, Modbus hoặc OPC-UA) hoặc lớp ứng dụng (MQTT, CoAP, web-sockets). Các giải pháp an ninh đã được sử dụng trong lớp này có thể được kể đến như (1) Giải pháp bảo mật tập trung 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.

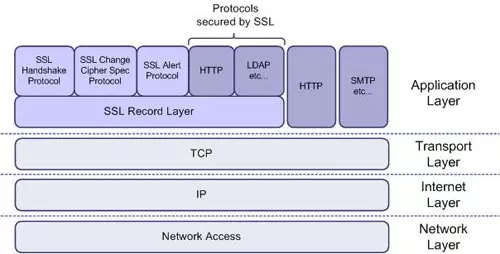
Để chống lại các thách thức của an ninh IoT, việc tuân thủ các nguyên tắc chính này ở cả lớp thiết bị cảm biến và lớp truyền thông sẽ giúp giảm nguy cơ trong tương lai đối với các cấu trúc cơ bản về hệ thống an ninh IoT như hiện nay.

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.



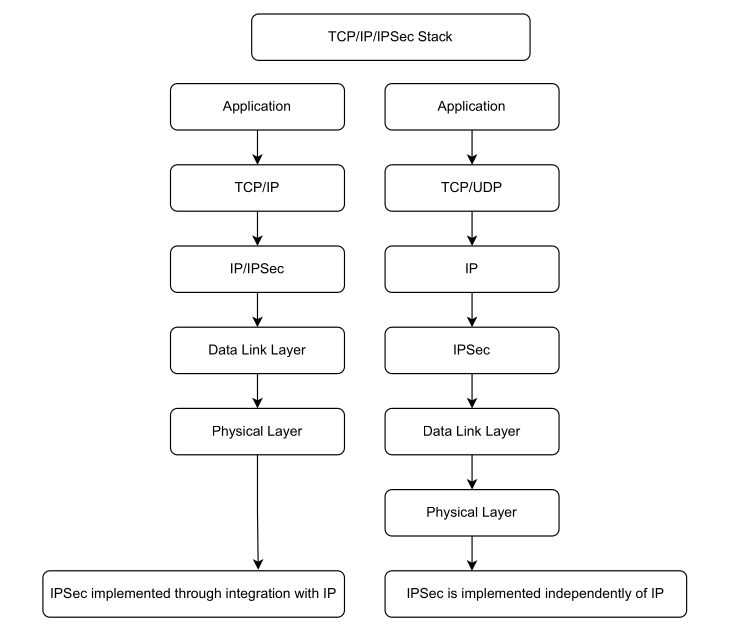
Hình 3. Mô hình bảo mật IPsec và TSL/SSL

TLS/SSL 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) 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. 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

## 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 . 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 . 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.

## 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 userid/password thông thường.

## 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.

## 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 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 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. 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. 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, 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. Tại Việt Nam, cuối năm 2014, thông tin của hơn 1.000 camera đã bị đánh cắp và công bố rộng rãi. 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, 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. 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.