SYSTEMIC: Information System and Informatics Journal
ISSN: 2460-8092, 2548-6551 (e)
Vol 6 No 1 – Agustus 2020

Implementasi Kriptografi AES untuk Keamanan Pengiriman Data Internet of Things Menggunakan Web Service Rest pada NodeMCU

Afrijal Rizqi Ramadan[1], Ardito Wahyu Prakoso[2], Ghifari Dwi C[3]

[1,2,3)] UIN Maulana Malik Ibrahim Malang

arizqiramadan@gmail.com[1], arditowahyu19@gmail.com[2], dungeoncity16@gmail.com[3]

Kata Kunci

IoT,
REST,
web service,
NodeMCU,
kriptografi,
AES

Abstrak

Munculnya istilah Internet of Things pada era ini pada umumnya mempunyai peran positif untuk manusia diberbagai aspek seperti kesehatan, perindustrian, perkotaan dan bahkan pertanian. Namun terdapat masalah yang menjadi ancaman serius dalam lingkungan IoT, yaitu tentang keamanan data. Keamanan data merupakan hal yang diharuskan dalam menyimpan atau mengirim sebuah informasi yang penting. Berbahaya jika data jatuh dan diambil oleh pihak yang nantinya dimanfaatkan dengan tidak bertanggung jawab yang nantinya dapat mengambil bahkan merubah data yang sebenarnya. Oleh karena itu, penggunaan kriptografi AES dibutuhkan untuk menyelesaikan masalah tersebut. AES singkatan dari Advanced Encryption Standard adalah algoritma enkripsi kunci berbentuk simetris yang memiliki proses keamanan data lebih cepat daripada algoritma asimetris. Tujuan penelitian ini yaitu untuk memaparkan cara menerapkan algoritma AES pada perangkat IoT sebagai upaya mengamankan data. Data berupa nilai suhu dan kelembaban yang dienkripsikan dengan algoritma AES sebelum nantinya dikirimkan kepada server basis data dengan wadah berupa jaringan nirkabel atau disebut wifi. Dalam web server data yang terenkripsi dikembalikan dengan bentuk berupa data asli sebelum masuk ke basis data. Hasil dari pengujian ini yaitu mengkonfirmasi bahwa sistem berjalan dengan optimal. Penggunaan algoritma AES dinyatakan berhasil dalam memenuhi tujuan yaitu untuk keamanan serta kerahasiaan data.

Keywords

IoT,
REST,
web service,
NodeMCU,
kriptografi,
AES

Abstract

The emergence of the term Internet of Things in this era generally has a positive role for humans in various aspects such as health, industry, cities and even agriculture. However, there is a problem that is a serious threat in the IoT environment, namely data security. Data security is something that is required in storing or sending important information. It is dangerous if the data falls and is taken by parties who will be used irresponsibly who can later retrieve and even change the actual data. Therefore, the use of AES cryptography is needed to solve this problem. AES stands for Advanced Encryption Standard is a symmetric key encryption algorithm that has a faster data security process than an asymmetric algorithm. The purpose of this study is to describe how to apply the AES algorithm to IoT devices as an effort to secure data. Data in the form of temperature and humidity values are encrypted by the AES algorithm before being sent to the database server with a container in the form of a wireless network or called wifi. In the web server, encrypted data is returned in the form of the original data before entering the database. The results of this test are to confirm that the system is running optimally. The use of the AES algorithm is declared successful in meeting the objectives, namely for data security and confidentiality.

1. Pendahuluan

Internet of Things (IoT) mengalami perkembangan seiring berjalannya perkembangan internet dan mikrokontroller. IoT merupakan konsep dari suatu objek yang bisa melakukan pengiriman suatu data tanpa adanya campur tangan manusia. Namun salah satu unsur penting yang berhubungan dengan pengiriman data yaitu tentang keamanan. Kerahasiaan dari data merupakan suatu kelengkapan pelayanan agar beberapa atau banyak data yang terkirim tidak sampai dibaca pada pihak ketiga yang tidak berhak menerima. Kriptografi merupakan unsur dari keamanan data yang sering digunakan dan diaplikasikan pada segala bentuk teknologi informasi. Kriptografi mampu merahasiakan segala bentuk data menjadi sebuah data rahasia

DOI : 10.29080/systemic.v6i1.752

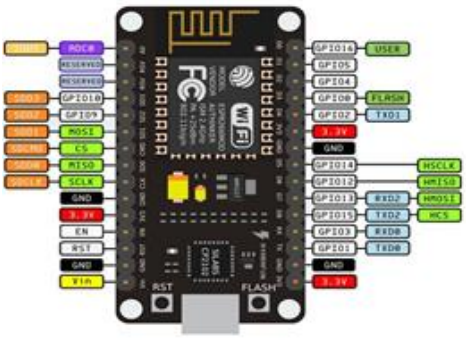
(chipertext). Guna menjaga sebuah data yang berada pada perangkat IoT, maka data tersebut harus dilakukan proses enkripsi dan dekripsi yang berfungsi sebagai menjaga kerahasiaan data. Proses enkripsi yaitu suatu proses perubahan dari suatu pesan asli (plain text) menjadi pesan yang rahasia (chipper text), sedangkan proses dekripsi yaitu proses untuk mengembalikan pesan rahasia menjadi pesan dalam bentuk asli. Dalam hal ini, penulis mengaplikasikan kriptografi ke dalam sebuah projek berbasis Internet of Thing (IoT) menggunakan mikrokontroler NodeMCU sebagai perangkat IoT tersebut. Mikrokontroler ini digunakan sebagai media pencari informasi data yang diperoleh dengan bantuan sensor. Lalu data tersebut dikirimkan ke sebuah website pribadi dengan arsitektur RESTful Web Service. Tetapi pada pengiriman data tersebut belum dirahasiakan sehingga data tersebut bisa saja diambil oleh pihak sewenang – wenang. Maka dari itu penulis menggunakan kriptografi yang simetris agar proses keamanan data lebih cepat. Salah satunya yaitu algoritma kriptografi Advanced Encryption Standard (AES).

Pada penelitian ini terkonsep pada penerapan algoritma AES guna berfungsi sebagai keamanan sebuah pengiriman data pada perangkat mikrokontroler NodeMCU. Setelah melakukan proses penerapan algoritma AES, selanjutnya adalah dilakukannya pengujian guna menguji waktu proses dan memori yang digunakan pada piranti mikrokontroler yang mendapatkan sebuah atau beberapa kesimpulan berdasarkan pengujian yang dilakukan. Untuk penelitian yang dilakukan oleh penulis diharapkan dapat membuat sebuah langkah awal implementasi algoritma AES dengan proses enkripsi pada pengiriman sebuah data pada lingkungan IoT.

2. Teori Dasar

2.1 Mikrokontroller NodeMCU V3

NodeMCU V3 adalah sebuah platform Internet of Thing (IoT) yang bersifat opensource, merupakan tahapan perkembangan produk ESP 8266 melalui sebuah firmware menggunakan basis e-Lua. Selain menggunakan bahasa Lua, NodeMCU dapat bekerja sama dengan perangkat lunak bernama Arduino IDE dengan sedikit perubahan di bagian board manager pada Arduino IDE. NodeMCU V3 merupakan perangkat yang kompatibel dengan Bahasa mesin yaitu pemrograman C serta kontak antar perangkat lain atau bisa melalui internet melalui nirkabel. Normalnya NodeMCU mempunyai ukuran panjang 47 mm dan lebar 31 mm. NodeMCU V3 juga termasuk kedalam sebuah mikrokontroler yang mempunyai processor dan memori berukuran kecil sebagaimana spesifikasi dari NodeMCU V3 dijelaskan dibawah ini:

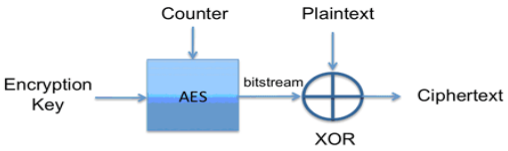


SPESIFIKASI	NODEMCU V3
Mikrokontroller	ESP8266
Ukuran Board	57 mmx 30 mm
Tegangan Input	3.3 ~ 5V
GPIO	13 PIN
Kanal PWM	10 Kanal
10 bit ADC Pin	1 Pin
Flash Memory	4 MB
Clock Speed	40/26/24 MHz
WiFi	IEEE 802.11 b/g/n
Frekuensi	2.4 GHz – 22.5 Ghz
USB Port	Micro USB
Card Reader	Tidak Ada
USB to Serial Converter	CH340G

Gambar 1. Model dan Spesifikasi Mikrokontroler NodeMCU V3

2.2 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah salah satu algoritma pada kriptografi simetris berfungsi sebagai pengaman pada banyak jenis data. Algoritma ini berupa blok bersifat chipertext simetris yang mempunyai fungsi dapat melakukan kegiatan enkripsi serta kegiatan dekripsi di informasi pada data. Enkripsi dapat merubah sebuah data yang dimana tidak bisa dibaca yang biasa disebut ciphertext; lawan katanya adalah dekripsi yang berguna merubah data ciphertext menjadi bentuk awal data yang dikenal sebagai plaintext. Algoritma AES menggunakan kunci kriptografi blok 128, 192, serta 256 bits guna melakukan proses enkripsi serta proses dekripsi pada sebuah data di blok 128 bits.



Gambar 2. Urutan algoritma AES.

Pada gambar 2 yang tercantum diatas menjelaskan tentang tipe algoritma AES dengan panjang pada kunci, panjang blok serta banyak putaran yang berbeda. Untuk penelitian ini digunakan AES-128 bit dengan jumlah putaran enkripsi sebanyak 10 kali. Terdapat 4 transformasi putaran pada proses enkripsi dan dekripsi [7] :

1. SubBytes

Berfungsi menukar isi dari komponen data yaitu byte dengan menggunakan tabel substitusi.

2. ShiftRows
   Proses pergeseran blok per baris pada state array.
3. MixColumn
   Proses mengalikan blok data (pengacakan) di masing-masing state array dengan rumus sebagai berikut:
   (x) = {03}2 + {01}2 + {01} + {02}
4. AddRoundKey
   Mengombinasikan state array dan round key dengan hubungan XOR.

Pada proses dekripsi algoritma AES :

a. InvShiftRows
   Melakukan pergeseran bit ke kanan pada setiap blok baris.
b. InvSubBytes
   Elemen state ditentukan dewngan menggunakan sebuah tabel Inverse S-Box.
c. InvMixColumn
   Kolom pada state dikalikan menggunakan matriks AES.
d. AddRoundKey
   Mengombinasikan state array dan round key dengan hubungan XOR.

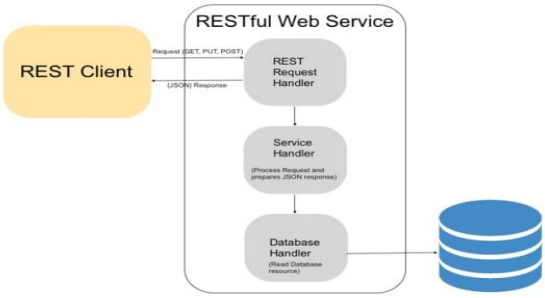
2.3 Web Service

Web Service merupakan sistem software yang dibangun guna mengoptimalkan interaksi dan interoperabilitas antar suatu sistem di suatu jaringan [1]. Web service memiliki interface pada ektensi yang umumnya dapat dibaca oleh suatu perangkat yang berfungsi sebagai fasilitas untuk menyediakan layanan untuk sistem lainnya agar supaya bisa berinteraksi ke sebuah sistem melewati layanan yang tersedia.

Sistem lain berinteraksi ke web service dengan memakai pesan sejenis SOAP yang pada dasarnya terkirim melewati HTTP dalam bentuk XML [5]. Pada umumnya, web service bukan hanya selalu terdapat pada standar SOAP. Terdapat pustaka yang menjelaskan mengenai web service yang didefinisikan secara umum dengan penjelasan bahwa web service merupakan sebuah aplikasi yang menggunakan jaringan internet untuk mengakses protokol standar internet serta juga untuk menyimpan data informasi berektensi JSON maupun XML, sehingga akses data tersebut dapat digunakan oleh sistem lain walaupun ada perbedaan pada platform, sistem operasi, dan bahasa pemrograman.

2.4 Representational State Transfer (REST)

Representational State Transfer atau REST, merupakan salah satu jenis arsitektur untuk penerapan web service pada konsep perpindahan antar state [2]. State ini menggambarkan jika browser mengakses suatu halaman web atau situs, server akan mentransfer halaman web pada state baru ke browser. Navigasi URL yang telah disiapkan sama halnya seperti mengganti state lama dengan state baru dari halaman situs.



Gambar 3. Kinerja RESTful Web Service (Sumber : https://phppot.com/php/php-restful-web-service/)

Pada gambar 3, saat REST aktif, dengan bernavigasi dengan pembuatan link-link HTTP disaat proses tertentu, seakan-akan state mengalami perpindahan. Perintah HTTP yang biasa dipakai dalam REST adalah perintah GET, POST, PUT dan DELETE. Lalu balasan dikirim dalam format XML sederhana dan tidak ada protokol pemaketan data, sehingga penerimaan informasi lebih gampang dibaca dan dipasang pada client. Sebutan web service dengan arsitektur REST adalah RESTful web service.

3. Perancangan Dan Implementasi Sistem

3.1 Perancangan Sistem

Komponen IoT yang digunakan untuk implementasi projek penelitian ini yaitu pada tabel 1 dibawah ini.

Tabel 1:Tabel komponen IoT

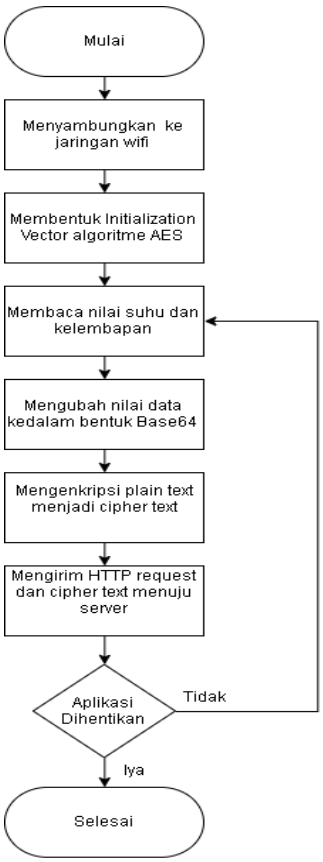
Kebutuhan	Keterangan
Sensor DHT11	Modul sensor untuk membaca suhu dan kelembapan
NodeMCU V3 (ESP8266)	Microcontroller yang terintegrasi dengan modul wifi dihubungkan dengan sensor DHT11. Dan NodeMCU juga bertindak sebagai klien REST.
Hosting	Bertindak sebagai server penympanan data dan server REST
Wifi Hotspot	Wi-Fi hotspot untuk memberikan koneksi jaringan internet

Pada gambar 4, dapat dijelaskan mengenai rancangan konektivitas antar perangkat yang terjadi pada sistem. Pada umumnya sistem tersebut menerapkan arsitektur web service

REST. Dalam pembentukan arsitektur web service yaitu terdapat dua unsur yaitu server dan klien yang saling berkomunikasi melalui jaringan internet. Pada sistem ini, klien akan mengirimkan data dengan request GET kepada server. Lalu server melayani request dan data tersebut. Data kemudian diproses seperti URL yang diakses oleh klien.

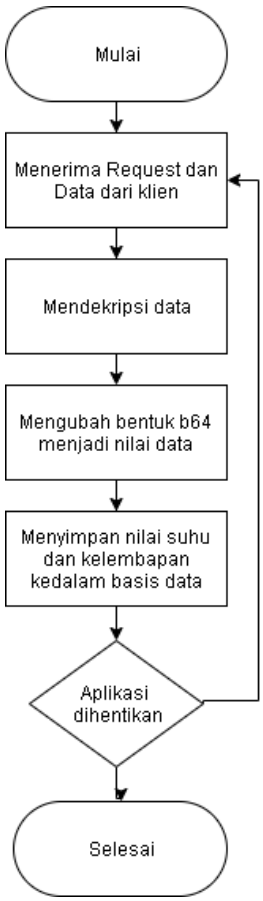
Gambar 4. Rancangan proses komunikasi klien server REST.

Gambar 5 menjelaskan tentang tahapan alur proses jalannya data dan kerja sistem pada klien. Sistem dirancang dapat membentuk keystream algoritma AES, tersambung ke router, serta melakukan pembacaan nilai sensor suhu dan kelembapan dari DHT11 lalu data tersebut di enksipsi sebelum dikirim ke server.



Gambar 5. Rancangan alur kerja klien REST.

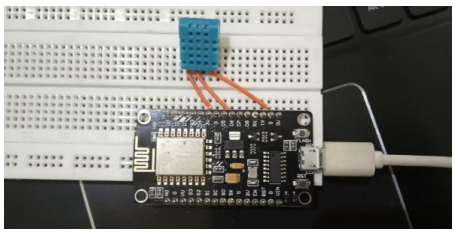
Gambar 6 merupakan tahapan alur proses kerja sistem di bagian server. Data dari klien terlebih dahulu akan didekripsi. Dilanjutkan nilai suhu dan kelembapan pada data disimpan oleh basis data MySQL. Terdapat satu tabel yang terdiri dari tiga kolom yaitu kolom id, nama, dan status. Kolom id akan dibentuk secara auto-increment sebagai identitas dari data nama sensor. Kolom nama untuk menyimpan nama sensor yaitu ada sensor suhu dan kelembapan. Kolom status yang bertipe untuk menyimpan data berupa nilai sensor yang diterima oleh server.



Gambar 6. Rancangan alur kerja server REST.

3.1 Implementasi

Pada implementasi ini dibutuhkan beberapa komponen diantaranya yaitu sensor DHT11, Projectboard, dan mikrokontroler NodeMCU V3. Sensor DHT11 dan mikrokontroller NodeMCU dihubungkan ke projectboard. Pin kaki positif pada sensor DHT11 dihubungkan dengan kaki 3V pada mickrokontroller NodeMCU V3. Pin kaki negatif pada sensor suhu DHT11 dihubungkan dengan pin GND pada NodeMCU V3. Dan Pin data pada DHT11 dihubungkan dengan pin D6 pada NodeMCU. Kemudian kode program di dalam mikrokontroler diunggah dengan menghubungkan perangkat NodeMCU dengan laptop.

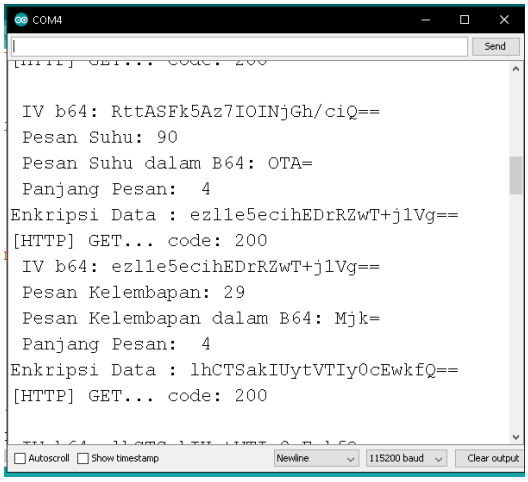


Gambar 7. Implementasi perangkat keras

Tabel 3. Pengaturan perangkat lunak Arduino IDE.

Board	NodeMCU 1.0 (ESP12-E Module)
Flash size	4M (3M SPIFFS)
Debug port	Serial
Debug level	None
IwIP variant	v2 Prebuilt (MSS=536)
CPU frequency	80 MHz
Upload speed	115200

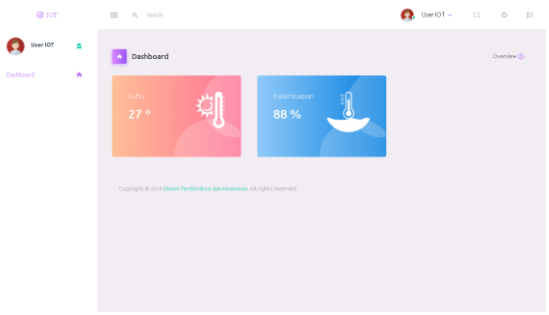
dan mengunggah kode yaitu menggunakan Arduino IDE. Dalam penggunaanya beberapa konfigurasi juga diperlukan seperti penambahan board pada perangkat lunak Arduino IDE dan merubah pengaturan agar bisa digunakan dan kode program bisa diunggah ke perangkat NodeMCU V3. Berikut adalah tabel pengaturan bisa dilihat pada Tabel 3.



Gambar 8. Tampilan hasil pembacaan serial pada Arduino IDE.

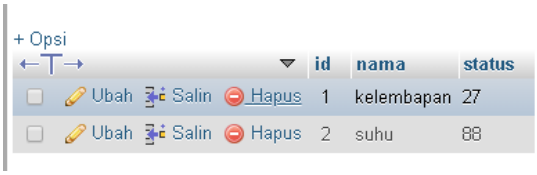
Gambar 8 merupakan output hasil enkripsi dan sistem klien web service REST di dalam Serial Arduino IDE dari gambar tersebut kita dapat menemukan beberapa informasi. Diantaranya yaitu :

- IV b64 : hasil dari proses pembentukan IV dalam format b64.
- Pesan Suhu: hasil pembacaan nilai sensor suhu
- Pesan Kelembapan : hasil pembacaan nilai sensor kelembapan
- Panjang Pesan : panjang nilai pesan dalam b64, , hasil enkripsi data,
- Enkripsi Data : status request dari klien ke server.



Gambar 9. Tampilan hasil dari implementasi server REST.

Pada Gambar 9 diatas merupakan hasil dari tampilan REST server saat diakses. Kode program web REST server ditulis dengan bahasa pemrograman PHP. Data dalam web REST server didekripsi sampai data berbentuk plaintext dan diubah kembali menjadi bentuk nilai asli yang sebelumnya masih format b64. Dan akhirnya, nilai suhu dan kelembapan dapat disimpan ke dalam tabel basis data MySQLServer seperti pada Gambar 10.



Gambar 10. Tampilan dari hasil penyimpanan data pada MySQL-Server.

4. Pengujian

4.1 Pengujian Fungsional

Pengujian fungsional berfungsi menguji kesesuaian fungsi-fungsi hasil penerapan rancangan tersebut. Berikut Hasil pengujian fungsional pada Tabel 4.

Tabel 4. Hasil pengujian fungsional sistem.

No	Fungsi	Hasil Uji
1	Menyambungkan ke jaringan wifi	Berhasil
2	Membentuk *Initialization Vector* algoritma AES	Berhasil
3	Membaca nilai data suhu dan kelembapan	Berhasil
5	Mengubah nilai data kedalam bentuk Base64	Berhasil
6	Mengenkripsi *plain text* menjadi *cipher text*	Berhasil
7	Mengirim HTTP *request* dan *cipher text menuju* server	Berhasil

8	Menerima HTTP *request* dan cipher text dari klien	Berhasil
9	Mendekripsi *cipher text* menjadi *plain text*	Berhasil
10	Mengubah Base64 menjadi bentuk nilai asli	Berhasil
11	Menyimpan data ke dalambasis data	Berhasil

4.2 Pengujian Kinerja

Pengujian kinerja dilakukan sebanyak 50 kali lalu hasil pengujian dirata-rata. Pengujian kinerja ini dilakukan untuk melihat efektifitas memori dan waktu yang dibutuhkan dalam proses enkripsi algoritma AES pada perangkat NodeMCU. Hasil rata-rata penggunaan waktu yang dibutuhkan saat uji enkripsi plain text suhu membutuhkan waktu 5542 mikrodetik sedangkan kelembapan 5868 mikrodetik. Proses enkripsi pada perangkar NodeMCU membutuhkan memori 42984.bita.

5. Kesimpulan

1. Hasil pengujian fungsionalitas dan keamanan tersebut dapat disimpulkan bahwa algoritma AES bisa digunakan sebagai keamanan data pada proses transfer data ke server basis data menggunakan NodeMCU.
2. Hasil pengujian kinerja tersebut dapat disimpulkan bahwa algoritma AES selaku kriptografi pada perangkat NodeMCU bersifat valid dan benar.
3. Proses enkripsi data pada perangkat mikrokontroler NodeMCU disinyalir membutuhkan waktu 0,005542 detik, sedangkan memori yang dibutuhkan sebesar 0,8% bagian total memori perangkat. Nilai data pada plain text berbanding lurus dengan nilai waktu dan memori yang dibutuhkan oleh perangkat NodeMCU saat proses enkripsi data.

Daftar Pustaka

[1] P.-N. Tan, M. Steinbach, and V. Kumar, “Introduction to Data Mining,” 2005.

[2] J. Han, M. Kamber, and J. Pei, “Data Mining: Concepts and Techniques,” *Data Min. Concepts Tech.*, 2012.

[3] A. K. Jain, M. N. Murty, and P. J. Flynn, “Data clustering: a review,” *ACM Comput. Surv.*, vol. 31, no. 3, pp. 264–323, 1999.

[4] A. K. Jain, “Data clustering: 50 years beyond K-means,” *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 651–666, 2010.

[5] S. Guha, R. Rastogi, and K. Shim, “Rock: a robust clustering algorithm for categorical attributes,” *Inf. Syst.*, vol. 25, no. 5, pp. 345–366, 2000.

[6] Abdur, R. M., 2016. Middleware for Internet of Things:A Survey. IEEE Internet of Things Journal. Vol. 03 No.01.

[7] Ariyus, D., 2008. Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi. Yogyakarta: ANDI

[8] Nawir, M., et al., 2018. Internet of Things (IoT): Taxonomy of Security Attacks. Malaysia: University Malaysia Perlis.

[9] Munir, Rinaldi. 2006. Kriptografi. Penerbit Informatika. Bandung.

[10] Adhi, J. S. 2005. Kriptografi dengan Algoritma AES untuk Penyandian Data.*Skripsi*. Universitas Kristen Duta Wacana. Yogyakarta.