Công ty xuất bản Hindawi

Tạp chí quốc tế về mạng cảm biến phân tán

Tập 2015, ID bài viết 286860, 9 trang <http://dx.doi.org/10.1155/2015/286860>

*Bài viết nghiên cứu*

**Hướng tới sự tích hợp giữa IoT và**

**Điện toán đám mây: Một cách tiếp cận an toàn**

**Tự cấu hình thiết bị nhúng**

# Antonio Puliafito, Antonio Celesti, Massimo Villari và Maria Fazio

*DICIEAMA, Đại học Messina, Contrada di Dio, Sant'Agata, 98166 Messina, Ý*

Thư từ nên được gửi tới Antonio Celesti; acelesti@unime.it

Nhận ngày 17 tháng 4 năm 2015; Được chấp nhận ngày 2 tháng 9 năm 2015

Biên tập viên học thuật: Melike Erol-Kantarci

Bản quyền © 2015 Antonio Puliafito và cộng sự. Đây là bài viết truy cập mở được phân phối theo Giấy phép Ghi nhận tác giả Creative Commons, cho phép sử dụng, phân phối và sao chép không hạn chế trong bất kỳ phương tiện nào, miễn là tác phẩm gốc được trích dẫn hợp lý.

Việc khởi động và thiết lập an toàn các thiết bị Internet of Things (IoT) được kết nối qua Đám mây là một vấn đề mở đầy thách thức. Bài viết này đề cập đến việc cấu hình tự động các thiết bị IoT một cách an toàn thông qua Đám mây nhằm cung cấp các dịch vụ giá trị gia tăng mới. Sau cuộc thảo luận về các giới hạn của các giải pháp IoT và Đám mây hiện tại về khả năng tự cấu hình an toàn, chúng tôi trình bày kiến trúc dựa trên Đám mây cho phép các thiết bị IoT tương tác với một số nhà cung cấp Đám mây liên kết. Đặc biệt, chúng tôi trình bày hai tình huống có thể xảy ra, đó là môi trường Đám mây đơn và Đám mây liên kết, tương tác với các thiết bị IoT và chúng tôi giải quyết các vấn đề cụ thể của cả hai. Hơn nữa, chúng tôi trình bày một số điểm nổi bật về thiết kế về cách vận hành khi xem xét phần cứng và phần mềm mở thực sự.

sản phẩm đã có trên thị trường.

# Giới thiệu

Internet of Things (IoT) là bước phát triển tiếp theo của Internet, trong đó mọi vật thể/vật thể có/được trang bị khả năng tính toán và giao tiếp đều có thể được tích hợp liền mạch, ở các cấp độ khác nhau, vào Internet. Việc khai thác các công nghệ điện toán đám mây đang là thách thức để hỗ trợ phát triển hệ thống IoT vì nó đảm bảo khả năng mở rộng và độ tin cậy cao của các dịch vụ sẵn có. Do đó, IoT và điện toán đám mây cung cấp những khả năng mới để chia sẻ dữ liệu và dịch vụ qua Internet, bằng cách giới thiệu một hệ thống mạng toàn cầu động với khả năng tự cấu hình dựa trên các giao thức truyền thông tiêu chuẩn và có thể tương tác [1].

Như đã nhấn mạnh trong *Chương trình nghị sự kỹ thuật số cho Châu Âu [2]* , một trong những thách thức chính đối với Ủy ban Châu Âu là có cơ sở hạ tầng Đám mây có tính cạnh tranh toàn cầu cho “Internet dịch vụ” được kết nối với “Mọi thứ” được phân bổ trên các khu vực vùng sâu vùng xa. IoT hiện được áp dụng trong nhiều lĩnh vực ứng dụng, như xây dựng tòa nhà, giám sát giao thông ô tô, phân tích môi trường, hỗ trợ chăm sóc sức khỏe, dự báo thời tiết và giám sát video. Do đó, IoT sẽ cung cấp các dịch vụ mới để làm cho các thành phố “Thông minh hơn” và nó sẽ cải thiện sự tương tác của con người và các thiết bị/dịch vụ IoT với môi trường xung quanh, nâng cao chất lượng cuộc sống của Người dân. Trong những kịch bản này, bảo mật là một trong những yếu tố chính cản trở việc áp dụng và triển khai IoT và điện toán đám mây trên quy mô lớn và nhanh chóng.

Không có giới hạn nào đối với các kịch bản có thể thực hiện được khi kết hợp IoT và điện toán đám mây và một số kiến trúc đã được đề xuất cho đến nay [3]. Theo quan điểm của chúng tôi, IoT có thể xuất hiện như một phần mở rộng tự nhiên của Điện toán đám mây, trong đó Đám mây cho phép chúng ta truy cập các tài nguyên và khả năng dựa trên IoT, để quản lý các môi trường phổ biến thông minh. Ngoài ra, điện toán đám mây có thể hỗ trợ việc cung cấp dịch vụ IoT. Do đó, dịch vụ IoT có thể được coi là Dịch vụ cảm biến và kích hoạt theo yêu cầu (SAaaS). Một trong những vấn đề chính trong việc triển khai các thiết bị IoT là việc tự cấu hình các thiết bị cần thiết để kết nối chúng qua Đám mây.

Theo tầm nhìn của chúng tôi, thiết bị IoT phải có khả năng tự cấu hình để tương tác với Đám mây một cách an toàn và sẽ tự động tùy chỉnh hành vi của thiết bị bằng cách tải xuống các tính năng cần thiết từ theCloud.Fromtheuserpointofview, khi người dùng bật thiết bị IoT của mình và kết nối nó qua WiFi ( hoặc các công nghệ truyền thông khác), họ chỉ cần đợi thiết bị tự cấu hình và sau đó có thể bắt đầu sử dụng.

Để tự định cấu hình các thiết bị IoT một cách an toàn và cho phép chúng tương tác qua Đám mây, các thiết bị cần được trang bị các khả năng bao gồm khóa bảo mật, thuật toán mã hóa và ID ẩn. Cách tiếp cận này đã trở thành hiện thực. Một ví dụ được biểu thị bằng http://www.my-devices.net/, nghĩa là nhà cung cấp Đám mây cung cấp các dịch vụ truy cập từ xa an toàn tới các thiết bị nhúng thông qua HTTP(S) hoặc các giao thức dựa trên TCP khác. Đồng thời, *Temboo* (https://www .temboo.com/) cung cấp các giải pháp thương mại sáng tạo để kết nối các thiết bị IoT với các dịch vụ Đám mây (ví dụ: Lưu trữ, Xử lý và Nhắn tin) bằng cách sử dụng Giao diện Chương trình Ứng dụng (API) đơn giản. Những ví dụ này chỉ đại diện cho “một vài giọt trong đại dương IoT và điện toán đám mây” do sự quan tâm lớn của các công ty nghiên cứu và kinh doanh trong lĩnh vực ứng dụng này.

Trong nghiên cứu trước đây [4], chúng tôi đã phân tích các vấn đề hiện tại về khả năng tự cấu hình của thiết bị IoT được kết nối qua Internet với các nhà cung cấp Đám mây. Cụ thể, chúng tôi đã đề xuất một phương pháp an toàn để khởi động và thiết lập các thiết bị nhúng. Trong bài viết này, chúng tôi thảo luận cách áp dụng giải pháp của mình trong môi trường thực, trình bày hai tình huống có thể xảy ra: Môi trường Đám mây đơn và Đám mây liên kết tương tác với các thiết bị IoT. Hơn nữa, chúng tôi trình bày một số điểm nổi bật về thiết kế, thảo luận cách vận hành khi xem xét các sản phẩm phần cứng và phần mềm mở thực sự đã có sẵn trên thị trường. Giải pháp được đề xuất ở đây nhằm vào các doanh nghiệp IoT coi điện toán đám mây là chiến lược để cải thiện hoạt động kinh doanh của họ.

Phần còn lại của bài báo được tổ chức như sau. Phần 2 thảo luận về các công việc liên quan. Phần 3 trình bày hai kịch bản đầy thách thức khi tích hợp IoT và điện toán đám mây. Trong Phần 4, chúng tôi thảo luận về các yếu tố chính liên quan đến việc tự nhận dạng an toàn các thiết bị IoT. Trong Phần 5, chúng tôi đề xuất kiến trúc dựa trên Đám mây IoT. Trong Phần 6, chúng tôi thảo luận về cách các thiết bị IoT tham gia hệ thống Đám mây có thể tự đăng ký để thực hiện quy trình tự cấu hình. Phần 7 kết thúc bài viết.

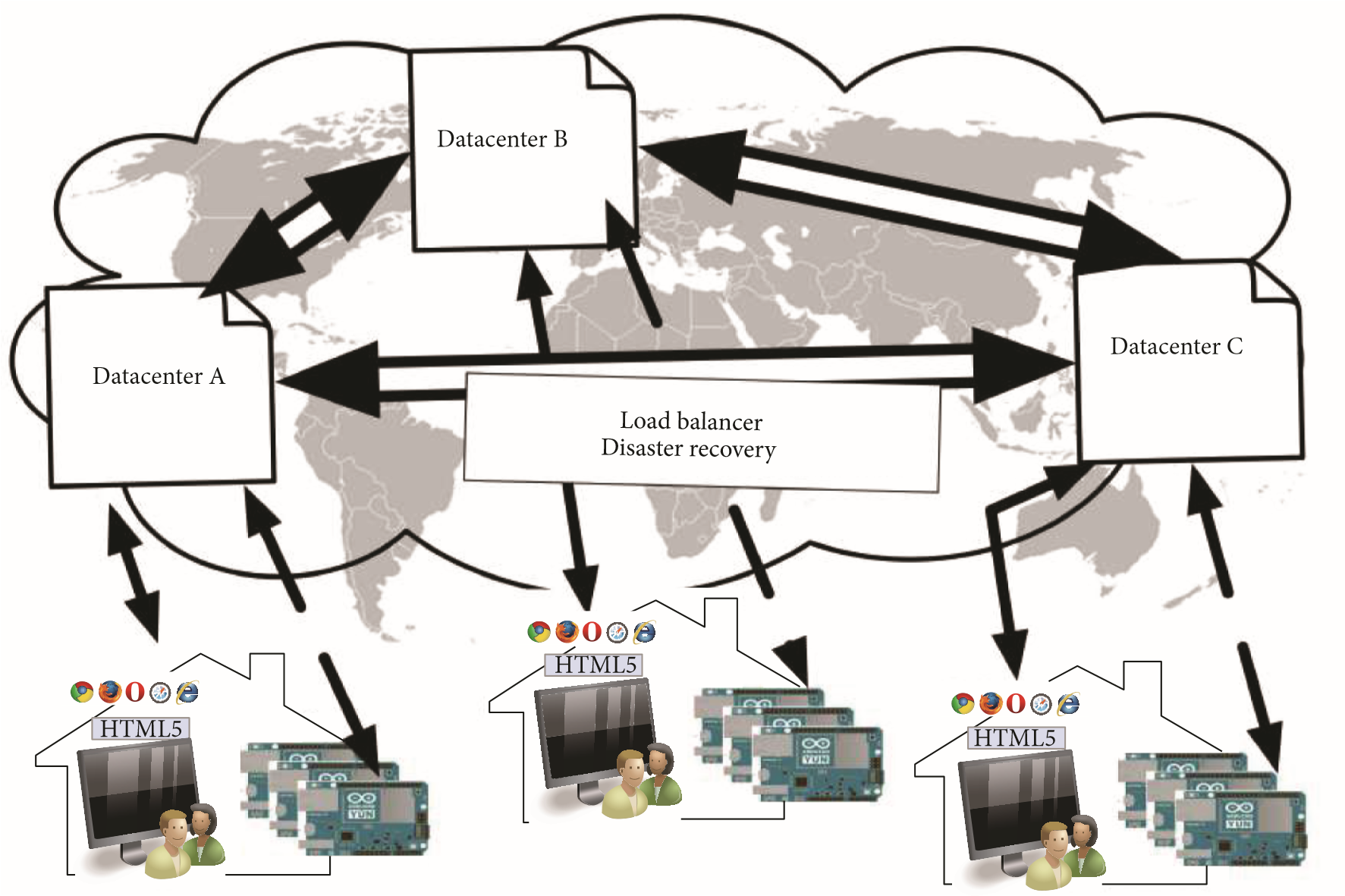
# Tác phẩm liên quan

Bảo mật trong IoT và điện toán đám mây là một chủ đề được thảo luận rộng rãi và hầu như không ảnh hưởng đến việc áp dụng và triển khai quy mô lớn và nhanh chóng các công nghệ đó [5, 6]. Trong [7], các tác giả điều tra các vấn đề và thách thức bảo mật trên SmartGrids(SG) dựa trên IoT và xác định các dịch vụ bảo mật chính cần được xem xét khi xử lý bảo mật SG. Một cách tiếp cận để quét đồng thời nhiều đối tượng IoT trong thời gian ngắn được trình bày trong [8]. Các tác giả trình bày khái niệm Bằng chứng Yoking Xác suất (PYP) và đưa ra ba tiêu chí chính để đánh giá hiệu suất liên quan: chi phí, bảo mật và tính công bằng. Đề xuất này kết hợp cấu trúc thông báo của các cấu trúc chứng minh nhóm cổ điển với quy trình lấy mẫu Poisson lặp trong đó xác suất mỗi đối tượng được lấy mẫu thay đổi theo thời gian. Cách tiếp cận phân phối khóa cho các ứng dụng y tế điện tử an toàn trong IoT được trình bày trong [9], trong đó các tác giả tiến hành xác nhận chính thức các thuộc tính bảo mật. Sơ đồ xác thực lẫn nhau an toàn cho hệ thống cấy ghép RFID được trình bày trong [10]. Các tác giả đề xuất một sơ đồ dựa trên mật mã đường cong elip và thiết kế băm nhẹ D-Quark. Thiết kế băm nhẹ D-Quark được thiết kế riêng cho các thiết bị phổ biến có hạn chế về tài nguyên, có tính đến chi phí và hiệu suất. Phân tích hiệu suất tính toán cho thấy giải pháp được đề xuất có chi phí truyền thông ít hơn 48% so với các sơ đồ tương tự hiện có. Trong [11], các tác giả đề xuất một hệ thống lưu trữ IoT an toàn và có thể mở rộng dựa trên sơ đồ chia sẻ bí mật đã được sửa đổi với sự hỗ trợ về khả năng mở rộng, tính linh hoạt và độ tin cậy ở cả cấp độ dữ liệu và hệ thống. Sơ đồ chia sẻ bí mật của Shamir được áp dụng để đạt được bảo mật dữ liệu mà không cần quản lý khóa phức tạp liên quan đến các thuật toán mã hóa truyền thống. Sơ đồ chia sẻ bí mật ban đầu được sửa đổi để sử dụng tất cả các hệ số trong đa thức để có dung lượng dữ liệu lớn hơn ở cấp độ dữ liệu. Trong [12], các tác giả đề xuất một cách tiếp cận để cung cấp các dịch vụ IoT an toàn bằng cách sử dụng Bảo mật lớp truyền tải dữ liệu (DTLS) làm giao thức bảo mật trên thực tế. Đặc biệt, họ đã xem xét các vấn đề trong việc áp dụng giao thức DTLS cho IoT, bao gồm các thiết bị và mạng bị hạn chế. Để giải quyết những vấn đề như vậy, họ tách giao thức DTLS thành *giai đoạn bắt tay* (tức là giai đoạn thiết lập) và *giai đoạn mã hóa* (tức là giai đoạn truyền). Tổng quan về những thách thức bảo mật chính trong các ứng dụng robot được hỗ trợ bởi IoT được trình bày trong [13], đặc biệt tập trung vào bảo mật mạng. Trong [14], các tác giả nghiên cứu khả năng hợp nhất điện toán đám mây linh hoạt và IoT an toàn trong các kịch bản Thành phố thông minh. Xem xét vấn đề tự cấu hình của các thiết bị IoT trong kịch bản Điện toán đám mây, trong [15], các tác giả trình bày một kiến trúc Đám mây IoT thú vị khai thác các thiết bị Arduino, trong khi đó, trong [16], các tác giả đề xuất cung cấp dịch vụ IoT bằng Điện toán đám mây hệ thống. Tuy nhiên, cả [15, 16] đều thiếu cơ chế tự cấu hình an toàn trong giai đoạn khởi động. Trên thực tế, chúng yêu cầu sự tương tác của con người và cấu hình ưu tiên của thiết bị. Trong bài viết này, chúng tôi cố gắng khắc phục khoảng cách này.

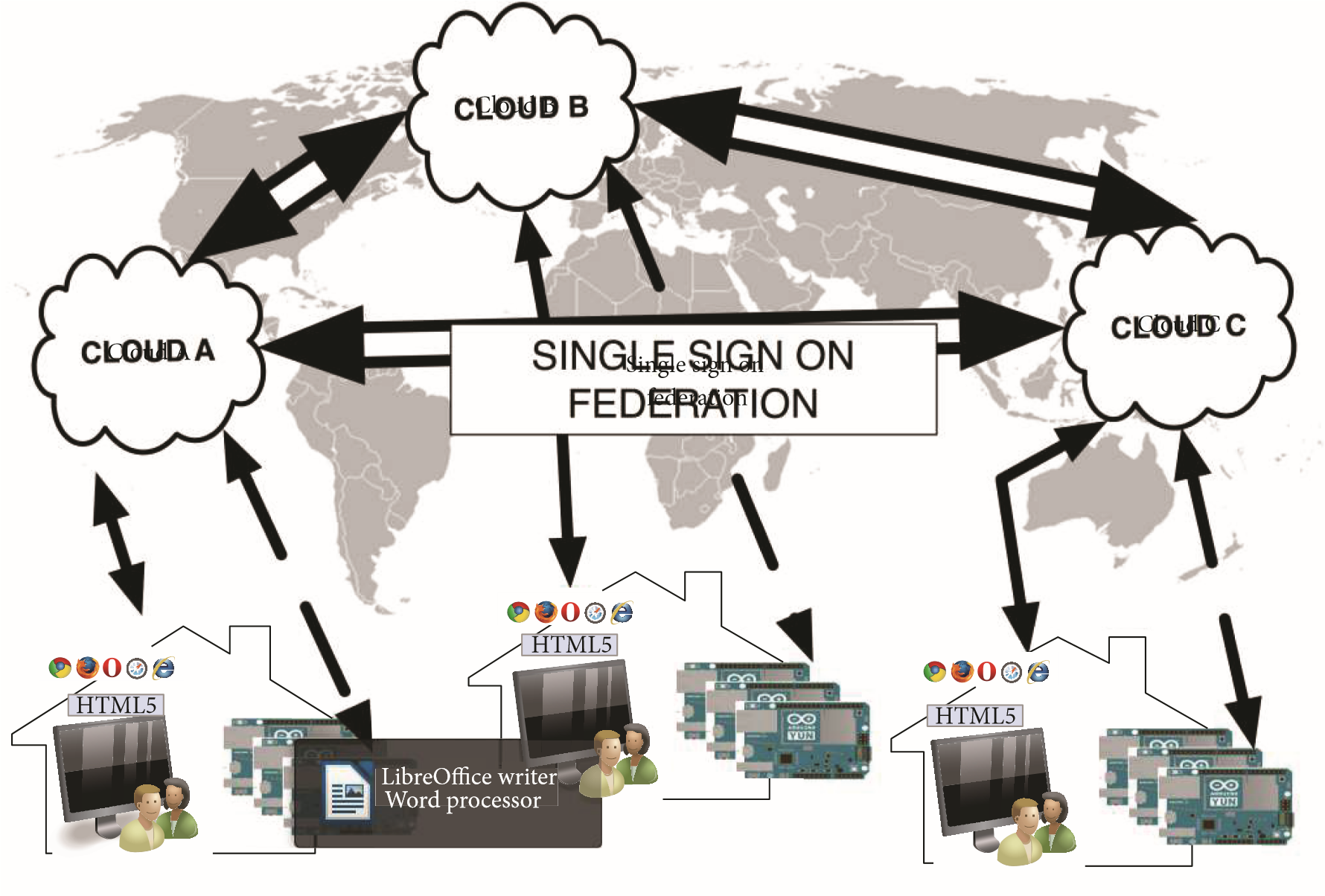
# Kịch bản đơn và đa đám mây cho IoT

Trong phần này, chúng tôi trình bày hai kịch bản đầy thách thức mà chúng tôi lần lượt xác định là “Một đám mây” và “Đa đám mây” [17] (xem Hình 1 và 2). Cả hai kịch bản đều bao gồm những người dùng khác nhau cầm một số thiết bị nhúng IoT được kết nối với Internet (ví dụ: thông qua mạng WiFi gia đình). Mỗi thiết bị có thể tự động cấu hình tải xuống cấu hình của nó từ một nhà cung cấp Đám mây nhất định. Như được hiển thị trong Hình 1, trong kịch bản Đám mây đơn, một số trung tâm dữ liệu thuộc về nhà điều hành Đám mây được trải rộng trên toàn thế giới. Ví dụ: trung tâm dữ liệu A được đặt ở Hoa Kỳ, trung tâm dữ liệu B được đặt ở Châu Âu và trung tâm dữ liệu C được đặt ở Châu Á. Mỗi trung tâm dữ liệu thu thập dữ liệu đến từ các thiết bị nhúng IoT được kết nối trong khu vực địa lý mà nó phục vụ.

Kịch bản Multicloud hiển thị trong Hình 2 khó khăn hơn nhiều so với kịch bản trước, vì các trung tâm dữ liệu thuộc về các nhà cung cấp Đám mây hợp tác khác nhau [18]. Trong ví dụ, Cloud B là nhà sản xuất thiết bị, trong khi Clouds A



Hình 1: Kịch bản Đám mây đơn với một nhà khai thác Đám mây được phân phối giữa nhiều trang web, thiết bị IoT và khách hàng hơn.



Hình 2: Kịch bản Multicloud với nhiều nhà khai thác Đám mây, thiết bị IoT và khách hàng hơn.

Hình 3: Arduino Yun mở rộng khả năng bảo mật.



ATmega

Rx

Rx

WiFi

interface

interface

ETH

Tx

Tx

Linino

USB

USB

Arduino environment

Linux environment

prog.

SD

card

hID (hidden ID)

Public key (CA)

Private key (CA)

(

compute on-board secure

operations)

host

AR 9331

32

u

4

Bridge

và C là nhà cung cấp dịch vụ IoT. Các đám mây A, B và C thiết lập mối quan hệ liên đoàn với mục tiêu cải thiện hoạt động kinh doanh của họ. Một câu hỏi thú vị là làm thế nào để thiết lập được thỏa thuận giữa các Đám mây này. Cloud B có thể cung cấp các loại dịch vụ khác nhau cho khách hàng của mình cũng như cho Cloud A và C cung cấp dịch vụ IoT. Ngoài ra, Cloud B có thể là đơn vị bên thứ ba chịu trách nhiệm chứng nhận tính tốt và độ tin cậy của các thiết bị IoT của mình. Một tình huống tương tự đã xảy ra trong Máy tính đáng tin cậy khi xem xét các Mô-đun nền tảng đáng tin cậy (TPM) được các nhà sản xuất xác nhận trong bo mạch chủ. Lúc đầu, Cloud A và B thỏa thuận về dịch vụ Đăng nhập một lần. Khi thiết bị nhúng IoT muốn truy cập Cloud A, thiết bị đó phải thực hiện xác thực trên Cloud B. Nếu xác thực thành công, Cloud A sẽ tin cậy Cloud B. Như vậy, Cloud A sẽ hoàn tất việc đăng ký cho thiết bị. Sau đó, Mây A và B thiết lập mối quan hệ liên bang. Để đạt được mục đích này, Cloud B (tức là nhà sản xuất thiết bị) theo dõi từng thiết bị nhúng IoT về phiên bản chương trình cơ sở, báo cáo lỗi, v.v., do đó có thể xác thực thiết bị mà không cần biết cũng như vị trí thực của thiết bị cũng như chủ sở hữu của nó. Cloud A (tức là nhà cung cấp dịch vụ IoT) có thể được thông báo từ Cloud B. Cloud B cần nhận dạng thiết bị mà không cần trao đổi dữ liệu của người dùng và địa chỉ Media Access Control (MAC) của thiết bị.

Trong Hình 2, thỏa thuận liên kết cho SSO có thể được mở rộng hơn nữa khi triển khai các cơ chế bổ sung về khả năng tương tác giữa các Đám mây. Theo kịch bản tham chiếu, mỗi người dùng thu thập dữ liệu đến từ các thiết bị IoT nhúng của mình bằng cổng web của Đám mây và lưu trữ chúng vào Đám mây. Để quản lý dữ liệu lớn như vậy, các loại thông tin khác nhau từ các nhà cung cấp khác nhau phải được xử lý. Ví dụ: để cung cấp dịch vụ liền mạch cho người dùng, Đám mây A và B phải quản lý các thông tin sau:

1. Thông tin thiết bị trên Cloud B.
2. Thông tin xác thực, ủy quyền và kế toán của người dùng trên Cloud B.
3. Cấu hình thiết bị để thiết lập ban đầu trên Cloud A.
4. Cấu hình thiết bị cho các hoạt động trong vòng đời của Cloud A.
5. Các thiết bị đã cảm nhận được dữ liệu trên Đám mây A.

Để lưu trữ và quản lý tất cả những dữ liệu này theo cách có thể mở rộng, mọi Đám mây phải lưu trữ một cơ sở dữ liệu phân tán cục bộ. Trong cấu hình chia sẻ và cơ hội của Đám mây thuộc một liên kết, cũng có thể nghĩ về cơ sở dữ liệu toàn cầu được phân bổ giữa các miền liên kết khác nhau, hoạt động như một danh mục lớn toàn cầu chứa thông tin cho người dùng và thiết bị (đăng nhập, khóa, mã, ID , kho lưu trữ MAC, v.v.).

# Hướng tới việc tự nhận dạng an toàn các thiết bị IoT

Trong phần này, chúng tôi thảo luận về cách các thiết bị nhúng IoT hiện có có thể được mở rộng và sử dụng để thực hiện quá trình tự nhận dạng trong các tình huống được mô tả trước đây. Cụ thể, các thiết bị IoT phải được cài đặt sẵn khóa bảo mật, thuật toán mã hóa và ID ẩn (hID). Vì vậy, chúng tôi phân tích một nền tảng IoT nổi tiếng, đó là Arduino Yun, để thảo luận về tính hiệu quả của cơ chế tự nhận dạng.

*4.1. Arduino Yun.* Khung phần cứng mở Arduino là một kiến trúc hợp nhất có thể đáp ứng các yêu cầu của IoT, đặc biệt là vì tính rẻ tiền và dễ sử dụng. Nhiều phiên bản, tấm chắn và phần mở rộng tồn tại trên thị trường dành cho nền tảng Arduino. Trong số đó, Arduino Yun là framework có thể cung cấp các khả năng của Arduino cùng với các tính năng nhúng của Linux. Cụ thể, Yun khác với các bo mạch Arduino khác vì bộ điều khiển ATmega giao tiếp với bộ xử lý Atheros AR9331 . Cái sau hỗ trợ bản phân phối Linux dựa trên OpenWRT có tên Linino, cung cấp một máy tính nối mạng mạnh mẽ với sự dễ dàng của Arduino.

Hình 3 cho thấy kiến trúc Yun. Phía bên trái của hình ảnh mô tả phần Arduino, trong khi ở bên phải là phần Linino được hiển thị. Yun có bo mạch WiFi/Ethernet tích hợp cung cấp khả năng liên lạc. Trong trường hợp của chúng tôi, Linino có thể được sử dụng để thực hiện các tính năng bảo mật và thực hiện các tương tác với Đám mây. Đặc biệt, Webclient (tức là Curl), ứng dụng khách XMPP, Python và OpenSSL có thể dễ dàng phát triển trên thiết bị này để tương tác với các thiết bị khác và với Đám mây một cách an toàn.

*4.2. Khóa bảo mật, thuật toán mã hóa và ID ẩn.* Để đạt được các kịch bản được thảo luận trong Phần 3, một thiết bị IoT như Arduino Yun phải được nhà sản xuất trang bị một thành phần mới được gắn trên bo mạch và cung cấp một số khả năng bảo mật. Đặc biệt, các khả năng bảo mật này phải bao gồm các khóa bảo mật (ví dụ: một vài khóa chung/riêng dựa trên X509v3 (𝐾 pub , 𝐾 priv ) ), thuật toán mã hóa và ID ẩn (hID). HID là số thứ tự được nhà sản xuất sử dụng để nhận dạng từng bảng. Nó bị ẩn đi vì không ai được phép đọc nó. Ở đây, chúng tôi đã giới thiệu khái niệm ID bị xáo trộn (obH) bắt nguồn từ hàm băm MD5. Thuộc tính chính của hàm băm là tính không thể chối cãi của nó; trên thực tế, nó cũng được định nghĩa là hàm một chiều (tức là từ đầu ra của hàm băm không thể khấu trừ đầu vào). Do đó, obH rất hữu ích để theo dõi các bảng ẩn thông tin về địa chỉ MAC công cộng và chủ sở hữu bảng:

obH = hàm băm ( hID , MAC ). (1)

obH đại diện cho một chỉ mục bảng không cung cấp thông tin nhạy cảm trên bảng và do đó, có thể được lưu trữ trong bất kỳ cơ sở dữ liệu công cộng nào. Trong mọi giao tiếp giữa thiết bị và nhà điều hành Đám mây (ví dụ: Cloud A trong Hình 2), Thông báo ( 𝑀 ) phải được đưa vào nội dung của tất cả các giao tiếp kết nối obH, MAC và khóa chung 𝐾 pub để triển khai liên lạc an toàn. Coi như

𝑀 = concat ( obH , MAC , 𝐾 pub ) . (2)

Cơ chế chữ ký dựa trên khóa công khai 𝐾 pub đảm bảo độ tin cậy của người gửi. 𝐾 pub được Cơ quan chứng nhận (CA) của nhà sản xuất thiết bị IoT chỉ định ở giai đoạn sản xuất. Ngược lại, khóa riêng 𝐾 bí mật không thể truy cập được từ bên ngoài từ chip nhúng trong thiết bị, nhưng nó có thể được sử dụng bởi các thuật toán bảo mật nội bộ:

SM = chữ ký (𝐾 riêng tư , 𝑀) . (3)

*4.3. Thêm khả năng phần cứng an toàn.* Máy tính đáng tin cậy (TC), được xác định bởi Nhóm máy tính đáng tin cậy (TCG) [19], kết hợp các cơ chế bảo mật phần cứng và phần mềm để nâng cao mức độ bảo mật của môi trường máy tính. Mục tiêu chính của TC là cung cấp khả năng bảo mật mạnh mẽ hơn các hệ thống bảo mật dựa trên phần mềm truyền thống và thực thi tính toàn vẹn của hệ thống khi nó tương tác với các hệ thống khác. Đặc điểm nổi bật của TC là sự kết hợp của Roots of Trust (RoT) nhằm thực hiện các chức năng cụ thể theo cách an toàn, chẳng hạn như đo lường, lưu trữ, báo cáo, xác minh và/hoặc cập nhật. TC ngụ ý việc sử dụng chip phần cứng có tên là Mô-đun nền tảng đáng tin cậy (TPM) có khả năng cung cấp RoT và mở rộng niềm tin đến các bộ phận khác của thiết bị bằng cách xây dựng chuỗi tin cậy. Nó cung cấp các phương tiện để tạo khóa mật mã an toàn và có khả năng thực hiện xác thực nền tảng, vì mỗi chip TPM có một khóa RSA bí mật và duy nhất được ghi vào khi nó được tạo ra (tức là Khóa xác thực (EK)). TPM bao gồm các khả năng như xác thực máy, mã hóa phần cứng, ký, lưu trữ khóa an toàn và chứng thực. Sinh ra để bảo mật Máy tính cá nhân truyền thống, TCG hiện đang xem xét cả thiết bị nhúng và thiết bị di động có bản dự thảo đặc tả kiến trúc tham chiếu lần lượt được phát hành vào tháng 4 và tháng 6 năm 2014. Các thông số kỹ thuật này cung cấp hướng dẫn về cách tích hợp TPM trong thiết bị ngay cả khi vẫn chưa có nhiều triển khai trên các thiết bị phần cứng thực sự. TC và các hệ thống nhúng đang ở giai đoạn đầu; tuy nhiên, theo quan điểm của chúng tôi, TC là một giải pháp hợp lý để phát triển khả năng bảo mật phần cứng trong các thiết bị IoT tương tác với Đám mây.

# Kiến trúc dựa trên đám mây IoT

Trong phần này, chúng tôi mô tả kiến trúc dựa trên Đám mây IoT có thể hỗ trợ việc tự nhận dạng trên các liên lạc an toàn, như được mô tả trong các phần trước. Để đạt được mục đích này, chúng tôi đặc biệt đề cập đến Môi trường ảo hỗ trợ đám mây (CLEVER), Phần mềm trung gian hướng thông báo (MOM) an toàn có thể hỗ trợ các dịch vụ Đám mây liên kết được phát triển trong phòng thí nghiệm oru [20]. CLEVER thiết lập hệ thống Đám mây có thể quản lý cả dịch vụ cảm biến và ảo hóa bằng giao thức XMPP. Ngoài ra, phần mềm trung gian hỗ trợ quản lý dữ liệu lớn thông qua cơ sở dữ liệu NoSQL MongoDB. Hình 4 cho thấy kiến trúc dựa trên Đám mây IoT của chúng tôi hỗ trợ cả kịch bản Đám mây đơn và Nhiều đám mây. Cơ sở hạ tầng cần dựa vào nền tảng ảo hóa để đảm bảo mức độ linh hoạt và đàn hồi cao thông qua Máy ảo (VM). Tất cả các Máy vật lý (PM) đều được trang bị một phần mềm trung gian CLEVER để quản lý cụm. Hình tròn có nhãn A đại diện cho cụm nơi các phiên bản ảo của dịch vụ IoT được dùng bữa trưa. Đám mây nhằm mục đích duy trì giải pháp hiện tại cũng như quản lý khách hàng. Trong phiên bản phân tán của MongoDB, thông tin về IoT obH, trạng thái thiết bị (ví dụ: phiên bản chương trình cơ sở, tiện ích bổ sung tích hợp) và dữ liệu thu thập được trên thiết bị sẽ được lưu trữ. Máy chủ XMPP thiết lập các kênh bus hai chiều. Hình elip có nhãn B làm nổi bật việc thực thi một số VM thành một PM. Mỗi VM chứa các dịch vụ khác nhau và tương tác với các khách hàng và thiết bị khác nhau. Các hình dạng có nhãn C và D hiển thị các dịch vụ có thể có, chẳng hạn như dịch vụ Apache, MySQ, PHP, VM có phiên bản tối thiểu của CLEVER, máy chủ XMPP và MongoDB. Hình dạng D biểu thị một thùng chứa trong đó dữ liệu được cảm nhận được lưu trữ và giới hạn bên trong VM. Nhiều IoT, có máy khách XMPP, được gán động (sau lần liên hệ đầu tiên với máy khách web an toàn) cho máy chủ XMPP được triển khai trong VM. Nhiều khách hàng (kể từ khi có IoT của họ) có thể dựa vào cùng một VM. Dịch vụ này có thể mở rộng quy mô lên xuống tùy theo số lượng khách hàng và IoT. Hình C đại diện cho dịch vụ cổng web chính được sử dụng cho khách hàng và để tạo liên kết Người dùng MAC. Thậm chí nó có thể mở rộng quy mô lên xuống tùy theo số lượng khách hàng.

|  |
| --- |
| Hình 4: Ví dụ về nhà sản xuất thiết bị IoT quản lý trung tâm dữ liệu của riêng mình bằng kiến trúc của chúng tôi. Hình minh họa cho thấy một số máy khách web và thiết bị IoT được mở rộng với khả năng bảo mật tương tác với hệ thống Đám mây được bố trí bằng CLEVER. |

*5.1. Sắp xếp hệ thống đám mây bằng CLEVER.* Như được mô tả trong Hình 5, mỗi cụm CLEVER bao gồm một số PM được tổ chức trong một cụm. Mỗi PM được điều khiển bởi một mô-đun quản lý, được gọi là Trình quản lý máy chủ (HM) và chỉ một PM chạy mô-đun quản lý cụm, được gọi là Trình quản lý cụm (CM). CM đóng vai trò là giao diện giữa các máy khách Đám mây (ví dụ: IoT, ứng dụng, dịch vụ web và người dùng cuối khai thác tài nguyên Đám mây) và các tác nhân phần mềm chạy trên PM. CM nhận lệnh từ khách hàng, đưa ra hướng dẫn cho HM, xây dựng thông tin và cuối cùng gửi lại kết quả cho chính khách hàng. Nó cũng thực hiện các nhiệm vụ quản lý tài nguyên Đám mây và giám sát trạng thái hoạt động của cụm. Một CM được bầu trong số tất cả các HM sử dụng *giao thức tự bầu cử phân tán* và nó hoạt động ở chế độ HOẠT ĐỘNG. CM thứ hai cũng được chọn làm dự phòng nhưng được cấu hình ở chế độ GIÁM SÁT. CM GIÁM SÁT không tham gia vào việc quản lý cụm nhưng nó giữ một bản sao được đồng bộ hóa về trạng thái bên trong của CM HOẠT ĐỘNG; do đó, nó có thể thiết lập tất cả các dịch vụ đang hoạt động nếu CM HOẠT ĐỘNG bị lỗi. Để làm cho luận án của chúng tôi dễ dàng hơn, từ nay trở đi, chúng tôi gọi CM HOẠT ĐỘNG chỉ là CM.

Giao tiếp giữa các thành phần phân tán trong Đám mây CLEVER dựa trên XMPP do tính linh hoạt và mức độ phản hồi cao của nó. Máy chủ Jabber/XMPP cung cấp các tính năng nhắn tin, hiện diện và định tuyến XML cơ bản trong Đám mây. Tất cả các PM trong Đám mây được kết nối thông qua Trò chuyện nhiều người dùng (MUC) có nhãn *Phòng chính* và hợp tác theo chỉ thị điều phối CM. MUC, được xác định là *Shell Room* , cho phép khách hàng gửi yêu cầu của họ và nhận dịch vụ. Do kiến trúc dựa trên cụm của CLEVER, chỉ CM và khách hàng mới có thể truy cập Shell Room. Hai kênh liên lạc này được hiển thị trong Hình 5 dưới dạng các đường màu đen dày.

Để thiết lập một liên kết, các CM thuộc các Đám mây khác nhau sẽ trao đổi tin nhắn thông qua MUC được xác định là *Phòng Liên kết* và chỉ các CM của các Đám mây được liên kết mới truy cập được. GIÁM SÁT CM không thể vào Phòng Liên đoàn vì họ không trực tiếp tham gia quản lý tài nguyên.

Máy chủ XMPP cần thiết để thiết lập liên kết và do đó để quản lý Phòng Liên kết có thể được ủy thác bởi một thực thể bên thứ ba, tổ chức này sẽ thiết lập Máy chủ Jabber từ miền của các nhà cung cấp Đám mây, chỉ để đáp ứng các yêu cầu liên kết. Vì MUC chỉ có thể được truy cập bởi các thành phần trong các miền liên kết nên cần phải kiểm tra thông tin xác thực của chúng. Để tránh cấu hình tĩnh ưu tiên của các tài khoản vào máy chủ XMPP, tổ chức bên thứ ba phải xác thực thông tin xác thực thành phần. Để đạt được mục đích này, XMPP federationcapabilitiescanbeexploited. Thực thể bên thứ ba không cần duy trì thông tin xác thực của tất cả các CM liên quan đến liên kết, nhưng thỏa thuận tin cậy giữa tất cả các Máy chủ Jabber cho phép thiết lập một liên kết XMPP trong đó thông tin xác thực của các thành phần được xác minh bởi ít nhất một Máy chủ Jabber (mã thông báo).

*5.2. Tương tác của thiết bị IoT với đám mây: Phương pháp tiếp cận kết hợp.* Trong phần này, chúng tôi thảo luận về cách tiếp cận kết hợp để cho phép thiết bị IoT tương tác với hệ thống Đám mây, chẳng hạn như được sắp xếp bằng CLEVER. Để mô tả các phương pháp tương tác, chúng tôi đề cập đến hai trường hợp có thể xảy ra.

*Trường hợp 1.* Chúng tôi xem xét kịch bản “đơn giản hóa”, trong đó nhà sản xuất thiết bị trùng với nhà điều hành Đám mây (tức là Đám mây B); do đó, nó có toàn quyền kiểm soát bảng mạch bằng giao tiếp XMPP hai chiều.

|  |
| --- |
| Hình 5: Kiến trúc CLEVER. |

*Trường hợp 2.* Chúng tôi xem xét kịch bản “thử thách”, trong đó nhà sản xuất thiết bị (tức là Cloud B) đưa ra thỏa thuận đầy đủ rõ ràng với nhà cung cấp dịch vụ Iot (tức là Cloud A) và cả hai đều thuộc liên đoàn Đám mây. Trong trường hợp này, Cloud B cung cấp Plaftorm dưới dạng Dịch vụ (PaaS) này cho các Đám mây khác (máy chủ XMPP, hệ thống xác thực, cơ sở dữ liệu NoSQL, v.v.). Hai phòng trò chuyện được cấu hình sẵn giữa máy khách XMPP của thiết bị IoT và máy khách XMPP của nhà cung cấp Đám mây: phòng đầu tiên được sử dụng để triển khai chương trình cơ sở và quản lý lỗi. Nhà sản xuất thiết bị (tức là Cloud B) sử dụng hệ thống liên lạc như vậy để liên lạc với thiết bị IoT. Cloud A có thể tham gia giao tiếp này. Phòng trò chuyện thứ hai được sử dụng để gửi dữ liệu được cảm nhận: nhà cung cấp dịch vụ IoT (tức là Đám mây A) là một hệ thống liên lạc như vậy cho mục đích của nó, nhưng Đám mây B không thể nghe thấy liên lạc nếu sử dụng kênh được mã hóa.

Phương pháp tương tác kết hợp này bao gồm hai loại máy khách khác nhau chạy trên các thiết bị IoT hoạt động ở các giai đoạn khác nhau: máy khách web để liên lạc RestFul an toàn và máy khách XMPP để liên lạc hai chiều.

1. *Máy khách web RESTFul* . Ý tưởng chính là sử dụng máy khách web sau lần liên kết đầu tiên của thiết bị IoT với mạng WiFi gia đình. Do đó, máy khách web truy cập Internet và liên hệ với máy chủ web mặc định của nhà cung cấp Đám mây bằng giao thức https. Thiết bị IoT, chẳng hạn như Arduino Yun của chúng tôi, sử dụng khóa riêng của nó để thực hiện quy trình phản hồi thử thách để thực hiện xác thực lẫn nhau SSL với máy chủ web và nếu thành công, thiết bị IoT sẽ gửi tin nhắn 𝑀 (xem (2) trong Phần 4.2 ) trong nội dung của tài liệu JSON tới máy chủ web. Do đó, thiết bị IoT được nhận dạng và liên kết với dịch vụ.

Máy khách web bảo mật chỉ được sử dụng ở phần đầu cho kịch bản đơn giản hóa. Sau đó tin nhắn 𝑀 được gửi; máy chủ web trên Đám mây của nhà sản xuất nắm quyền điều khiển thiết bị IoT và có thể thực hiện các hành động tiếp theo bằng giao thức XMPP.

1. *Ứng dụng khách XMPP* . Nó cho phép đơn giản hóa sự tương tác giữa thiết bị IoT và một số nhà cung cấp Đám mây, đặc biệt là trong “kịch bản đầy thách thức”. Xem xét kịch bản như vậy, chúng ta hãy giả sử rằng CloudA (nhà cung cấp dịch vụ IoT) cần thiết lập hai yếu tố, đó là thẻ SD để cắm vào thiết bị IoT và dịch vụ web. Thẻ SD chứa dữ liệu để truy cập vào Đám mây A (ví dụ: URI và chứng chỉ công khai của CA). Dịch vụ web có thể thực hiện xác thực SSO, chuyển hướng yêu cầu tới Đám mây B để nhận mã thông báo xác thực. Do đó, Cloud B (nhà sản xuất thiết bị) và Cloud A (nhà cung cấp dịch vụ IoT) đều chịu trách nhiệm hoàn thiện bước nhận dạng thiết bị sớm. Giao thức XMPP ban đầu được thiết kế để quản lý hiệu quả các tin nhắn giữa các thiết bị ngang hàng trên Internet. Bản chất của XMPP cho phép truy cập Internet một cách minh bạch, sử dụng cơ chế xuyên tường lửa mà không cần bất kỳ sự can thiệp nào của người dùng, thiết lập liên lạc hai chiều. Nó dựa trên tiêu chuẩn XML; do đó, việc mở rộng để thực thi các cơ chế bảo mật và ký kết khá đơn giản. Ngoài ra, có thể thực hiện chữ ký và mã hóa các thông điệp XML bằng cách sử dụng khóa chung/riêng. Bất kỳ thiết bị nào có ngăn xếp OpenSSL đều có thể sử dụng các chức năng như vậy. Máy khách XMPP bắt đầu thực thi; sau đó, sự tương tác của máy khách web kết thúc thành công. Ứng dụng khách XMPP này có thể được sử dụng cả trong các tình huống đơn giản hóa và đầy thử thách.

# Chiến lược đăng ký thiết bị IoTTham gia đám mây

Ví dụ: thiết bị IoT, Arduino Yun được mở rộng với khả năng bảo mật, có thể thực hiện theo hai phương thức đăng ký khác nhau:

1. Không giám sát: tự động đăng ký địa chỉ MAC và obH.
2. Được giám sát: đăng ký web của người dùng cuối về địa chỉ MAC và obH.

Trong cả hai trường hợp, người dùng cuối cần kích hoạt thiết bị IoT (ví dụ: bo mạch Arduino Yun) để duy trì liên kết mạng WiFi bằng nút wps trên AP không dây của mình. Do đó, thiết bị IoT có thể truy cập Internet bằng cách thực hiện xác thực như mô tả trong Phần 4. Trong trường hợp được giám sát, bo mạch thiết bị IoT sẽ nhấp nháy đèn LED màu cam và sau khi đăng ký một phần, bảng mạch này sẽ hiển thị đèn LED cố định màu cam. Việc đăng ký đầy đủ đạt được khi người dùng cuối liên kết bo mạch thiết bị IoT với hồ sơ web của họ. Người dùng sử dụng một trang web để đăng ký bo mạch, cụ thể là gõ địa chỉ MAC hiển thị ở phần bên ngoài của hộp do nhà sản xuất cung cấp. Nếu MAC trong 𝑀 khớp với MAC được nhập trên trang web, bảng sẽ nhấp nháy đèn LED màu xanh lục và người dùng có thể xác nhận thao tác; nếu không (không có đèn LED nhấp nháy), anh ấy/cô ấy nên lặp lại quy trình. Sau đó, quá trình đăng ký đầy đủ đã được hoàn tất và bảng hiển thị đèn LED cố định màu xanh lục. Giờ đây Đám mây có toàn quyền kiểm soát bo mạch, do đó nó có thể triển khai chương trình cơ sở, quản lý cấu hình, cài đặt phần mềm, v.v. Người dùng chỉ nhấn một nút (wps) và nhập mã vào trang web của nhà điều hành Cloud.

Giải pháp được đề xuất có thể đi theo hai nhánh phiên bản chính. Phiên bản đầu tiên bị ràng buộc chặt chẽ với nhà sản xuất thiết bị (tức là Cloud B) chịu trách nhiệm về các nhiệm vụ sau: (i) lập trình trước thiết bị IoT, (ii) cập nhật chương trình cơ sở và (iii) phát hành ứng dụng mới. Phiên bản thứ hai xem xét các tình huống trong đó nhà sản xuất thiết bị chịu trách nhiệm về nhiệm vụ (i), trong khi các nhà cung cấp dịch vụ IoT khác (ví dụ: Clouds A và C) có thể xử lý các nhiệm vụ 2 và 3. Những nhiệm vụ này có thể thực hiện được nếu Cloud Các nhà cung cấp dịch vụ IoT thiết lập một thỏa thuận với Đám mây đóng vai trò là nhà sản xuất thiết bị. Đám mây đóng vai trò là nhà sản xuất thiết bị IoT phải trang bị thẻ SD cho thiết bị IoT để đạt được kịch bản như vậy. Do đó, ý tưởng của chúng tôi là tận dụng khái niệm Đăng nhập một lần để cho phép thiết bị đăng ký với nhà cung cấp dịch vụ Cloud IoT, tương tác với Đám mây đóng vai trò là nhà sản xuất thiết bị IoT. Khi thiết bị IoT có thể thiết lập kết nối, nó sẽ liên hệ với nhà cung cấp dịch vụ Cloud IoT; do đó, dịch vụ của nó thực hiện chuyển hướng đến nhà sản xuất thiết bị Cloud IoT đóng vai trò là nhà cung cấp danh tính để xác minh thông báo obH bằng chữ ký của nó. Nếu nhà sản xuất Đám mây nhận ra thiết bị, nó sẽ phát hành mã thông báo; do đó, nhà cung cấp dịch vụ CloudIoT có thể hoàn tất đăng ký không giám sát. Việc đăng ký có giám sát được thực hiện bởi người dùng cuối, những người ban đầu có thể thực hiện theo cách tiếp cận tương tự. Để thực hiện kịch bản này, nhà cung cấp dịch vụ Cloud IoT cần đạt được thỏa thuận rõ ràng với nhà sản xuất thiết bị Cloud IoT để hiểu cách tương tác với nhau. Thông báo obH không thể cho phép nhà sản xuất thiết bị Cloud biết thông tin chi tiết về bo mạch. Tuy nhiên, nó có thể theo dõi trạng thái chung, phiên bản chương trình cơ sở, lỗi, v.v.

# Phần kết luận

Trong bài viết này, chúng tôi đã thảo luận về cách tiếp cận tích hợp IoT với điện toán đám mây. Đặc biệt, một hệ thống được trình bày để phân tích các yếu tố khác nhau có liên quan và cách chúng tương tác với nhau. Ví dụ: sử dụng Arduino Yun, chúng tôi đã thảo luận về cách các thiết bị IoT có thể được mở rộng để hỗ trợ tương tác với Đám mây. Đặc biệt, chúng tôi tập trung vào một hệ thống cho phép nhà cung cấp Đám mây triển khai chương trình cơ sở và định cấu hình thiết bị, đồng thời một mặt thực hiện truyền dữ liệu được cảm nhận từ thiết bị sang nhà cung cấp Đám mây. Cuối cùng, chúng tôi đã thảo luận về cách hoạt động của toàn bộ hệ thống, đồng thời trình bày hai kịch bản Đám mây có thể xảy ra. Hiện tại, các thiết bị IoT đang ở giai đoạn đầu và như đã thảo luận trong bài viết này, chúng vẫn chưa sẵn sàng hỗ trợ các kịch bản Đám mây phức tạp, mặc dù lộ trình hướng tới các dịch vụ Cloud IoT đổi mới đã bắt đầu được theo dõi.

# Xung đột lợi ích

Các tác giả tuyên bố rằng không có xung đột lợi ích liên quan đến việc xuất bản bài viết này.

# Nhìn nhận

Nghiên cứu này được hỗ trợ bởi dự án BEACON của Chương trình Nghiên cứu và Đổi mới Horizon 2020 của Liên minh Châu Âu theo Thỏa thuận tài trợ số. 644048.

# Người giới thiệu

1. M. Fazio và A. Puliafito, “Cloud4sens: kiến trúc dựa trên đám mây để kiểm soát và giám sát cảm biến,” *Tạp chí Truyền thông IEEE* , tập. 53, không. 3, trang 41–47, 2015.
2. Giải phóng tiềm năng của Internet trong tương lai và điện toán đám mây, tháng 11 năm 2013, https://ec.europa.eu/digital-agenda/en/news/ ununting-potential-future-internet-and-cloud-computing.
3. M. Villari, A. Celesti, M. Fazio và A. Puliafito, “AllJoyn Lambda: kiến trúc để quản lý môi trường thông minh trong IoT,” trong *Kỷ yếu của Hội nghị Quốc tế về Hội thảo Điện toán Thông minh (SMARTCOMP '14)* , trang . 9–14, Hồng Kông, tháng 11 năm 2014.
4. M. Villari, A. Celesti, M. Fazio và A. Puliafito, “Cơ chế tự nhận dạng an toàn để cho phép các thiết bị IoT tham gia điện toán đám mây” trong *Internet of Things. Cơ sở hạ tầng IoT* , R. Giaffreda, D. Cagov, Y. Li, R. Riggio và A. Voisard, Eds., tập. 151 trong *Bài giảng của Viện Khoa học Máy tính, Tin học Xã hội và Kỹ thuật Viễn thông* , trang 306–311, Springer, Berlin, Đức, 2015.
5. YH Hwang, “Bảo mật và quyền riêng tư của IoT: các mối đe dọa và thách thức,” trong *Kỷ yếu của Hội thảo ACM lần thứ nhất về Quyền riêng tư, sự tin cậy và bảo mật của IoT (IoTPTS '15)* , tr. 1, ACM, Singapore, tháng 4 năm 2015.
6. Z.-K. Zhang, MCY Cho và S. Shieh, “Các mối đe dọa bảo mật mới nổi và các biện pháp đối phó trong IoT,” trong *Kỷ yếu của Hội nghị chuyên đề ACM lần thứ 10 về An ninh Thông tin, Máy tính và Truyền thông (ASIA CCS '15)* , trang 1–6, ACM, Singapore , tháng 4 năm 2015.
7. C. Bekara, “Các vấn đề và thách thức về bảo mật đối với lưới điện thông minh dựa trên iot,” *Khoa học máy tính Procedia* , tập. 34, trang 532–537, 2014.
8. JM de Fuentes, P. Peris-Lopez, JE Tapiador và S. Pastrana, “Bằng chứng về ách xác suất cho các hệ thống IoT quy mô lớn,” *Ad Hoc Networks* , tập. 32, trang 43–52, 2015.
9. MR Abdmeziem và D. Tandjaoui, “Giao thức quản lý khóa an toàn từ đầu đến cuối cho các ứng dụng y tế điện tử,” *Máy tính & Kỹ thuật Điện* , tập. 44, trang 184–197, 2015.
10. SR Moosavi, E. Nigussie, S. Virtanen và J. Isoaho, “Một sơ đồ xác thực lẫn nhau dựa trên đường cong elip cho các hệ thống cấy ghép RFID,” *Khoa học máy tính Procedia* , tập. 32, trang 198–206, 2014. [11] H. Jiang, F. Shen, S. Chen, K.-C. Li và Y.-S. Jeong, “Một hệ thống lưu trữ an toàn và có thể mở rộng cho dữ liệu tổng hợp trong IoT,” *Hệ thống máy tính thế hệ tương lai* , tập. 49, trang 133–141, 2015.
11. N. Kang, J. Park, H. Kwon và S. Jung, “ESSE: thiết lập phiên an toàn hiệu quả cho các mạng cảm biến không dây tích hợp internet,” *Tạp chí Quốc tế về Mạng Cảm biến Phân tán* , tập. 2015, ID bài viết 393754, 11 trang, 2015.
12. LA Grieco, A. Rizzo, S. Colucci và cộng sự, “Các ứng dụng robot được hỗ trợ IoT: ý nghĩa công nghệ, miền mục tiêu và các vấn đề mở,” *Truyền thông Máy tính* , tập. 54, trang 32–47, 2014.
13. G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran và V. Suciu, “Các thành phố thông minh được xây dựng trên điện toán đám mây linh hoạt và kết nối Internet an toàn,” trong *Kỷ yếu của Hội nghị quốc tế lần thứ 19 về Hệ thống điều khiển và Khoa học máy tính (CSCS '13)* , trang 513–518, Bucharest, Romania, tháng 5 năm 2013.
14. AA Chandra, Y. Lee, BM Kim, SY Maeng, SH Park và SRLee, “Reviewonsensorcloudanditsintegrationwitharduino dựa trên mạng cảm biến,” trong *Kỷ yếu của Hội nghị quốc tế lần thứ 3 về hội tụ và bảo mật CNTT (ICITCS '13)* , Macao, Trung Quốc, tháng 12 năm 2013 .
15. MS Aslam, S. Rea và D. Pesch, “Cung cấp dịch vụ cho đám mây WSN,” trong *Kỷ yếu của Hội nghị quốc tế lần thứ 5 của IEEE về Điện toán đám mây (CLOUD '12)* , trang 962–969, tháng 6 năm 2012.
16. A. Panarello, A. Celesti, M. Fazio, M. Villari và A. Puliafito, “Phân tích yêu cầu cho liên đoàn đám mây iaas,” trong *Kỷ yếu của Hội nghị quốc tế lần thứ 4 về Khoa học dịch vụ và điện toán đám mây (CLOSER '14)* , Setubal, Bồ Đào Nha, tháng 4 năm 2014.'
17. M. Fazio, A. Celesti, M. Villari và A. Puliafito, “Sự cần thiết của phương pháp lưu trữ kết hợp cho IoT trong liên đoàn đám mây PaaS,” trong *Kỷ yếu của Hội nghị quốc tế IEEE lần thứ 28 về Hội thảo ứng dụng và mạng thông tin nâng cao (WAINA '14)* , trang 779–784, Victoria, Canada, tháng 5 năm 2014.
18. Nhóm máy tính đáng tin cậy (TCG), http://www.trustedcomputinggroup.org/.
19. A. Celesti, M. Fazio và M. Villari, “SE CLEVER: phần mềm trung gian định hướng thông điệp an toàn cho liên đoàn đám mây,” trong *Kỷ yếu của Hội nghị chuyên đề IEEE lần thứ 18 về Máy tính và Truyền thông (ISCC '13)* , trang 35–40, Split, Châu Âu, tháng 7 năm 2013.