Journal of Mining and Earth Sciences

Website: http://jmes.humg.edu.vn

Applying AES algorithm for secure data transmission between Sensor node and LoRa Gateway to Web Server

Chi Van Dang [1,*], Khoat Duc Nguyen [1], Luc The Nguyen[1], Dung Ngoc Le [2], Quan Hong Luu [2], Son Thanh Huynh [2]

[1] *Hanoi University of Mining and Geology, Hanoi, Vietnam*
[2] *Dong Nai Technology University, Dong Nai, Vietnam*

ARTICLE INFO

Article history:
Received 01st Sept. 2021
Revised 20th Dec. 2021
Accepted 18th Jan. 2022

Keywords:
AES algorithm,
Data transmission,
Internet of Thing (IoT),
Security LoRa Gateway,
Web server.

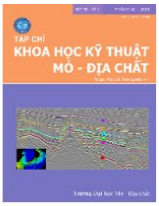
ABSTRACT

Lora Gateway is an intermediary device that can connect devices in the IoT system. IoT is the Internet of Things, consisting of a system of interrelated digital and mechanical devices and machines, capable of transmitting data over a network without requiring human-computer interaction. Lora is a long distance wireless communication technology that enables communication over a wide range between devices. Through this device, the Sensor nodes in the IoT system can transmit and receive data by LoRa waves to the Gateway and by Wifi/3G to the web server via the Internet. Data communicates in the internet environment, so important information needs to be protected by data encryption. This paper presents research and application of 128-bit AES symmetric encryption algorithm in LoRa wide area sensor network to secure data transmission between IoT devices and web server through LoRa Gateway device. The research team has designed and built models for testing sensor stations with integrated humidity and temperature sensors, LoRa Gateway integrating Lora module and wifi/3G module, developing the interface on web server with decoding, monitoring, and data storage features, and proposing a solution with AES encryption algorithm and architecture applied in the development of embedded software for LoRa module. The research results are tested on the model to test the encryption, data transmission, and decryption functions in applications for IoT LoRa Gateway systems. With this initial research, it is possible to apply the AES algorithm to secure data transmission in IoT Gateway systems.

*Corresponding author
E - mail: dangvanchi@humg.edu.vn
DOI: 10.46326/JMES.2022.63(1).10

Tạp chí Khoa học Kỹ thuật Mỏ - Địa chất

Trang điện tử: http://tapchi.humg.edu.vn



Ứng dụng thuật toán AES để bảo mật dữ liệu truyền thông giữa Sensor node và LoRa Gateway đến Web server

Đặng Văn Chí [1, *], Nguyễn Đức Khoát [1], Nguyễn Thế Lực [1], Lê Ngọc Dùng [2], Lưu Hồng Quân [2], Huỳnh Thanh Sơn [2]

[1] *Trường Đại học Mỏ - Địa chất, Hà Nội Việt Nam*

[2] *Trường Đại học Công nghệ Đồng Nai, Đồng Nai, Việt Nam*

THÔNG TIN BÀI BÁO

Quá trình:
Nhận bài 01/9/2021
Sửa xong 20/12/2021
Chấp nhận đăng 18/01/2022

Từ khóa:
AES algorithm,
Data transmission
Internet of Thing (IoT),
Security LoRa Gateway,
Web server.

TÓM TẮT

LoRa Gateway là thiết bị trung gian có thể kết nối các thiết bị (Device) trong một hệ thống IoT (Internet of Things). IoT là một hệ thống các thiết bị tính toán, máy móc cơ khí và kỹ thuật số có liên quan với nhau và khả năng truyền dữ liệu qua mạng mà không yêu cầu sự tương tác giữa con người với máy tính. LoRa là công nghệ truyền thông không dây với khoảng cách xa cho phép giao tiếp trên một phạm vi rộng giữa các thiết bị. Thông qua thiết bị này các trạm cảm biến (Sensor node) trong hệ thống IoT có thể dễ dàng truyền nhận dữ liệu bằng sóng LoRa đến Gateway và bằng wifi/3G đến web server thông qua mạng internet. Dữ liệu truyền thông trong môi trường internet nên các thông tin nhạy cảm và quan trọng cần được bảo mật bằng việc mã hóa dữ liệu. Bài báo này trình bày đến nghiên cứu ứng dụng thuật toán mã hóa đối xứng AES 128 bit trong mạng cảm biến diện rộng LoRa để bảo mật truyền dữ liệu giữa các thiết bị IoT và web server thông qua thiết bị LoRa Gateway. Nhóm nghiên cứu đã tiến hành thiết kế, xây dựng mô hình để thử nghiệm bao gồm: các trạm cảm biến tích hợp cảm biến đo độ ẩm và nhiệt độ, LoRa Gateway tích hợp module Lora và module wifi/3G và phát triển giao diện phần mềm trên web server với các tính năng giải mã, giám sát và lưu trữ dữ liệu, đồng thời đề xuất giải pháp với kiến trúc và thuật toán mã hóa AES được áp dụng trong việc phát triển phần mềm nhúng cho các module LoRa. Kết quả nghiên cứu được chạy thử nghiệm trên mô hình thực tế để kiểm tra về các tính năng mã hóa, truyền dữ liệu và giải mã trong các ứng dụng cho các hệ thống IoT Lora Gateway. Với nghiên cứu bước đầu này cho phép triển khai ứng dụng thuật toán AES để bảo mật truyền dữ liệu trong các hệ thống IoT Gateway.

1. Mở đầu

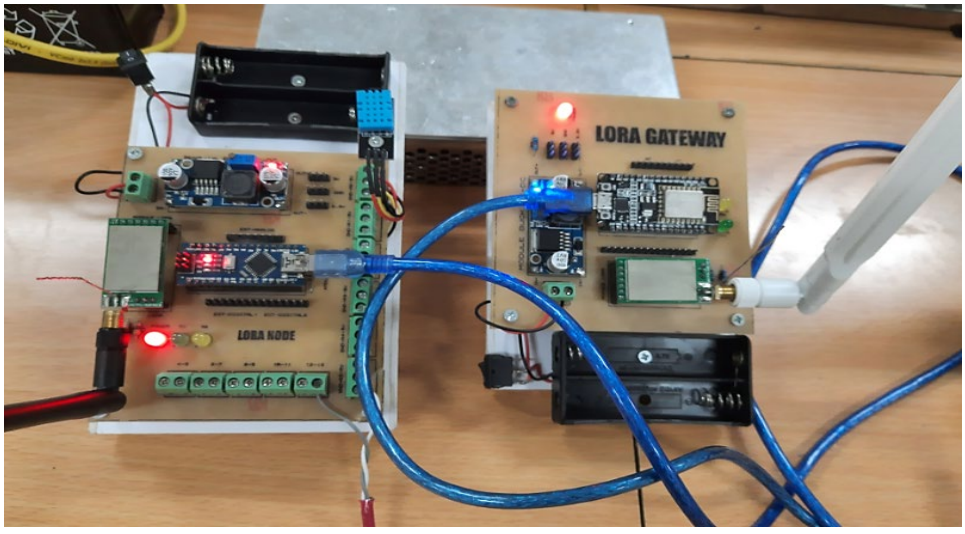
Công nghệ IoT (Internet of Things) đang trở nên phổ biến và được ứng dụng rộng rãi ở Việt Nam và trên thế giới. Khái niệm IoT đang được sử

*Tác giả liên hệ
E - mail: dangvanchi@humg.edu.vn
DOI: 10.46326/JMES.2022.63(1).10

dụng trong nhiều ứng dụng liên quan đến các hệ thống đo lường và giám sát trên Internet. LoRa là một công nghệ truyền thông không dây với khoảng cách xa (có thể tới 15 km) cùng với nguồn năng lượng hạn chế (chạy pin), công nghệ LoRa cho phép giao tiếp trên diện rộng, 2 chiều giữa các cảm biến từ xa (Sensor node) và các cổng kết nối với Internet (LoRa Gateway).

Hiện nay, trong nước cũng đã có một số dự án, công trình hay các đề tài được các nhà khoa học quan tâm nghiên cứu và từng bước triển khai ứng dụng Lora Gateway (Cao, 2015; Nguyễn, 2018; Vũ và nnk., 2018) vào các hệ thống đo lường giám sát xa. Điển hình là đề tài của Viện Công nghệ thông tin - Viện KHCN Việt Nam: "Phương pháp giám sát và điều khiển các thông số môi trường trên nền tảng điện toán đám mây qua mạng truyền thông không dây WIMAX" (Phạm và nnk., 2015). Hay đề tài nghiên cứu cấp nhà nước "Ảnh hưởng của ENSO đến các cực trị và lượng mưa ở Việt Nam và khả năng dự báo (Nguyễn, 2012). Hoặc đề tài nghiên cứu thuộc dự án PAM Air "Nghiên cứu hệ thống giám sát chất lượng không khí cho các mỏ lộ thiên Quảng Ninh" được thực hiện với sự hợp tác nghiên cứu giữa Trường Đại học Đông A (Hàn Quốc) và Đại học Mỏ - Địa chất thực hiện vào năm 2018÷2020. Hầu như các nghiên cứu trên chủ yếu tập trung vào phương pháp thu thập, kỹ thuật xử lý và truyền dữ liệu. Tuy nhiên, công tác bảo mật và mã hóa dữ liệu giữa thiết bị và Internet chưa được quan tâm nghiên cứu một cách cụ thể và chi tiết. Khả năng các thông tin nhạy cảm không được bảo mật an toàn và dễ bị đánh cắp hay mất dữ liệu rất dễ xảy ra. Vì vậy, công tác bảo mật thông tin truyền thông trong mạng IoT Gateway là yêu cầu và cần được quan tâm nghiên cứu.

Trên thế giới, liên quan đến lĩnh vực nghiên cứu về bảo mật truyền dữ liệu trong mạng IoT Gateway, hiện nay cũng đã có một số nhà khoa học quan tâm nghiên cứu và từng bước đưa vào ứng dụng trong thực tiễn. Điển hình trong các nghiên cứu (Kayem, 2016; Shahzad và nnk., 2017), các tác giả đã đề xuất các thuật toán mã hóa khác nhau để bảo mật dữ liệu như các hệ thống mã dịch chuyển và mã thay thế. Tuy nhiên, các thuật toán này lại tương đối đơn giản và dễ bị phá vỡ. Tin tặc hoàn toàn có thể dễ dàng nghe trộm, đánh cắp và sửa đổi dữ liệu trong các gói dữ liệu truyền thông. Để cung cấp quyền truy cập từ xa, thiết bị hay máy tính nhúng Raspberry Pi cũng có thể được sử dụng như một Gateway (Choi và nnk., 2018; Lee và nnk., 2018). Tuy nhiên, các thiết bị này lại tiêu thụ một lượng điện năng gấp 3÷4 lần so với ESP8266. Vì vậy, bài báo này đề xuất và triển khai thuật toán mã hóa đối xứng AES (128bit) trong bảo mật truyền thông mạng IoT LoRa Gateway. Việc triển khai mã hóa thuật toán trên Arduino/ESP8266 được thực hiện và kiểm tra kết quả trên mô hình, trong đó dữ liệu nhận được từ Sensor node sẽ được mã hóa trước khi gửi tới Web server thông qua LoRa Gateway.



Hình 1. Các module lora được sử dụng để triển khai thuật toán AES 128bit (Đề tài CT2019.01.04)

2. Thuật toán mã hóa đối xứng AES 128bit trên module LoRa

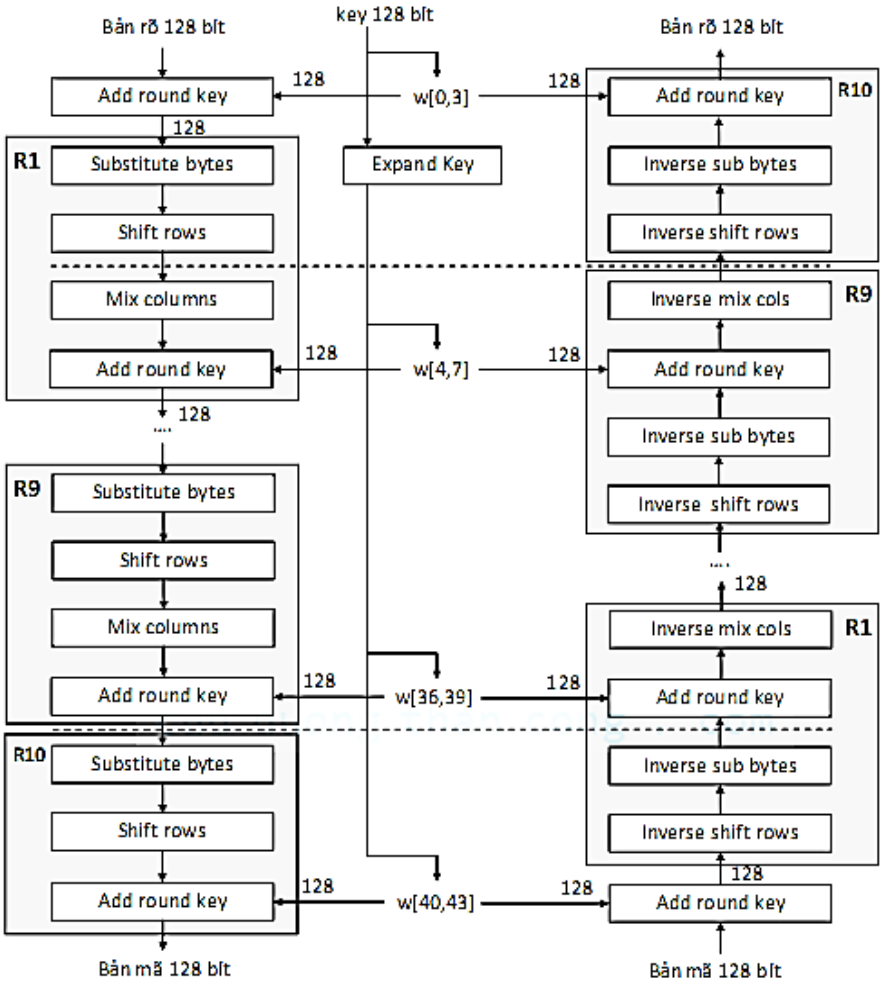
2.1. Giới thiệu mã hóa AES 128bit

Để đạt được các tính năng về bảo mật trong hệ thống IoT LoRa Gateway, có nhiều thuật toán mã hóa khác nhau để thực hiện và triển khai trên các module LoRa. Mỗi thuật toán đều cung cấp mức độ bảo mật cũng như ưu và nhược điểm khác nhau. Trong nghiên cứu này, thuật toán mã hóa đối xứng AES 128 bit được đề xuất để triển khai, Hình 1 là module LoRa được sử dụng để thực hiện việc thu thập dữ liệu, mã hóa và truyền thông trong mạng IoT Gateway.

Thuật toán AES được cho là một trong những thuật toán truyền thông an toàn nhất được biết cho đến thời điểm hiện tại (Patil, 2016; El-meligy và nnk., 2017). Hình 2 mô tả lưu đồ thực hiện các quy trình của thuật toán này. Theo đó, dữ liệu trước khi được gửi đi sẽ được mã hóa bằng phương pháp mã hóa đối xứng AES và được gắn kèm theo một địa chỉ MAC (Media Access Control) duy nhất được tạo ra từ bản rõ (Plain text). Bản mã và MAC được kết hợp với nhau sau đó được gửi đi. Phía bên nhận, trước tiên địa chỉ MAC và bản mã được tách ra, sau đó được xác minh địa chỉ MAC và giải mã bản mã gốc.

2.2. Các bước thực hiện

Mã AES là một mã hóa theo khối 128 bit (Trần, 2008). AES dùng 4 phép biến đổi chính để mã hóa một khối: khóa cộng hàng (Add row key), phép thế các byte (Substitute bytes), phép dịch hàng (Shift rows) và phép trộn cột (Mix



Hình 2. Lưu đồ nguyên lý mã hóa và giải mã thuật toán AES. (Trần, 2008)

columns). Mỗi phép biến đổi nhận tham số đầu vào có kích thước 128 bit và cho ra kết quả có kích thước 128 bit. AES thực hiện 4 phép biến đổi trên nhiều lần tạo thành 10 vòng biến đổi như Hình 2, trên sơ đồ cho thấy quá trình mã hóa và giải mã AES có 1 chu kỳ và mỗi chu kỳ thông qua 4 bước như sau:

Bước 1: (Add round key) tổng XOR được xác định bằng phép toán XOR bit 0 trên bản rõ với bít khóa (key) tương ứng.

Bước 2: (Substitude bytes) sau khi tính tổng XOR, mỗi byte của cặp ký tự HEX được thay thể bằng bảng Rijndael tương ứng (bảng tiêu chuẩn bao gồm 256 giá trị).

Bước 3: (Shift rows) sau khi thay thế tổng số 16 byte được phân phối để tạo ma trận vuông 4x4. Trong ma trận kết quả, hàng đầu tiên không thay đổi trong khi phần còn lại của 3 hàng (thứ 2, 3 và thứ 4) lần lượt được xoay sang trái 1, 2, 3 byte.

Bước 4: (Mix column) giai đoạn này phép nhân trái ma trận được áp dụng bằng cách sử dụng ma trận tiêu chuẩn 4x4. Thuật toán này không chỉ tạo ra một bộ khóa lớn (2.128 keys) và được bảo mật bởi nhiều thuật toán phân tích mật mã như dịch chuyển, tích hợp, tuyến tính, tập hợp,... Trong thuật toán AES, mỗi một vòng và mỗi một key mới sẽ được lấy từ key ở vòng trước đó cũng như bản mã của vòng trước. Như vậy, bản mã trong mỗi vòng sẽ có các bản mã khác nhau được thực hiện trên mã nhị phân và chính thuật toán này làm cho hệ thống an toàn hơn.

3. Đề xuất sơ đồ nguyên lý hệ thống bảo mật mạng LoRa IoT Gateway

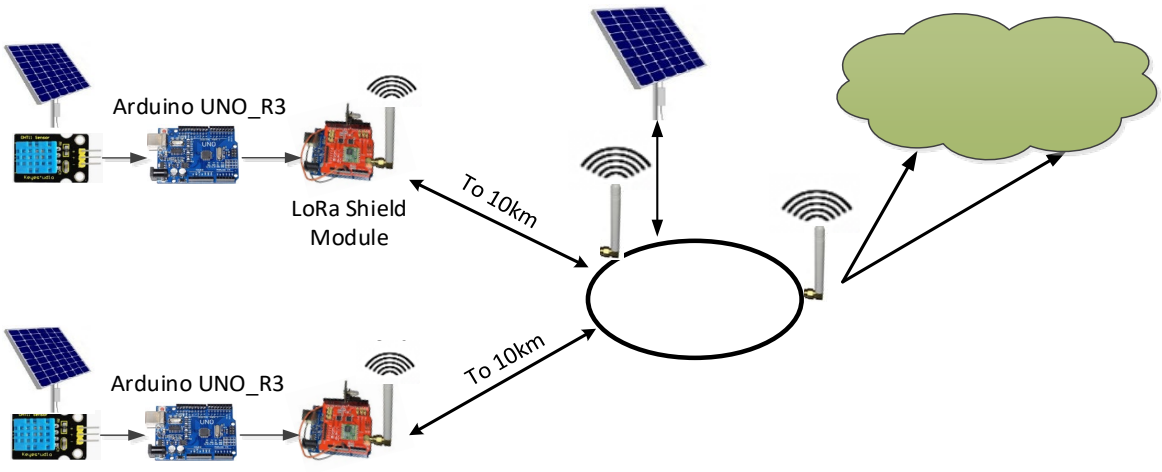
Bên cạnh một số tính năng bảo mật tiêu chuẩn được cung cấp bởi giao thức truyền thông LoRa, mạng LoRa cần phải triển khai bổ sung thêm tính năng bảo mật dựa trên thuật toán AES. Công việc này sẽ góp phần hoàn thiện tính bảo mật trong truyền dữ liệu giữa LoRa Gateway đến Web Server và các thiết bị. Cách thức tiếp cận này sẽ cung cấp một giải pháp bảo mật hoàn chỉnh, bảo đảm tính toàn vẹn và bảo mật trong trao đổi dữ liệu và truyền tin trong mạng IoT lora Gateway. (Dao, M.H và nnk., 2018).

3.1. *Sơ đồ cấu trúc hệ thống thu thập dữ liệu xa ứng dụng LoRa* Gateway

Trong sơ đồ Hình 3, dữ liệu đo giám sát từ các Sensor node, được tích hợp cảm biến đo nhiệt độ và độ ẩm. Mã lập trình đọc giá trị đo được nhúng thuật toán mã hóa AES trước khi gửi tới LoRa Gateway để vận chuyển dữ liệu đến Web server. Dữ liệu nhận được dưới dạng một bản mã sẽ được Server xác minh để giải mã dưới dạng bản rõ.

3.2. Giải pháp bảo mật dữ liệu từ thiết bị đến Web server

Hình 4 mô tả quá trình truyền dữ liệu từ các thiết



Hình 3. Sơ đồ nguyên lý hệ thống thu thập dữ liệu từ xa LoRa Gateway (Đề tài CT2019.01.04).

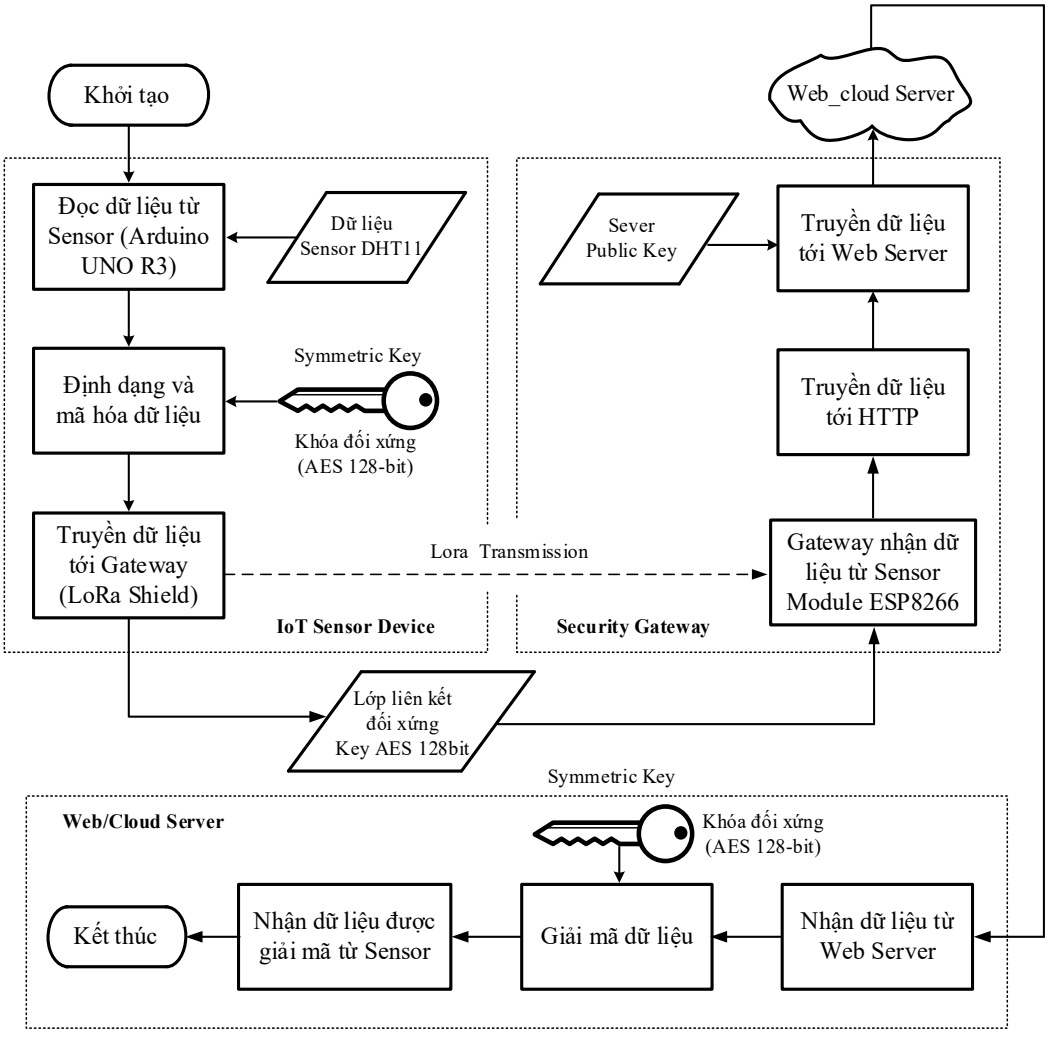
bị đến Server. Dữ liệu đọc được từ các cảm biến sẽ được định dạng và tiến hành mã hóa bằng thuật toán AES 128 bit trước khi truyền đến cổng không dây. Truyền thông không dây được bảo mật bằng WPA2-PSK và AES128 bit-PSK (Pre-Shared-Key). Gateway sẽ nhận dữ liệu từ Sensor node và chuyển tiếp thông tin liên lạc an toàn đến Server thông qua mạng internet. Các dữ liệu hoặc tin nhắn sẽ được mã hóa bằng khóa công khai của Server được cài đặt trong Gateway. Chỉ Server mới có thể giải mã tin nhắn bằng khóa riêng được thiết lập trên Server và không được chia sẻ với bất kỳ thiết bị nào khác. Tính toàn vẹn của dữ liệu được cung cấp ở lớp đối tượng đã mã hóa dữ liệu trước khi truyền đi. Đích đến có thể thực hiện công việc kiểm tra dữ liệu nhận được từ thiết bị IoT và xác minh dữ liệu đó khớp hay không.

4. Thiết kế tích hợp hệ thống và các kết quả chạy thực nghiệm trên mô hình

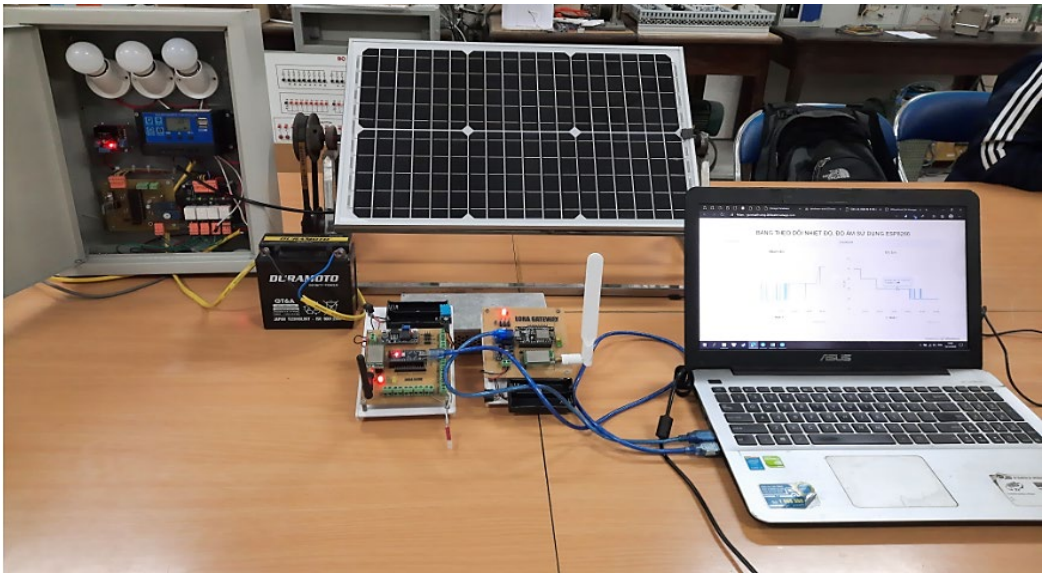
4.1. Thiết kế tích hợp hệ thống

Dựa trên cấu trúc hệ thống thu thập dữ liệu từ xa sử dụng Lora Gateway như Hình 3. Tiến hành thiết kế, tính chọn các thiết bị và tích hợp xây dựng mô hình như Hình 5 bao gồm:

- Hệ thống pin năng lượng mặt trời có tích hợp bộ điều khiển sạc.
- Trạm Sensor node tích hợp module LoRa.
- Module IoT LoRa Gateway.
- Phát triển giao diện giám sát trên Web dựa trên https://www.000webhost.com/.
- Phần mềm nhúng tích hợp thuật toán AES mã hóa và giải mã dữ liệu.



Hình 4. Lưu đồ thuật toán giải pháp bảo mật từ thiết bị đến Server.



Hình 5. Mô hình thực nghiệm thu thập dữ liệu ứng dụng LoRa Gateway (Đề tài CT2019.01.04).

4.2. Các kết quả chạy thực nghiệm

Các kết quả chạy thực nghiệm trên mô hình được tích hợp như ở Hình 5. Tiến hành kết nối các thiết bị, cài đặt mã thu thập dữ liệu, mã hóa bằng thuật toán AES trên các Sensor node, thiết kế xây dựng Web server và cài đặt mã để giải mã. Kết quả hiển trị các giá trị trên Web dưới dạng bản mã, cơ sở dữ liệu và đồ thị như ở các Hình 6, 7, 8.

Hình 8 có sự đột biến của nhiệt độ và độ ẩm (khoảng 12:15) chính là các điểm kiểm tra thử nghiệm ở các điều kiện môi trường khác nhau.

Server: localhost:3306 » Database: id15746314_dataesp » Table: SensorData

Browse | Structure | SQL | Search | Insert | Export | Import | Operations | Triggers

<< < 407 > >> | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

+ Options

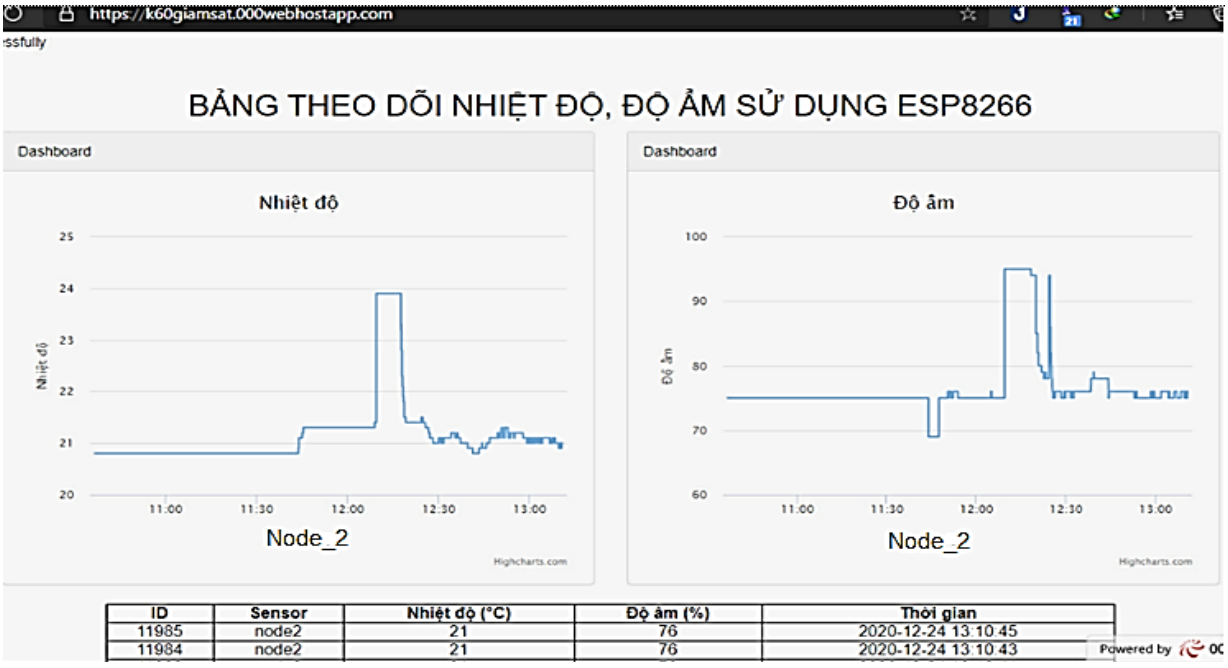
	id	sensor	nhiet_do	do_am	time_act
Edit Copy Delete	10151	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:16
Edit Copy Delete	10152	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:18
Edit Copy Delete	10153	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:19
Edit Copy Delete	10154	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:21
Edit Copy Delete	10155	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:23
Edit Copy Delete	10156	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:25
Edit Copy Delete	10157	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:27
Edit Copy Delete	10158	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:29
Edit Copy Delete	10159	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:31
Edit Copy Delete	10160	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:32
Edit Copy Delete	10161	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:34
Edit Copy Delete	10162	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:36
Edit Copy Delete	10163	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:38
Edit Copy Delete	10164	node2	clDaWMnrXQHJwjnLkX4l3w==	W32AP7wFZSpsdifKv8A iw==	2020-12-24 12:12:40

Hình 6. Bản mã nhận được trên Web server node 2 (nhiet_do & do_am) – ngày 24-12-2020.

https://k60giamsat.000webhostapp.com

ID	Sensor	Nhiệt độ	Độ ẩm	Thời gian
10702	node2	21.1	76	2020-12-24 12:30:07
10701	node2	21.1	76	2020-12-24 12:30:06
10700	node2	21.1	76	2020-12-24 12:30:04
10699	node2	21.1	76	2020-12-24 12:30:02
10698	node2	21	76	2020-12-24 12:30:00
10697	node2	21	76	2020-12-24 12:29:58
10696	node2	21	76	2020-12-24 12:29:56
10695	node2	21	76	2020-12-24 12:29:55
10694	node2	21	76	2020-12-24 12:29:53
10693	node2	21	76	2020-12-24 12:29:51
10692	node2	21	75	2020-12-24 12:29:49
10691	node2	21	75	2020-12-24 12:29:47
10690	node2	21	75	2020-12-24 12:29:45
10689	node2	21	75	2020-12-24 12:29:44
10688	node2	21	75	2020-12-24 12:29:42
10687	node2	21	75	2020-12-24 12:29:40
10686	node2	21	75	2020-12-24 12:29:38
10685	node2	21	75	2020-12-24 12:29:36
10684	node2	21	75	2020-12-24 12:29:34
10683	node2	21	75	2020-12-24 12:29:33
10682	node2	21	75	2020-12-24 12:29:31
10681	node2	21	75	2020-12-24 12:29:29
10680	node2	21	76	2020-12-24 12:29:27
10679	node2	21	76	2020-12-24 12:29:25
10678	node2	21	76	2020-12-24 12:29:23

Hình 7. Ghi cơ sở dữ liệu được giải mã (nhiệt độ - độ ẩm) trên Web Server – ngày 24-12-2020.



Hình 8. Đồ thị hiển thị Nhiệt độ - Độ ẩm trên Web Server node 2 – ngày 24-12-2020.

4.3. Thảo luận

Mô hình phát triển mang tính chất thử nghiệm, số lượng các Sensor node còn ít và thuật toán mã hóa, giải mã AES và truyền dữ liệu với số lượng tham số giám sát còn hạn chế. Bên cạnh đó môi trường truyền nhận cũng chưa khảo sát tới sự ảnh hưởng của các thông số nhiễu trong môi trường. Nhóm tác giả tiếp tục cải tiến thông qua

việc tối ưu thuật toán AES hay sử dụng Chip Vi điều khiển có cấu hình và tài nguyên mạnh hơn.

Đề xuất tiếp tục đánh giá độ chính xác, tính ổn định và bền vững của hệ thống, phát triển các Sensor node có tính ứng dụng cao trong công nghiệp, nông nghiệp và trong mọi mặt đời sống xã hội với mục tiêu hướng đến một hệ thống làm việc ổn định và tin cậy. Có thể dễ dàng triển khai thuật toán mã hóa tiên tiến AES vào thực tế đối với các hệ thống LoRa IoT Gateway. Đáp ứng kịp thời sự phát triển rất mạnh mẽ của cuộc cách mạng công nghiệp 4.0.

5. Kết luận

Hệ thống đã được tích hợp, lập trình mã hóa truyền thông và chạy thử nghiệm trên mô hình giám sát 2 thông số nhiệt độ và độ ẩm. Bước đầu đánh giá cho kết quả đảm bảo các yêu cầu về kỹ thuật, công nghệ và bảo mật dữ liệu trong hệ thống IoT Gateway. Kết quả nghiên cứu cho phép triển khai hệ thống IoT vào thực tế với các ứng dụng có yêu cầu bổ sung thêm các tính năng bảo mật dữ liệu tiên tiến trong truyền thông với Web server.

Lời cảm ơn

Các nội dung được trình bày trong bài báo là kết quả nghiên cứu khoa học của đề tài cấp Bộ CT2019.01.04. Các tác giả chân thành cảm ơn.

Đóng góp các tác giả

Đặng Văn Chí: đề xuất ý tưởng, giải pháp, thiết kế, xây dựng sơ đồ nguyên lý và cấu trúc của hệ thống, tổng hợp và viết bài. Nguyễn Đức Khoát: giải pháp và thuật toán mã hóa AES. Nguyễn Thế Lực: tích hợp hệ thống và lập trình mã nhúng. Lê Ngọc Dùng & Lưu Hồng Quân: xây dựng và thiết kế các mạch module. Huỳnh Thanh Sơn: lắp đặt và chạy thực nghiệm mô hình.

Tài liệu tham khảo

Cao, H. T. (2015). Nghiên cứu thiết kế hệ thống quan trắc dùng trong nông nghiệp. *Hội thảo toàn quốc về CNTT – Trường Đại học Cần Thơ*, 128-133.

Choi, C. S., Jeong, J. D., Lee, I. W., & Park, W. K. (2018, January). LoRa based renewable energy monitoring system with open IoT platform. In *2018 international conference on Electronics, Information, and Communication (ICEIC),* IEEE, 1-2..

Dao, M. H., Hoang, V. P., Dao, V. L., & Tran, X. T. (2018). An energy efficient AES encryption core for hardware security implementation in IoT systems. In *2018 International Conference on Advanced Technologies for Communications (ATC),* IEEE, 301-304.

PAM Air. (2018÷2020). *Nghiên cứu hệ thống giám sát chất lượng không khí cho các mỏ than lộ thiên Quảng Ninh,* Trường Đại học Đông Á (Hàn Quốc) & Trường Đại học Mỏ - Địa chất; http://humg.edu.vn.

El-meligy, N., Amin, M., Yahya, E., & Ismail, Y. (2017, May). 130nm Low power asynchronous AES core. In *2017 IEEE International Symposium on Circuits and Systems (ISCAS),* 1-4..

Lee, H. R., Kim, W. J., Park, K. H., Cho, H. J., & Lin, C. H. (2018, January). Development of an easy payment system based on IoT gateway. In *2018 International Conference on Electronics, Information, and Communication (ICEIC),* IEEE, 1-3.

Kayem, A. V., Strauss, H., Wolthusen, S. D., & Meinel, C. (2016, March). Key management for secure demand data communication in constrained micro-grids. In *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA),* IEEE, 585-590.

Nguyễn, Đ. N. (2012). *Ảnh hưởng của Enso đến các cực trị và lượng mưa ở Việt Nam và khả năng dự báo*. Thư viện CRES, Trung tâm KHCN khí tượng thủy văn và môi trường. http://thuviencres.cres.edu.vn/

Nguyễn, V. P. (2018). *Ứng dụng IoT trong việc giám sát, cảnh báo mức độ ô nhiễm không khí trong đô thị*. http://aita.gov.vn.

Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*, 617-624.

Phạm, N. M. (2015). Phương pháp giám sát và điều khiển các thông số môi trường trên nền tảng điện toán đám mây qua mạng truyền thông không dây

WIMAX. *Tuyển tập báo cáo Hội nghị toàn quốc lần thứ 3 về Điều khiển và Tự động hóa*, 28-29/11, Thái Nguyên, Việt Nam.

Trần, M. V. (2008). *Bài giảng "An toàn và bảo mật thông tin*". Khoa Công nghệ thông tin – Trường Đại học Nha Trang. https://fb.com/tailieudientucntt.

http://www.000webhost.com

Shahzad, A., Kim, Y. G., & Elgamoudi, A. (2017, February). Secure IoT platform for industrial control systems. In *2017 International Conference on Platform Technology and Service (PlatCon)*, IEEE, 1-6.

Vũ, T. Q., Phạm, N. M., Nguyễn, Đ. K., Ngô, D. T. (2018). Thiết kế hệ thống quan sát đối tượng từ xa phục vụ công tác cứu hộ cứu nạn. *Tạp chí Khoa học Kỹ thuật Mỏ - Địa chất*, *59*(1), 1-8.