**LÝ THUYẾT BẢO MẬT AN TOÀN THÔNG TIN**

[Chương 1: Tổng quan về Internet vạn vật (IoT) và các vấn đề bảo mật 2](#_Toc917102465)

[1.1 Lược sử về internet vạn vật (IoT) 2](#_Toc1080354577)

[1.2 Kiến trúc hệ thống IoT 3](#_Toc736133720)

[1.3 Các thành phần chính và đặc điểm 5](#_Toc98730188)

[1.4 Ứng dụng trong các lĩnh vực 6](#_Toc510935740)

[1.5 Các lỗ hổng bảo mật thường gặp 7](#_Toc1274684788)

[1.6 Thách thức trong việc bảo vệ hệ thống IoT 14](#_Toc1160324036)

[1.7 Các phương pháp bảo mật hiện nay 17](#_Toc785038540)

[1.8 Phương pháp hậu lượng tử (Post-Quantum Encryption Standards) 19](#_Toc1199287639)

[References 23](#_Toc396942094)

## Chương 1: Tổng quan về Internet vạn vật (IoT) và các vấn đề bảo mật

# 1.1 Lược sử về internet vạn vật (IoT)

Internet vạn vật (IoT) là một lĩnh vực công nghệ phát triển mạnh mẽ, liên quan đến việc kết nối các thiết bị và hệ thống vói internet để chúng có thể giao tiếp, chia sẻ dữ liệu và thực hiện các nhiệm vụ tự động. Dưới đây là cái nhìn tổng quan về sự phát triển của IoT qua các giai đoạn [1]*:*

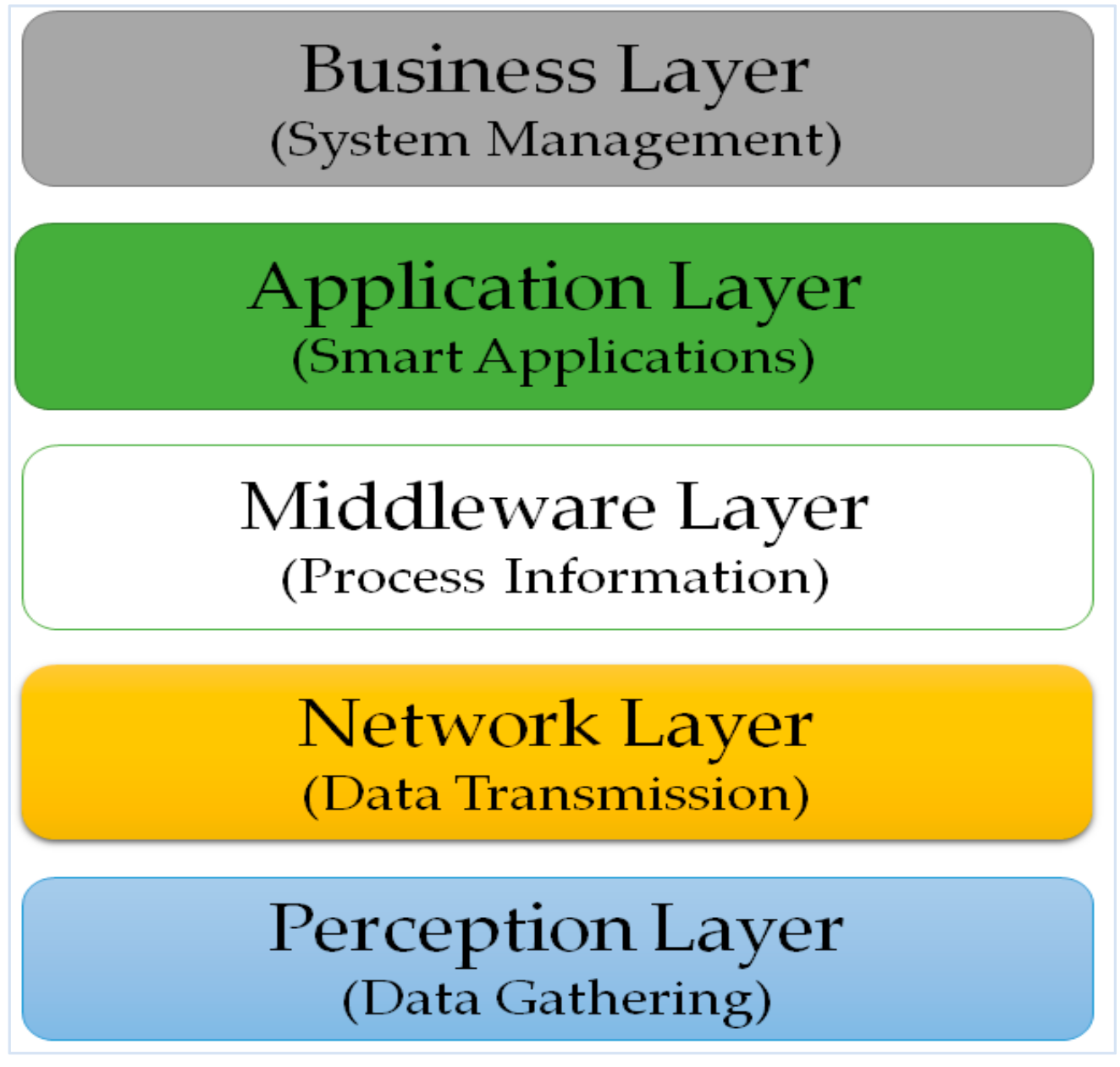
* Giai đoạn 1980 – 1990: IoT bắt đầu những từ những ý tưởng sơ khai, khi vào năm 1980 tại Đại học Carnegie Mellon phát triển hệ thống theo dõi máy bán hàng tự động từ xa.
* Năm 1993: máy pha cafe Trojan Room tại Đại học Cambridge sử dụng camera trực tuyến hiển thị trạng thái của cafe, đánh dấu một ứng dụng IoT thực tế đầu tiên.
* Năm 1999: Kevin Ashton đã đặt tên cho khái niệm “Internet of Things”, mô tả mạng lưới các vật thể vật lý kết nối qua cảm biến và phần mềm.
* Năm 2000: tủ lạnh thông minh đầu tiên được LG ra mắt, mở ra kỷ nguyên thiết bị kết nối internet trong đời sống hằng ngày.
* Trong thập niên 2000: IoT tiếp tục phát triển mạnh mẽ với sự ra đời của các thiết bị như FitBit (2009) - một thiết bị không dây cung cấp dữ liệu thời gian thực về chuyển động, giấc ngủ, ... IoT tiếp cận đến nhiều lĩnh vực trong đời sống.
* Năm 2011 Industrial IoT (IIoT) ra đời, sự đổi mới này để cập đến các cảm biến được nhúng vào máy móc và thiết bị trong các ứng dụng công nghiệp như sản xuất, y học và hậu cần.
* Năm 2014, Seoul trở thành thành phố thông minh đầu tiên, ứng dụng IoT vào quản lý giao thông và môi trường.
* Năm 2016 - 2020: với sự phát triển của điện toán đám mây và mạng 5G, IoT tiếp tục tăng trưởng mạnh, đặc biệt là trong giai đoạn dịch Covid.
* Năm 2021: số lượng thiết bị IoT vượt qua 10 tỷ.
* Năm 2023: sự kết hợp giữa IoT và trí tuệ nhân tạo đã mang đến khả năng tự động hóa và phân tích dữ liệu theo thời gian thực, mở ra kỷ nguyên mới cho IoT.

Tính đến nay, IoT thực sự đã len lỏi vào mọi măt trong đời sống, trong năm 2024 ước tính có 207 tỷ thiết bị được kết nối trên toàn thế giới ở đang dạng các lĩnh vực.

# 1.2 Kiến trúc hệ thống IoT

Theo [**link paper: trong google driver**], các nhà khoa học có nhiều ý kiến khác nhau về định nghĩa kiến trúc của hệ thống IoT.

* Mô hình ba lớp: một số nhà nghiên cứu mô tả kiến trúc IoT gồm ba lớp cơ bản: lớp cảm biến (Sensing), lớp mạng (Networking) và lớp ứng dụng (Application).
* Mô hình năm lớp: một số nhà nghiên cứu khác lại đưa ra mô hình năm lớp bao gồm: lớp cảm biến (Sensing), lớp truy cập (Access), lớp mạng (NeMột biến thể khác của mô hình năm lớp là: lớp nhận thức (Perception), lớp mạng (Networking), lớp trung gian (Middleware), lớp ứng dụng (Application) và lớp kinh doanh (Business).
* Mô hình sáu lớp: một số nhà nghiên cứu đã bổ sung thêm lớp thích ứng (Adaptation layer) nằm giữa lớp nhận thức (Perception) và lớp mạng (Networking), cho phép các thiết bị IoT không đồng nhất có thể giao tiếp với nhau.



Hình 1. Mô hình năm lớp trong hệ thống IoT

# 1.3 Các thành phần chính và đặc điểm

Theo [**link paper: trong google driver**] Hệ thống IoT gồm có bốn thành phần chính đó là:

* Thiết bị/Cảm biến (Devices/Sensors): đây là thành phần chính của bất kỳ ứng dụng IoT nào. Chúng là các thiết bị vật lý dùng để thu thập dữ liệu từ môi trường xung quanh và chuyển chúng thành các dạng tín hiệu nhằm mục đích phân tích. Những thiết bị này rất đơn giản như cảm biến nhiệt độ hoặc phức tạp hơn như camera giám sát an ninh hoặc các thiết bị đo lường trong y tế.
* Thành phần kết nối (Connectivity): các thiết bị đóng vai trò truyền tải dữ liệu giúp các thiết bị IoT có thể nhận và gửi dữ liệu. Các thiết bị này thường sử dụng công nghệ truyền tải như Wifi, Bluetooth hoặc mạng di động 4G/5G để liên lạc với nhau.
* Thành phần ứng dụng (Application): đây là thành phần giúp xử lý và lưu trữ dữ liệu ở giai đoạn cuối bằng các công cụ phân tích như cơ sở dữ liệu và các công cụ phần mềm. Dữ liệu sau khi xử lý, phân tích sẽ sẵn sàng cho các ứng dụng IoT sử dụng. Lớp này cũng quản lý định dạng dữ liệu, có thể là dữ liệu nhị phân hoặc dữ liệu dạng văn bản.
* Thành phần giao diện (Interface): đây là thành phần hữu hình của hệ thống IoT mà người dùng có thể truy cập. Đây là thành phần giúp người dùng quản lý hệ thống và thu thập thông tin, tương tác với hệ thống.

# 1.4 Ứng dụng trong các lĩnh vực

Internet vạn vật (IoT) là công nghệ kết nối thế giới vật lý và thế giới kỹ thuật số, mang lại những cải tiến đáng kể trong nhiều lĩnh vực để nâng cao chất lượng cuộc sống [**link paper: trong google driver**]. Các ứng dụng tiêu biểu có thể kể đến như:

**Trong cuộc sống hằng ngày:** Nhà thông minh là một ứng dụng phổ biến nhất. IoT giúp điều khiển và giám sát các hệ thống trong nhà như ánh sáng, nhiệt độ, điều hòa không khí, camera thông qua các cảm biến. Ngoài ra các thiết bị trong nhà đều có thể kết nối internet và được điều khiển từ xa thông qua điện thoại hoặc máy tính bảng.

**Trong lĩnh vực công nghiệp:** Trong ngành công nghiệp IoT giúp cải thiện quá trình sản xuất và giảm thiểu chi phí. Sau đây là các ứng dụng tiêu biểu:

* Giám sát và phân tích: IoT giúp doanh nghiệp thu thập và phân tích dữ liệu, hiệu suất để từ đó có thể đưa ra các dự đoán và biện pháp phòng ngừa các rủi ro tiềm ẩn.
* IoT cũng giúp tự động hóa các quy trình và giảm chi phí lao động như tự động tắt các thiết bị khi có sự cố, tự động kiểm soát chất lượng hàng hóa, sản phẩm.
* Các thiết bị IoT có thể được gắn trên hàng hóa giúp theo dõi vị trí, trạng thái lịch trình vận chuyển và lưu kho.

**Trong lĩnh vực y tế:** Các giải pháp IoT trong y tế hỗ trợ việc quản lý vật tư y tế và số hóa thông tin bệnh nhân.

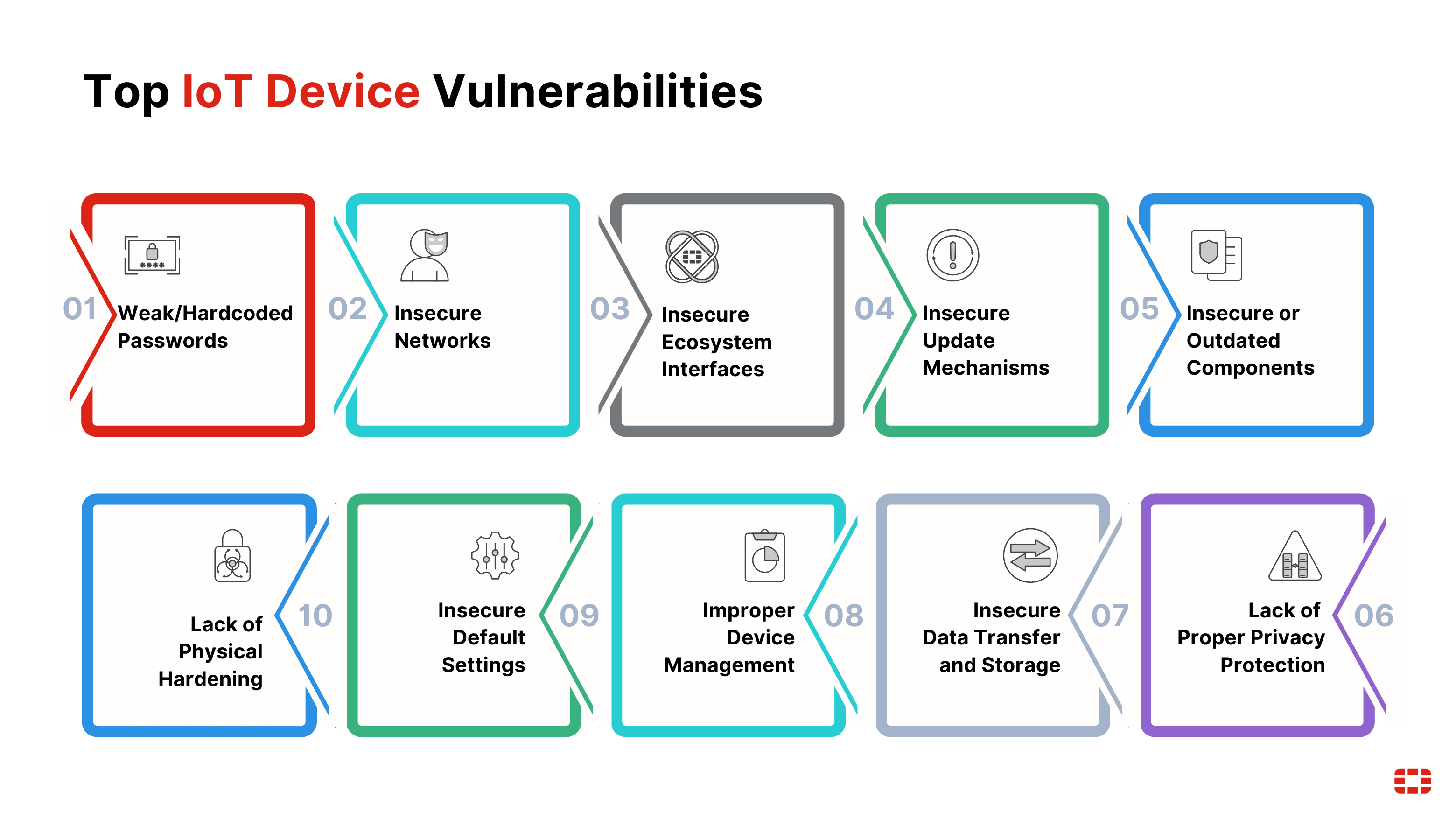
* Các thiết bị IoT hỗ trợ bác sĩ trong việc theo dõi các chỉ số bệnh nhân và đưa ra thông báo nếu có bất kỳ vấn đề gì. Ngoài ra tại các gia đình các thiết bị thông minh như vòng đeo sức khỏe, đồng hồ thông minh cũng tích hợp các chức năng theo dõi các chỉ số cơ thể. Một số thiết bị có khả năng tự phân tích các chỉ số và đưa ra đánh giá bất thường.
* IoT hỗ trợ giám sát các thiết bị y tế như máy xạ trị, máy tim. Các thiết bị này sẽ được kết nối tới một hệ thống quản lý để luôn đảm bảo chúng hoạt động bình thường và sẽ đưa ra cảnh báo nếu có bất kỳ sự cố nào.

**Trong lĩnh vực nông nghiệp:** Iot đóng vai trò quan trọng trong việc cải tiến quy trình và năng suất của ngành nông nghiệp.

* Các hệ thống IoT giúp tự động quy trình, tối ưu quá trình sản xuất. Các ví dụ điển hình có thể kể đến như hệ thống tự động tưới tiêu, phun thuốc.
* Các hệ thống IoT giúp giám sát các điều kiện môi trường, các yếu tố nhiệt độ, ánh sáng, độ ẩm, độ pH của đất. Đây đều là các quy trình giúp người nông dân điều chỉnh quy trình trồng trọt, tăng năng suất và giảm thiểu rủi ro.

# 1.5 Các lỗ hổng bảo mật thường gặp

Trong bối cảnh Internet vạn vật (IoT) ngày càng mở rộng, hàng tỷ thiết bị thông minh được kết nối và triển khai trong nhiều lĩnh vực từ y tế, giao thông, năng lượng cho đến nhà thông minh. Tuy nhiên, song hành với sự tiện lợi và ứng dụng rộng rãi, các lỗ hổng bảo mật trong IoT cũng trở thành mục tiêu hấp dẫn của tin tặc. Theo báo cáo của Fortinet về **các lỗ hổng thường gặp trên thiết bị IoT**, có thể thấy rằng bản chất kết nối rộng và thiếu chuẩn hóa bảo mật khiến IoT trở thành mục tiêu hấp dẫn cho tội phạm mạng. Những lỗ hổng này không chỉ đến từ yếu tố kỹ thuật (phần mềm, firmware, giao thức truyền thông), mà còn từ chính thói quen sử dụng và quản lý thiết bị của người dùng [2] [3]. Từ đó, có thể tổng hợp một số nhóm lỗ hổng tiêu biểu mà hệ thống IoT thường gặp phải như sau:



Hình 2. Các lỗ hổng thường gặp trên thiết bị IoT

1.5.1 Cơ chế xác thực yếu (Weak authentication mechanisms)

Mật khẩu yếu hoặc được mã hoá cứng (hardcoded) là một trong những điểm yếu phổ biến nhất mà kẻ tấn công lợi dụng để xâm nhập các thiết bị IoT. Những mật khẩu ngắn, dễ đoán hoặc bị tái sử dụng cho phép kẻ xấu bẻ khóa thiết bị một cách nhanh chóng, sau đó chiếm quyền điều khiển để thực hiện các cuộc tấn công quy mô lớn hoặc biến thiết bị thành phần của mạng botnet—vấn đề này càng nghiêm trọng khi nhà sản xuất tích hợp sẵn mật khẩu cố định mà người dùng không được hướng dẫn thay đổi. Mật khẩu yếu sẽ khiến hệ thống dễ bị tấn công vét cạn (brute-force) hoặc khai thác trái phép. Ví dụ điển hình là botnet Mirai (2016) đã lợi dụng lỗ hổng này để tạo ra các cuộc tấn công DDoS quy mô lớn.

1.5.2 Mạng không an toàn (Insecure networks)

Mạng không an toàn (Insecure networks) là một trong những lỗ hổng nghiêm trọng thường gặp trong hệ thống IoT, bởi toàn bộ quá trình truyền tải dữ liệu của thiết bị đều phụ thuộc vào hạ tầng mạng. Khi các giao thức truyền thông hoặc dịch vụ chạy trên thiết bị IoT không được bảo vệ đúng mức, kẻ tấn công có thể dễ dàng khai thác điểm yếu này để xâm nhập. Một khi đã chiếm quyền truy cập vào mạng, chúng có khả năng đánh cắp hoặc làm rò rỉ những dữ liệu quan trọng, bao gồm thông tin cá nhân, dữ liệu nhạy cảm của người dùng hoặc thậm chí cả dữ liệu vận hành của hệ thống. Đặc biệt, các mạng không an toàn thường trở thành mục tiêu cho kiểu tấn công **man-in-the-middle (MITM)** – trong đó kẻ tấn công chèn mình vào luồng giao tiếp giữa thiết bị và máy chủ để đánh cắp thông tin đăng nhập, giả mạo xác thực hoặc cài cắm mã độc. Điều này không chỉ gây ra rủi ro mất mát dữ liệu mà còn tạo điều kiện để tiến hành các cuộc tấn công mạng quy mô lớn hơn, khiến hệ thống IoT đối mặt với nhiều nguy cơ về an toàn và quyền riêng tư.

1.5.3 Các giao diện hệ sinh thái không an toàn (Insecure ecosystem interfaces)

Các giao diện hệ sinh thái không an toàn (Insecure ecosystem interfaces) – bao gồm **API, ứng dụng di động và ứng dụng web** – là một trong những mắt xích dễ bị khai thác nhất trong hệ thống IoT. Thông qua những kênh này, kẻ tấn công có thể tìm ra lỗ hổng trong cơ chế kết nối giữa thiết bị, dịch vụ đám mây và người dùng để xâm nhập và chiếm quyền kiểm soát. Nếu không có các lớp xác thực (authentication) và phân quyền (authorization) chặt chẽ, máy chủ sẽ khó phân biệt được đâu là thiết bị hợp lệ, đâu là truy cập độc hại. Hệ quả là dữ liệu nhạy cảm có thể bị đánh cắp, hoặc tệ hơn, hệ thống có thể bị điều khiển từ xa để phục vụ cho những mục đích phi pháp. Do đó, việc triển khai các công cụ nhận dạng an toàn, xác thực nhiều lớp, cùng với cơ chế bảo vệ giao diện đám mây và ứng dụng di động là điều tối quan trọng để ngăn chặn nguy cơ từ những giao diện dễ bị tổn thương này.

1.5.4 Cơ chế cập nhật không an toàn (Insecure update mechanisms)

Cơ chế cập nhật không an toàn (Insecure update mechanisms) là một lỗ hổng đặc biệt nguy hiểm đối với các thiết bị IoT. Khi quá trình cập nhật phần mềm, firmware hoặc bản vá bảo mật không được bảo vệ đúng cách, thiết bị có thể vô tình tải về và cài đặt những đoạn mã độc hại hoặc chưa được xác thực. Một bản cập nhật bị giả mạo hoặc bị chèn mã độc không chỉ khiến thiết bị mất khả năng hoạt động ổn định, mà còn có thể trở thành bàn đạp để kẻ tấn công chiếm quyền kiểm soát toàn bộ hệ thống. Nguy cơ này càng nghiêm trọng trong các lĩnh vực trọng yếu như **năng lượng, y tế hay công nghiệp**, nơi mà sự cố an ninh có thể dẫn đến thiệt hại lớn về tài sản, dữ liệu và thậm chí cả tính mạng con người. Vì vậy, mọi bản cập nhật cần được triển khai qua **kênh truyền mã hóa an toàn**, đồng thời toàn bộ phần mềm phải trải qua quy trình kiểm duyệt và xác thực nghiêm ngặt trước khi được cài đặt lên thiết bị.

1.5.5 Thành phần không an toàn hoặc đã lỗi thời (Insecure or outdated components)

Thành phần không an toàn hoặc đã lỗi thời (Insecure or outdated components) là một trong những nguyên nhân hàng đầu khiến hệ sinh thái IoT trở nên mong manh trước các mối đe dọa mạng. Việc sử dụng những đoạn mã, thư viện mã nguồn mở hoặc phần mềm của bên thứ ba mà không được kiểm tra, giám sát chặt chẽ có thể vô tình đưa các lỗ hổng tiềm ẩn vào hệ thống. Đặc biệt, các thành phần đã lỗi thời hoặc không còn được nhà phát triển hỗ trợ cập nhật bảo mật sẽ nhanh chóng trở thành “cửa ngõ” để kẻ tấn công khai thác. Hệ quả là bề mặt tấn công (attack surface) của tổ chức ngày càng mở rộng, khiến việc bảo vệ toàn diện trở nên khó khăn hơn. Vì vậy, để duy trì an toàn, các tổ chức cần thường xuyên rà soát, cập nhật và thay thế những thành phần cũ, đồng thời áp dụng cơ chế kiểm định bảo mật đối với mọi mã nguồn và phần mềm được tích hợp vào hệ thống IoT.

1.5.6 Thiếu cơ chế bảo vệ quyền riêng tư (Lack of proper privacy protection)

Thiếu cơ chế bảo vệ quyền riêng tư (Lack of proper privacy protection) là một trong những vấn đề nhức nhối nhất trong hệ sinh thái IoT hiện nay. Các thiết bị IoT thường xuyên thu thập và xử lý dữ liệu cá nhân của người dùng – từ thông tin định danh, thói quen sinh hoạt cho đến dữ liệu sức khỏe nhạy cảm. Nếu dữ liệu này không được mã hóa, lưu trữ an toàn và quản lý đúng theo các quy định bảo mật hiện hành (như GDPR hay các tiêu chuẩn địa phương), tổ chức sẽ phải đối mặt với nguy cơ rò rỉ thông tin, bị phạt nặng, mất uy tín và đánh mất lòng tin của khách hàng. Tệ hơn, một sự cố rò rỉ có thể khiến quyền riêng tư của người dùng bị xâm phạm nghiêm trọng, tạo điều kiện cho kẻ xấu khai thác cho các mục đích bất chính. Chính vì vậy, việc triển khai các biện pháp bảo vệ dữ liệu cá nhân – từ mã hóa, kiểm soát truy cập, cho đến cơ chế ẩn danh dữ liệu – không chỉ là yêu cầu kỹ thuật, mà còn là trách nhiệm pháp lý và đạo đức đối với người dùng trong kỷ nguyên kết nối IoT.

1.5.7 Truyền tải và lưu trữ dữ liệu không an toàn (Insecure data transfer and storage)

Truyền tải và lưu trữ dữ liệu không an toàn (Insecure data transfer and storage) là một lỗ hổng đặc biệt nguy hiểm trong hệ sinh thái IoT. Các thiết bị IoT thường xuyên trao đổi dữ liệu với máy chủ trung tâm hoặc với các thiết bị khác trong mạng, và nếu quá trình này không được mã hóa hoặc kiểm soát chặt chẽ, kẻ tấn công có thể dễ dàng nghe lén, giả mạo hoặc đánh cắp thông tin. Điều này không chỉ làm mất đi tính **toàn vẹn** (integrity) và **độ tin cậy** (reliability) của dữ liệu, mà còn có thể dẫn đến những quyết định sai lệch trong quá trình vận hành, quản lý hoặc phân tích. Việc lưu trữ dữ liệu trên thiết bị hoặc trong hệ thống đám mây mà thiếu các biện pháp bảo mật – như mã hóa, phân quyền truy cập, và kiểm tra tính toàn vẹn – càng làm tăng nguy cơ rò rỉ, gây tổn hại đến cả tổ chức lẫn người dùng. Chính vì vậy, đảm bảo dữ liệu IoT được truyền tải và lưu trữ an toàn là yếu tố cốt lõi để duy trì sự ổn định, tin cậy và bền vững của toàn bộ ứng dụng IoT.

1.5.8 Quản lý thiết bị không đúng cách (Improper device management)

Quản lý thiết bị không đúng cách (Improper device management) là một trong những nguyên nhân làm gia tăng đáng kể rủi ro bảo mật trong môi trường IoT. Trong suốt vòng đời hoạt động, nếu thiết bị không được giám sát, cập nhật và vô hiệu hóa đúng thời điểm, chúng có thể trở thành điểm yếu để kẻ tấn công khai thác—even khi thiết bị đã ngừng sử dụng. Thực tế cho thấy nhiều tổ chức không nắm rõ đầy đủ những tài sản hay thiết bị nào đang kết nối vào mạng của mình, dẫn đến tình trạng tồn tại các thiết bị không được kiểm soát hoặc bị bỏ quên. Những “cửa ngõ” vô hình này chính là cơ hội để kẻ xấu xâm nhập, đánh cắp hoặc nghe lén dữ liệu nhạy cảm. Do đó, việc **phát hiện, định danh và quản lý vòng đời thiết bị IoT một cách toàn diện** không chỉ là yêu cầu quản trị hạ tầng, mà còn là điều kiện tiên quyết để đảm bảo an ninh và duy trì sự tin cậy của hệ thống.

1.5.9 Cài đặt mặc định không an toàn (Insecure default settings)

Cài đặt mặc định không an toàn (Insecure default settings) là một trong những “gót chân Achilles” của các thiết bị IoT. Để thuận tiện cho việc triển khai và sử dụng, hầu hết thiết bị đều được nhà sản xuất tích hợp sẵn các cấu hình mặc định hoặc thậm chí là mật khẩu hardcoded. Tuy nhiên, chính sự đơn giản này lại vô tình mở ra cánh cửa cho kẻ tấn công, bởi những thiết lập mặc định thường ít được thay đổi và dễ dàng bị dò tìm công khai. Một khi khai thác thành công, tin tặc có thể chiếm quyền truy cập vào firmware, chèn mã độc hoặc biến thiết bị thành bàn đạp để mở rộng tấn công vào hạ tầng doanh nghiệp. Điều này không chỉ đe dọa tính bảo mật dữ liệu, mà còn làm gia tăng nguy cơ gián đoạn dịch vụ và tổn hại uy tín của tổ chức. Vì vậy, việc thay đổi, vô hiệu hóa các cấu hình mặc định ngay từ giai đoạn cài đặt ban đầu, kết hợp với áp dụng các chính sách bảo mật nghiêm ngặt, là bước đi thiết yếu để giảm thiểu nguy cơ từ điểm yếu này.

1.5.10 Thiếu cơ chế bảo vệ vật lý (Lack of physical hardening)

Thiếu cơ chế bảo vệ vật lý (Lack of physical hardening) là một điểm yếu dễ bị bỏ qua nhưng lại vô cùng quan trọng trong hệ sinh thái IoT. Khác với các hệ thống CNTT truyền thống thường được đặt trong trung tâm dữ liệu an toàn, nhiều thiết bị IoT lại được triển khai ở những môi trường hở, xa trung tâm, hoặc tại các khu vực khó kiểm soát. Chính sự phân tán này khiến chúng trở thành mục tiêu thuận lợi cho kẻ tấn công tiến hành các hành vi phá hoại vật lý, thao túng thiết bị, cài đặt phần cứng độc hại hoặc thậm chí đánh cắp toàn bộ thiết bị. Một cuộc tấn công vật lý thành công không chỉ làm gián đoạn hoạt động, mà còn mở đường cho việc khai thác sâu hơn vào hệ thống mạng nội bộ. Do đó, việc áp dụng các biện pháp bảo vệ vật lý – từ thiết kế phần cứng chống giả mạo, cơ chế niêm phong và phát hiện can thiệp, cho đến kiểm soát môi trường triển khai – là điều kiện cần thiết để đảm bảo an toàn tổng thể cho các thiết bị IoT trong suốt vòng đời hoạt động [2].

# 1.6 Thách thức trong việc bảo vệ hệ thống IoT

Ngày nay, hệ thống Internet vạn vật (IoT) càng trở nên phổ biến trong nhiều lĩnh vực như y tế, giao thông, nhà thông minh, và ngành công nghiệp. Chính sự kết nối rộng rãi và tính tự động cao của IoT mang lại nhiều tiện ích — nhưng cũng mở ra vô số lỗ hổng bảo mật. Các thiết bị IoT thường được triển khai trong môi trường phức tạp, phân tán, với tài nguyên hạn chế, nên việc bảo vệ chúng là một bài toán không hề đơn giản.

Dưới đây là các thách thức lớn nhất mà các nhà nghiên cứu và các doanh nghiệp đang đối mặt khi bảo vệ hệ thống IoT Theo phân tích trong Analysis of IoT Security Challenges and Its Solutions Using Machine Learning (Mazhar et al., 2023) và Challenges in IoT Security: A Comprehensive Survey (Mudholkar & Dobariya, 2024):

Trước hết, **gia tăng bề mặt tấn công (Attack Surface Expansion)** là hệ quả tất yếu của việc số lượng thiết bị kết nối không ngừng tăng lên, ước tính đã vượt quá 20 tỷ thiết bị vào năm 2022. Càng nhiều thiết bị tham gia mạng lưới, bề mặt tấn công càng mở rộng. Đáng lo ngại là chỉ cần một thiết bị yếu kém – như một camera giá rẻ hoặc cảm biến không được mã hóa – cũng có thể trở thành điểm khởi phát cho các cuộc xâm nhập quy mô lớn, gây ảnh hưởng đến toàn bộ hệ thống.

Tiếp đến là **hạn chế về tài nguyên (Resource Constraints)**. Hầu hết thiết bị IoT đều được thiết kế nhỏ gọn, tiêu thụ ít năng lượng, dẫn đến dung lượng bộ nhớ, khả năng xử lý và nguồn pin hạn chế. Chính điều này khiến cho việc áp dụng những cơ chế bảo mật truyền thống, vốn đòi hỏi tài nguyên lớn như mã hóa mạnh hay hệ thống phát hiện xâm nhập phức tạp, trở nên khó khả thi. Bài toán đặt ra cho các nhà nghiên cứu là phải phát triển những giải pháp bảo mật “nhẹ”, vừa tiết kiệm tài nguyên vừa đảm bảo an toàn thông tin.

Một thách thức khác đến từ **tính không đồng nhất (Heterogeneity)**. IoT là sự hội tụ của hàng loạt thiết bị với phần cứng, hệ điều hành, giao thức và tiêu chuẩn khác nhau – từ Zigbee, BLE, MQTT cho đến 5G. Chính sự đa dạng này khiến cho việc thiết kế một khung bảo mật thống nhất trở nên phức tạp. Một giải pháp hiệu quả trong môi trường công nghiệp có thể hoàn toàn không phù hợp với thiết bị đeo cá nhân hay xe tự lái, dẫn đến nguy cơ thiếu liên thông và tính tương thích trong bảo mật.

Song song với đó, **khó khăn trong cập nhật và vá lỗi (Firmware and Patching Issues)** cũng là vấn đề nan giải. Nhiều thiết bị IoT không hỗ trợ cơ chế cập nhật từ xa (OTA), hoặc thậm chí bị nhà sản xuất ngừng hỗ trợ ngay sau khi phát hành. Điều này khiến các lỗ hổng bảo mật tồn tại lâu dài và dễ dàng bị khai thác. Vụ tấn công botnet Mirai là minh chứng rõ ràng, khi hàng triệu thiết bị IoT bảo mật yếu bị lợi dụng để thực hiện các cuộc tấn công từ chối dịch vụ phân tán (DDoS) trên diện rộng.

Ngoài ra, bản thân kiến trúc nhiều lớp của IoT cũng tiềm ẩn **các mối đe dọa đa tầng (Multi-layer Threats)**. Ở lớp cảm biến, dữ liệu có thể bị giả mạo, nghe lén hoặc thậm chí phá hoại vật lý. Lớp mạng dễ bị tấn công kiểu Man-in-the-Middle, DDoS hoặc gây nhiễu tín hiệu. Lớp trung gian có nguy cơ bị khai thác thông qua ứng dụng độc hại hoặc lỗi trong xử lý dữ liệu, trong khi lớp ứng dụng lại thường mắc phải các vấn đề như API không an toàn hoặc lỗ hổng trong hệ điều hành. Chính vì vậy, bảo mật IoT đòi hỏi cách tiếp cận toàn diện, đa tầng và tích hợp.

Không dừng lại ở đó, **sự thiếu hụt khung bảo mật động và thích ứng (Lack of Adaptive Security)** cũng là một vấn đề nổi bật. Các công cụ truyền thống như tường lửa hay IDS tĩnh ngày càng tỏ ra kém hiệu quả trước các hình thức tấn công mới, vốn biến hóa liên tục và tinh vi. Xu hướng hiện nay là áp dụng các kỹ thuật dựa trên trí tuệ nhân tạo và học máy, cho phép phân tích lưu lượng, nhận diện hành vi bất thường và phản ứng gần như theo thời gian thực, mở ra một hướng đi hứa hẹn trong nghiên cứu và triển khai.

Cuối cùng, không thể bỏ qua **nguy cơ từ công nghệ mới – thách thức lượng tử (Quantum Computing Challenge)**. Khi máy tính lượng tử phát triển, các thuật toán mã hóa phổ biến hiện nay như RSA hay ECC có thể bị phá vỡ trong thời gian ngắn, đe dọa trực tiếp đến tính an toàn của các hệ thống IoT. Điều này buộc cộng đồng nghiên cứu phải sớm chuyển sang các thuật toán mật mã kháng lượng tử (Post-Quantum Cryptography) nhằm bảo đảm an ninh bền vững cho kỷ nguyên mới.

Tóm lại, các thách thức bảo mật trong IoT không chỉ đa dạng và phức tạp mà còn có xu hướng gia tăng cả về quy mô lẫn mức độ tinh vi. Việc nhận diện rõ những thách thức này là bước quan trọng để từ đó xây dựng các giải pháp bảo mật toàn diện, thích ứng và có khả năng chống chịu trước những nguy cơ ngày càng khó lường trong tương lai.

# 1.7 Các phương pháp bảo mật hiện nay

Sự phát triển mạnh mẽ của IoT trên nhiều lĩnh vực, từ y tế, công nghiệp, logistics cho đến đô thị thông minh, không chỉ mang lại tiện ích mà còn đặt ra những vấn đề nghiêm trọng về an ninh. Như đã được chỉ ra, hầu hết thiết bị IoT đều đối mặt với những hạn chế về tài nguyên tính toán, bộ nhớ và kết nối mạng, khiến các giải pháp bảo mật truyền thống khó có thể áp dụng hiệu quả. Điều này dẫn đến nhu cầu cấp thiết phải phát triển những phương pháp bảo mật chuyên biệt, vừa phù hợp với đặc thù tài nguyên hạn chế của IoT, vừa có khả năng ứng phó với các mối đe dọa ngày càng tinh vi. Trong bối cảnh đó, phần tiếp theo sẽ trình bày một số **phương pháp bảo mật hiện nay** đang được nghiên cứu và triển khai trong lĩnh vực IoT.

Để đối phó với những thách thức an ninh ngày càng gia tăng, nhiều phương pháp bảo mật đã và đang được nghiên cứu cũng như triển khai trong hệ sinh thái IoT. Ở mức cơ bản, **xác thực (authentication)** và **kiểm soát quyền truy cập (access control)** đóng vai trò tuyến phòng thủ đầu tiên, đảm bảo rằng chỉ các thiết bị và người dùng hợp lệ mới có thể tham gia mạng lưới. Các cơ chế như xác thực hai chiều, chứng thư số, hoặc PUF (Physically Unclonable Functions) đã được chứng minh hiệu quả trong việc ngăn chặn truy cập trái phép, dù vẫn còn tồn tại hạn chế về chi phí và quản lý khóa [4]. Bên cạnh đó, **mã hóa dữ liệu (encryption)** – cả khi truyền (in transit) và lưu trữ (at rest) – là giải pháp cốt lõi nhằm bảo vệ tính bí mật và toàn vẹn thông tin. Tuy nhiên, các thiết bị IoT thường bị giới hạn về năng lượng và tài nguyên tính toán, do đó việc áp dụng **thuật toán mã hóa nhẹ (lightweight cryptography)** hoặc giao thức truyền thông tối giản trở thành xu hướng tất yếu [5], [6].

Ngoài các biện pháp truyền thống, việc **cập nhật phần mềm và firmware an toàn (secure update)** thông qua cơ chế OTA (Over-the-Air) cũng đặc biệt quan trọng, giúp vá các lỗ hổng kịp thời. Dù vậy, nhiều thiết bị IoT không được hỗ trợ cập nhật hoặc bị nhà sản xuất ngừng duy trì, khiến nguy cơ bị khai thác vẫn hiện hữu. Để tăng cường khả năng phòng thủ, **giám sát an ninh và phát hiện bất thường (anomaly detection/IDS)** dựa trên học máy và học sâu đang nổi lên như một giải pháp triển vọng, cho phép nhận diện hành vi bất thường và mẫu tấn công trong thời gian gần như thực, mặc dù vẫn gặp thách thức về dữ liệu huấn luyện và tỷ lệ cảnh báo sai [7].

Ở cấp độ kiến trúc, **phân đoạn mạng (network segmentation)** và sử dụng firewall hoặc gateway chuyên biệt giúp giới hạn phạm vi tấn công, trong khi các công nghệ mới như **blockchain và sổ cái phân tán** được kỳ vọng sẽ mang lại tính minh bạch, không chối bỏ và loại bỏ sự phụ thuộc vào bên trung gian trong quản lý danh tính và truy cập. Tuy nhiên, các giải pháp này cũng làm phát sinh thách thức về độ trễ và tiêu thụ năng lượng [8]. Đặc biệt, xu hướng “**secure by design**” – tức là tích hợp bảo mật ngay từ giai đoạn thiết kế phần cứng, phần mềm và giao thức – được coi là nguyên tắc dài hạn để giảm thiểu rủi ro ngay từ đầu [9].

Tổng thể, các phương pháp bảo mật hiện nay cho IoT cho thấy sự dịch chuyển từ **các cơ chế bảo mật truyền thống** sang **các giải pháp động, thích ứng và chuyên biệt**. Nghiên cứu gần đây nhấn mạnh tầm quan trọng của việc kết hợp nhiều công nghệ – chẳng hạn như học máy, blockchain và mật mã kháng lượng tử – để tạo nên một khung bảo mật đa tầng, linh hoạt và đủ mạnh trước các mối đe dọa hiện tại lẫn tương lai [5], [6], [7], [8].

# 1.8 Phương pháp hậu lượng tử (Post-Quantum Encryption Standards)

Các hệ mật mã công khai phổ biến như **RSA** và **ECC** dựa trên các bài toán khó (phân tích thừa số nguyên, logarit rời rạc). Nếu xuất hiện máy tính lượng tử quy mô lớn, **thuật toán Shor** có thể giải các bài toán này trong thời gian đa thức, đe doạ trực tiếp tính an toàn của hạ tầng mật mã hiện hữu. Vì vậy, cộng đồng tiêu chuẩn hoá đã chủ động chuẩn bị lộ trình chuyển đổi sang các thuật toán **kháng lượng tử**. Từ tháng 8/2024, **NIST** đã ban hành ba tiêu chuẩn FIPS đầu tiên cho mật mã hậu-lượng-tử: **FIPS 203 (ML-KEM/Kyber), FIPS 204 (ML-DSA/Dilithium), FIPS 205 (SLH-DSA/SPHINCS+)**; đến 3/2025, **HQC** cũng được lựa chọn để chuẩn hoá tiếp theo. Đây là các mốc then chốt khẳng định tính cấp thiết của chuyển đổi PQC ở cấp quốc gia và công nghiệp [10].

1.8.1 Khái niệm

**Post-Quantum Cryptography (PQC)** là lớp thuật toán mật mã công khai (trao đổi khoá, chữ ký số, mã hoá) được thiết kế dựa trên các bài toán mà, theo hiểu biết hiện nay, **không có thuật toán lượng tử hiệu quả** để phá vỡ. Các họ chính gồm: **lattice-based** (Kyber, Dilithium, NTRU), **code-based** (Classic McEliece/HQC/BIKE), **hash-based** (SPHINCS+), **multivariate**, và **isogeny-based** (một số biến thể mới như SQIsign sau khi SIKE bị bẻ). Trong bối cảnh **IoT**, chuẩn ngành **GSMA PQ.04 (2024)** phân tích rủi ro lượng tử đối với hệ kết nối dựa trên **3GPP** và đề xuất nguyên tắc **crypto-agility/migration** cho hệ sinh thái thiết bị–mạng–điện toán biên. Các khảo sát gần đây trên học giới cũng hệ thống hoá toàn cảnh thuật toán, tiêu chí lựa chọn và khuyến nghị triển khai cho môi trường hạn chế tài nguyên [11].

Thiết bị IoT thường hạn chế CPU/bộ nhớ/năng lượng, vì vậy khi chuyển sang PQC cần chọn **thuật toán nhẹ** và/hoặc tối ưu hoá triển khai (phần mềm và phần cứng). Các khảo sát năm 2024–2025 ghi nhận chi phí tính toán và kích thước tham số của nhiều thuật toán PQC cao hơn so với RSA/ECC, song **lattice-based KEM** (như Kyber, NTRU) tỏ ra cân bằng tốt giữa bảo mật và hiệu năng trên thiết bị phổ thông/nhúng khi được tối ưu hợp lý [12].

Trong khi mật mã hậu lượng tử (PQC) mở ra một hướng đi quan trọng để bảo vệ hệ thống IoT trước nguy cơ từ máy tính lượng tử, việc triển khai trên thực tế lại đối mặt với nhiều rào cản đáng kể. Các nghiên cứu gần đây và cả lộ trình tiêu chuẩn hoá của NIST cho thấy rằng thách thức không chỉ nằm ở mặt lý thuyết thuật toán mà còn bao gồm toàn bộ vòng đời tích hợp vào hệ thống IoT. Có thể tóm lược bốn nhóm thách thức cốt lõi sau đây: (i) chi phí tính toán, bộ nhớ và tiêu thụ năng lượng; (ii) khả năng tương thích và chuyển đổi dần (crypto-agility) trong hệ thống đang hoạt động; (iii) nhu cầu gia tốc phần cứng để đạt độ trễ chấp nhận được; và (iv) yêu cầu tiêu chuẩn hoá và niềm tin dài hạn, gắn liền với lộ trình FIPS do NIST ban hành [13].

1.8.2 Phân loại và các thuật toán PQC tiêu biểu

**Lattice-based -** Đại diện: **Kyber (KEM), Dilithium (DSA), NTRU**. Điểm mạnh là **cân bằng bảo mật–hiệu năng**, phù hợp cho trao đổi khoá/chuỗi TLS, được NIST chuẩn hoá sớm; điểm yếu là kích thước tham số/khóa và độ trễ có thể tăng nếu không tối ưu. Các nghiên cứu so sánh trên môi trường IoT/nhúng cho thấy **Kyber và NTRU** đều khả thi khi có cấu hình/giảm nhẹ thích hợp [13].

**Code-based -** Đại diện: **Classic McEliece/HQC/BIKE**. Lâu đời, cơ sở lý thuyết vững; hạn chế lớn nhất là **kích thước khoá công khai rất lớn**, gây áp lực bộ nhớ/băng thông cho thiết bị IoT. (HQC được NIST chọn bổ sung 3/2025) [13].

**Hash-based signatures -** Đại diện: **SPHINCS+** (được NIST phê chuẩn FIPS 205). Dựa trên hàm băm, cấu trúc đơn giản, độ tin cậy lý thuyết cao; đổi lại **kích thước chữ ký lớn** và chi phí tính toán cao hơn ECDSA [13].

**Multivariate & Isogeny-based -** Một số lược đồ **multivariate** có tốc độ ký nhanh nhưng đối mặt với các kết quả phân tích/bẻ khoá gần đây; **isogeny-based** (ví dụ SQIsign) có ưu thế **khoá/chữ ký nhỏ** nhưng triển khai phức tạp và tốc độ còn hạn chế trong thực tế IoT. (Hướng này hiện được xem là tiền tiêu nhưng chưa phải trụ cột triển khai đại trà) [14].

**Bằng chứng thực nghiệm -** Trên nền **TLS 1.3** và giao thức tầng ứng dụng (MQTT), một số nghiên cứu cho thấy **KEM dạng lattice** có thể **nhanh hơn ECDH** ở khâu bắt tay dù gói tin lớn hơn, trong khi **chữ ký PQ** vẫn thường **chậm hơn ECDSA** trên thiết bị ARM phổ thông, hàm ý cần chọn hybrid hoặc tinh chỉnh điểm chèn chữ ký trong đường đi dữ liệu [15].

1.8.3 Khả năng triển khai PQC trong IoT và mô hình & thực tiễn

**(i) Hybrid (Kết hợp PQC + cổ điển).** Trong giai đoạn chuyển đổi, cấu hình **hybrid** (ví dụ **X25519 + Kyber**) giúp duy trì khả năng tương thích và “phòng hộ kép”: nếu một trong hai trụ cột bị suy yếu, kênh vẫn an toàn. Các đánh giá hiệu năng PQ-TLS trên nền thư viện như **Open Quantum Safe (OQS)** cho thấy hybrid có thể triển khai được trên **Raspberry Pi/vi điều khiển** với tham số phù hợp [16].

**(ii) Offloading ra biên (edge-offloading).** Với thiết bị siêu hạn chế, một hướng là **đẩy phép toán nặng** (đổi khóa, ký) sang **edge server** trong kiến trúc MEC, kết hợp các cơ chế bảo mật lớp vật lý hoặc phân đoạn mạng để kiểm soát bề mặt tấn công. (Xu hướng này xuất hiện trong một số nghiên cứu gần đây về tối ưu hoá độ trễ và năng lượng cho PQC trên IoT) [14].

**(iii) Khung mã hoá hỗn hợp.** Một số hệ thống đề xuất **kết hợp nhiều lớp**: mật mã đối xứng nhanh (cho dữ liệu khối lượng lớn), **PQC KEM/DSA** (cho khoá & nhận thực), thậm chí **QKD** trong kịch bản đặc thù; mục tiêu là cân bằng an toàn lượng tử–hiệu năng–chi phí [14].

**(iv) Trạng thái triển khai công nghiệp.** Bên cạnh tiêu chuẩn FIPS, tài liệu **GSMA PQ.04** hướng dẫn **crypto-agility** và **lộ trình di trú** cho chuỗi IoT kết nối 3GPP; ở lớp dịch vụ, nhiều nhà cung cấp (ví dụ các CDN/đám mây) đã công bố **mở rộng hỗ trợ PQC cho giao thức/hệ sản phẩm** từ 2024–2025, cho thấy tính sẵn sàng của chuỗi cung ứng [11].

## 1.9 Kết luận

Internet vạn vật (IoT) đang tạo ra những bước đột phá lớn trong nhiều lĩnh vực, mang lại tiện ích và hiệu quả vượt trội. Tuy nhiên, sự phát triển này cũng kéo theo không ít thách thức, đặc biệt là vấn đề bảo mật. Các lỗ hổng từ mã hóa yếu đến các thiết bị không bảo mật đang là mối nguy tiềm tàng đối với sự an toàn của hệ thống IoT.

Để bảo vệ các hệ thống này, việc áp dụng các phương pháp bảo mật như mã hóa, xác thực đa yếu tố và quản lý quyền truy cập là vô cùng quan trọng. Đồng thời, công nghệ hậu lượng tử (Post-Quantum Encryption) cũng mở ra hướng đi mới, giúp tăng cường bảo mật trong kỷ nguyên máy tính lượng tử.

Với những yếu tố này, bảo mật sẽ là yếu tố quyết định để IoT có thể phát triển mạnh mẽ và bền vững trong tương lai.

# References

|  |  |
| --- | --- |
| [1] | Thales, "The history of IoT: From concept to reality," 21 01 2025. [Online]. |
| [2] | Fortinet, "IoT device vulnerabilities," 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities. |
| [3] | "IoT security issues and solutions," 9 April 2024. [Online]. Available: https://webbylab.com/blog/iot-security-issues-and-solutions/. |
| [4] | P. Williams, "A survey on security in Internet of Things with a focus on authentication and access control," *ScienceDirect,* 2022. |
| [5] | B. e. a. Gușiță, "Securing IoT Edge: A Survey on Lightweight Cryptography and Protocols.," *SpringerLink,* 2025. |
| [6] | "A Survey on IoT Security Using Cryptographic Algorithms," *Internet of Things,* 2023. |
| [7] | M. e. a. Mazhar, "Analysis of IoT Security Challenges and Its Solutions Using Machine Learning and Deep Learning," *PCM,* 2023. |
| [8] | "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats & Countermeasures.," *arXiv.* |
| [9] | E. &. T. M. Dritsas, "A Survey on Cybersecurity in IoT," *MDPI,* 2025. |
| [10] | N. I. o. S. a. T. (NIST), "NIST Newsroom (U.S. Department of Commerce)," NIST Releases First 3 Finalized Post-Quantum Encryption Standards, 8 2024. [Online]. |
| [11] | G. A. (GSMA), "Post Quantum Cryptography in IoT Ecosystem," in *Non-confidential*, 2024. |
| [12] | G. R. R. J. Tao Liu, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," *Computer Science,* 2024. |
| [13] | NIST, "Computer Security Resource Center," Post-Quantum Cryptography Standardization, 13 3 2024. [Online]. |
| [14] | M. A. W. I. Y. A. Khwaja Mansoor, "Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices," *Cluster Computing,* Vols. Vol.28, No.2, 2024. |
| [15] | G. R. a. R. J. Tao Liu, "Post-Quantum Cryptography for Internet of Things:," *arXiv,* 2024. |
| [16] | J. A. Montenegro, "A performance evaluation framework for post-quantum TLS," *Future Generation Computer Systems,* vol. 175, 2025. |