Implementasi Algoritme AES-256 pada Sistem Pemantauan Getaran Gempa Bumi Menggunakan Perangkat LoRa

Rizki Kurniandi[1)], Desi Marlena[2)], Dian Novita Aryani[3)]

1) Badan Siber dan Sandi Negara, rizki.kurniadi@bssn.go.id
2) Politeknik Siber dan Sandi Negara, desi.marlena@bssn.go.id
3) Badan Siber dan Sandi Negara, dian.novita@bssn.go.id

Abstrak

Teknologi pemantauan getaran gempa bumi masih terdapat kendala dalam pengumpulan data informasi seperti membutuhkan tenaga manusia dan waktu cukup lama. Salah satu teknologi getaran gempa yaitu sistem jaringan sensor nirkabel yang dapat mempermudah dalam pengukuran data lapangan serta memberikan suatu sistem deteksi gempa bumi. Dengan menggunakan media transmisi yang banyak diterapkan dalam jaringan sensor yaitu LoRa (Long Range) diharapkan prototype sistem pemantauan getaran gempa dapat mengatasi masalah yang terjadi. Pada penelitian ini menggunakan metodologi penelitian System Development Life Cycle (SDLC) dengan pendekatan waterfall Development terdiri dari 4 tahapan yaitu planning, analysis, design, dan implementation. Pengujian dilakukan dengan dua skema yaitu sistem tanpa AES dan sitem dengan AES serta pengujian di dua kondisi yaitu LOS dan NLOS. Hasil pengujian jarak maksimal yang dicapai dalam berkomunikasi pada kondisi LOS adalah 9600 Meter sedangkan kondisi NLOS mencapai 6000 Meter. Hasil rata-rata nilai RSSI tertinggi pada jarak 500 Meter kondisi LOS tanpa AES adalah -88,8 dBm sedangkan nilai terendah pada jarak 6000 Meter kondisi NLOS dengan AES adalah -123,7 dBm. Berdasarkan hasil tersebut disimpulkan bahwa prototipe berhasil melakukan proses kirim terima data dengan baik.

Kata kunci: AES, Gempa Bumi, LoRa, LOS, NLOS, RSSI, Sensor

Abstract

Earthquake vibration monitoring technology still has obstacles in collecting information data such as requiring human labor and a long time. One of the earthquake vibration technologies is a wireless sensor network system that can facilitate field data measurement and provide an earthquake detection system. By using a transmission medium that is widely applied in sensor networks, namely LoRa (Long Range), it is hoped that the prototype earthquake vibration monitoring system can overcome the problems that occur. This research uses the System Development Life Cycle (SDLC) research methodology with a waterfall development approach consisting of 4 stages, namely planning, analysis, design, and implementation. Testing is done with two schemes, namely the system without AES and the system with AES and testing in two conditions, namely LOS and NLOS. The maximum distance achieved in communicating in LOS conditions is 9600 meters while NLOS conditions reach 6000 meters. The highest average RSSI value at a distance of 500 meters LOS conditions without AES is -88.8 dBm while the lowest value at a distance of 6000 meters NLOS conditions with AES is -123.7 dBm. Based on these results, it is concluded that the prototype successfully performs the process of sending and receiving data properly.

Keywords: *AES, Earthquake, LoRa, LOS, NLOS, RSSI, Sensor*

1. PENDAHULUAN

Secara geografis Indonesia terletak diantara dua lempeng benua yaitu Asia dan Australia juga diapit oleh dua samudera yaitu samudera Pasifik dan samudera Hindia. Negara Indonesia juga dilalui oleh tiga lempeng tektonik dunia yaitu lempeng Eurasia, lempeng Indonesia Australia, dan lempeng Pasifik [1]. Oleh karena itu, dengan kondisi geografis yang ada menjadikan Indonesia daerah yang rawan terjadi bencana gempa bumi, baik gempa tektonik maupun gempa vulkanik. Bencana gempa bumi tidak dapat di prediksi kejadiannya. Sehingga bencana ini dapat menimbulkan berbagai macam kerusakan dan kerugian, seperti kerusakan bangunan, jatuhnya korban jiwa, dan sebagainya. Dari peristiwa tersebut, maka dibutuhkan suatu alat pemantauan getaran gempa bumi yang dapat memberikan peringatan informasi darurat serta lokasi terjadinya gempa.

Pada penelitian ini bertujuan untuk merancang suatu teknologi pemantauan getaran gempa bumi dengan sistem jaringan sensor nirkabel yang dapat mempermudah dalam pengukuran data lapangan, yang dapat memberikan informasi darurat serta titik lokasi dengan jarak yang jauh [2][3]. Selain itu sistem ini dapat bekerja secara realtime. Sehingga data yang masuk dapat digunakan untuk mengantisipasi bencana di daerah lainnya dan penanggulangan bencana dapat diantisipasi secepat mungkin.

Salah satu teknologi media transmisi nirkabel yang banyak diterapkan dalam jaringan sensor adalah menggunakan perangkat LoRa (Long Range) [4][5]. LoRa merupakan perangkat dalam sistem komunikasi radio yang memanfaatkan teknik modulasi FM.

Memiliki jarak jangkauan yang mampu mencapai 15 KM dan berdaya rendah [6]. Selain itu LoRa menunjukkan kompatibel dan performa yang baik dalam sensor jaringan [7]**.** LoRa bekerja pada frekuensi 433 MHz di Asia, 868 MHz di Eropa, dan 915 MHz di Amerika [8].

Permasalahan dalam menerapkan LoRa berada pada keamanan data dalam pemantauan jarak jauh yang menggunakan transmisi via nirkabel. Informasi dari data menjadi rentan terkena serangan oleh pihak yang tidak bertanggung jawab. Serangan tersebut dapat berbentuk penyadapan, modifikasi dan pencurian informasi [9]. Salah satu mekanisme untuk menjaga kerahasian suatu pesan dengan mengimplementasikan kriptografi. Algoritme yang aman dan sering digunakan adalah Algoritme AES (*Advanced Encryption Standard*). Algoritme AES adalah suatu algoritme block chipper dan bersifat simetri yang menggunakan kunci simetri pada proses enkripsi dan dekripsi. AES memiliki kelebihan pada kecepatan, efisien, dan keamanan yang sangat baik [10].

Berdasarkan latar belakang diatas, peneliti akan merancang bangun sebuah prototipe sistem pemantauan getaran gempa bumi yang mengimplementasikan algoritme AES-256 menggunakan perangkat LoRa untuk pengiriman informasi darurat yang aman, dan peneliti akan melakukan uji coba simulasi pada sistem dengan jarak jauh. Pengujian dilakukan dengan membandingkan hasil performa dari kedua skema yaitu sistem tanpa AES dan sistem dengan AES.

2. LANDASAN TEORI

Pada bagian ini akan disampaikan beberapa landasan teori yang menjadi acuan dalam penelitian ini, mulai dari Algoritme AES, LoRa (*Long Range*), Sensor SW-420, Antena Yagi.

2.1 Algoritme AES

AES (*Advanced Encryption Standard*) merupakan algoritme *cryptographic* yang digunakan untuk mengamankan data [11]. Algoritme AES adalah suatu algoritme *block chipper* dan bersifat simetri yang menggunakan kunci simetri dalam proses enkripsi dan dekripsi [12]. Pada tahun 2001, AES didesain oleh Vincent Rijmen dan John Daemen dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai standar algoritme terbaru menggantikan algoritme DES (*Data Encryption Standard*) [13]. Algoritme AES memiliki panjang kunci yang bervariasi yaitu 128 bit, 192 bit, dan 256 bit [14].

2.2 LoRa (Long Range)

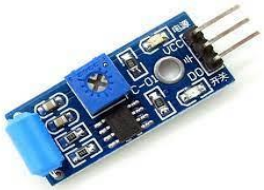
LoRa (*Long Range*) merupakan teknik modulasi *spread spectrum* dari teknologi CSS (*Chirp Spread Spectrum)* yang dibuat oleh Semtech [15]. Inti pada pemrosesan menghasilkan nilai frekuensi yang stabil. Sistem transmisi menggunakan PSK (*Phase Shift Keying*), FSK (*Frequency Shift Keying*) dan lainnya. LoRa memiliki dua lapisan berbeda yaitu *physical layer* yang menggunakan teknik modulasi radio *Chirp Spread Spectrum* (CSS) dan MAC *layer protocol* (LoRaWAN) [16]. *Long range* adalah teknologi nirkabel berdaya rendah yang menggunakan spektrum radio dengan nilai frekuansi bervariasi sesuai daerahnya 433 MHz di Asia, 868 MHz di Eropa, dan 915 MHz di Amerika [17]. Pada penelitian ini menggunakan Dragino LoRa Mini Dev 433 MHz dan LoRa Ra-02 433 MHz. Berikut merupakan modul Dragino LoRa Mini Dev pada Gambar 1 dan modul LoRa Ra-02 pada Gambar 2.

Gambar 1. Dragino LoRa Mini Dev 433 Mhz [18]

Gambar 2. LoRa Ra—02 [19]

2.3 Sensor SW-420

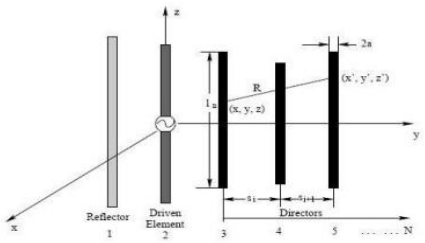
Sensor SW-420 merupakan sensor yang bereaksi terhadap getaran dari berbagai sudut. Cara kerja sensor ini adalah selama tidak ada getaran sensor memberikan Logic Low, sedangkan jika terdapat getaran sensor akan Logic High [20]. Modul ini terdiri dari resistor, kapasitor, potensiometer, IC LM393, daya dan LED. Manfaat modul ini yaitu untuk berbagai pemicu getaran, alarm pencurian, *smart car*, dan gempa bumi. Berikut merupakan modul Sensor SW-420 pada Gambar 3.



Gambar 3. Sensor SW-420 [20]

2.4 Antena Yagi

Antena Yagi merupakan antena *directional* yang terdiri dari elemen *dipole* paralel dalam satu garis. Antena ini ditemukan oleh Shintaro Uda dan Hidetsugu yagi pada tahun 1926, digunakan pada perang dunia II dalam sistem radar [21]. Antena Yagi terdiri dari sebuah *reflector*, *driven element*, dan beberapa *directors* yang dirangkai pada sebuah *Boom* pada Gambar 4.

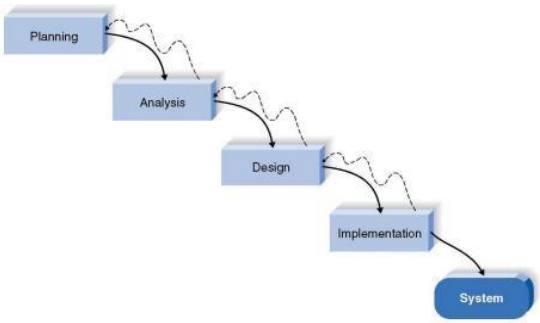


Gambar 4. Elemen Antena Yagi [22]

3. METODE PENELITIAN

Pada penelitian ini menggunakan metodologi penelitian *System Development Life Cycle* (SDLC) dengan pendekatan *waterfall Development*. SDLC adalah proses pembuatan, pengubahan sistem serta model untuk mengembangkan sebuah sistem. Pada metode pendekatan *waterfall Development* merupakan suatu metode pengembangan dimana pengerjaannya dilakukan secara terstruktur dan berurutan tahapannya. Selain itu memiliki kelebihan yaitu kebutuhan sistem sudah diidentifikasi dengan jelas dari tahap awal sehingga menyebabkan kecil adanya perubahan pada sistem [9].

Metode SDLC dengan pendekatan *waterfall Development* terdiri dari 4 tahapan yaitu *planning*, *analysis*, *design*, dan *implementation*. Tahap *planning* yaitu diawali dengan studi literatur dan konsultasi. Kemudian tahap *analysis* yaitu untuk menganalisis apa saja kebutuhan dari sistem, mulai dari kebutuhan perangkat keras, perangkat lunak, kebutuhan fungsional dan non fungsional dari sistem yang akan dibangun. Selanjutnya tahap *design* yaitu untuk membantu dalam menentukan model penelitian yang akan dilakukan, perangkat keras dan lunak yang digunakan, dan semua kebutuhan yang ada pada penelitian. Terakhir tahap implementation yaitu untuk menerapkan desain beserta pembahasan dengan melakukan pemrograman hasil rancangan yang telah dibuat dan mengintegrasikan seluruh sistem sehingga menghasilkan prototipe. Berikut adalah tahapan penelitian dengan pendekatan *waterfall* dapat dilihat pada Gambar 5.



Gambar 5. SDLC Pendekatan Waterfall Development [23]

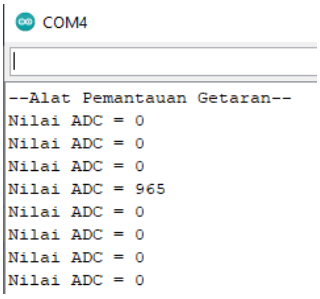
4. HASIL DAN PEMBAHASAN

4.1. Implementasi

Implementasi dilakukan dengan mengintegrasikan setiap perangkat menjadi sebuah prototipe. Perangkat tersebut terdiri dari Sensor SW-420, GPS Ublox Neo 6M, LED, Buzzer, Dragino LoRa Mini Dev 433 MHz, Antena Yagi, LoRa Ra-02 433 MHz, Arduino Uno, Micro SD Card Adapter, dan OLED display 128x64.

a. Implementasi Sensor SW-420

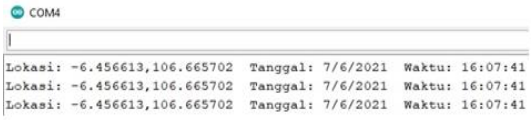
Implementasi sensor SW-420 berfungsi untuk mendeteksi adanya getaran maka data akan dikirimkan ke Dragino LoRa Mini Dev 433 MHz. Saat getaran dengan nilai ADC > 700 data akan dikirim ke perangkat *receiver*. Hasil implementasi dilakukan dengan cara simulasi gempa yaitu perangkat diletakkan diatas meja, kemudian meja digetarkan sebagai bukti sensor mendeteksi atau tidak getaran. Berikut hasil implementasi sensor SW-420 yang ditampilkan pada *serial monitor* pada Gambar 6.



Gambar 6. Hasil Implementasi Sensor SW-420

b. Implementasi GPS Ublox Neo 6M

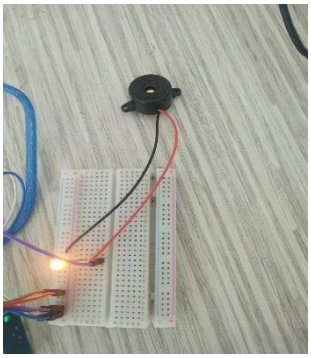
Implementasi GPS Ublox Neo 6M berfungsi untuk mengirimkan data berupa lokasi, tanggal dan waktu pada saat getaran terjadi ke Dragino LoRa Mini Dev 433 Mhz. Berikut hasil implementasi GPS Ublox Neo 6M yang ditampilkan pada *serial monitor* pada Gambar 7.



Gambar 7. Hasil Implementasi GPS Ublox Neo 6M

c. Implementasi LED dan Buzzer

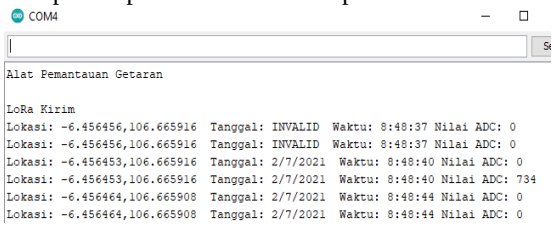
Implementasi LED dan Buzzer berfungsi sebagai penanda peringatan dini terjadi gempa. LED dan Buzzer akan menyala pada saat getaran dengan nilai ADC > 700. Berikut hasil implementasi LED dan Buzzer pada Gambar 8.



Gambar 8. Hasil Implementasi LED dan Buzzer

d. Implementasi Dragino LoRa Mini Dev 433 MHz

Implementasi Dragino LoRa Mini Dev 433 MHz berfungsi sebagai pemroses utama pada perangkat *transmitter*. Data yang diterima oleh Dragino LoRa Mini Dev saat getaran dengan nilai ADC > 700 akan dikirimkan melalui jaringan transmisi pada frekuensi 433 MHz ke perangkat *receiver*. Berikut hasil Implementasi Dragino LoRa Mini Dev yang ditampilkan pada *serial monitor* pada Gambar 9.



Gambar 9. Hasil Implementasi Dragino LoRa Mini Dev 433 MHz

e. Implementasi Antena Yagi

Dalam penelitian ini diimplementasikan dua buah antena Yagi 10 elemen yang sama untuk kedua sisi baik perangkat *transmitter* dan *receiver*. Antena tersebut dihubungkan dengan perangkat menggunakan kabel *coaxial*. Berikut implementasi antena Yagi di perangkat *transmitter* pada Gambar 10 dan antena Yagi di perangkat *receiver* pada Gambar 11.

Gambar 10. Implementasi Antena Yagi di *Transmitter*

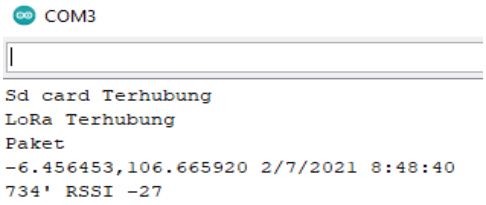
Gambar 11. Implementasi Antena Yagi di *Receiver*

f. Implementasi LoRa Ra-02

Implementasi LoRa 433 MHz berfungsi sebagai penerima data dari Dragino LoRa Mini Dev 433 MHz, selanjutnya akan di proses mikrokontroler Arduino Uno. Hasil implementasi LoRa Ra-02 433 MHz yang telah terintegarasi dengan mikrokontroler Arduino Uno pada Gambar 12.

g. Implementasi Arduino Uno

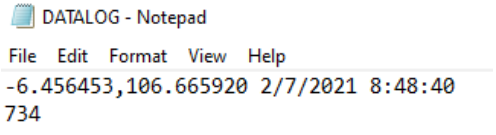
Implementasi Arduino Uno berfungsi sebagai pemroses utama dalam mengelola data yang diterima dengan LoRa Ra-02 433 MHz pada perangkat *receiver*. Berikut hasil implementasi Arduino Uno terintegrasi dengan LoRa Ra-02 yang ditampilkan pada *serial monitor* pada Gambar 12.



Gambar 12. Implementasi Arduino Uno Terintegrasi Dengan LoRa Ra-02

h. Implementasi Micro SD Card Adapter

Implementasi Micro SD Card berfungsi sebagai penyimpanan data yang diterima oleh perangkat receiver dalam bentuk file.txt. Berikut hasil implementasi Micro SD Card Adapter disimpan pada file DATALOG.txt pada Gambar 13.



Gambar 13. Implementasi Micro SD Card Adapter

i. Implementasi OLED Display 128x64

Implementasi OLED display 128x64 berfungsi sebagai *output* dari hasil data yang diterima oleh perangkat receiver. Berikut hasil implementasi OLED *display* 128x64 pada Gambar 14.

Gambar 14. Implementasi OLED *Display* 128x64

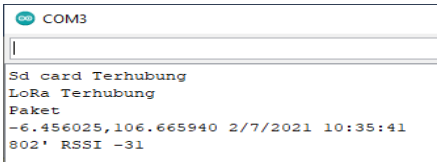
j. Implementasi Algoritme AES

Pada penelitian ini algoritme AES-256 digunakan sebagai algoritme untuk mengenkripsi data informasi pemantauan getaran gempa sehingga data aman dari ancaman pihak ketiga. Implementasi algoritme AES-256 pada perangkat *transmitter* bertujuan untuk mengenkripsi data informasi yang akan dikirim. Data pada Dragino LoRa Mini Dev dilakukan proses enkripsi dengan algortime AES-256 sehingga menghasilkan *ciphertext*. Kemudian dilakukan *encoding* hasil *ciphertext* untuk diubah menjadi

format Base-64. Hasil nilai ADC jika >700, *ciphertext* dikirim ke perangkat *receiver* menggunakan LoRa dengan frekuensi 433 MHz. Berikut hasil *ciphertext* ditampilkan pada *serial monitor* di perangkat *transmitter* pada Gambar 15.

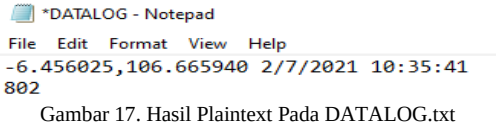
Implementasi algoritme AES-256 pada perangkat *receiver* bertujuan untuk mendekripsi data informasi yang diterima. Modul LoRa Ra-02 yang telah terintegrasi dengan Arduino Uno menerima data dari *transmitter* melalui frekuensi 433 MHz berupa *ciphertext*. Pada mikrokontroler Arduino Uno dilakukan proses *decoding* hasil *ciphertext* dengan format Base-64 menjadi format semula, selanjutnya dilakukan proses dekripsi menggunakan algoritme AES-256 sehingga menghasilkan *plaintext*. Berikut hasil *plaintext* ditampilkan pada serial monitor di perangkat *receiver* pada Gambar 16.

Gambar 15. Hasil Ciphertext Pada *Serial Monitor* di *Transmitter*



Gambar 16. Hasil Plaintext Pada Serial Monitor di *Receiver*

Gambar 16 merupakan hasil *plaintext* terdiri dari lokasi, tanggal, waktu, dan nilai ADC (*Analog to Digital Converter*). Informasi lokasi terdiri dari titik nilai *latitude* dan *longitude*. Informasi tanggal terdiri dari hari, bulan, dan tahun. Informasi waktu terdiri dari jam, menit, dan detik. Sedangkan nilai ADC adalah nilai kekuatan getaran. Selain itu terdapat nilai RSSI (*Received Signal Strength Indicator*) berfungsi untuk mengukur kekuatan sinyal yang diterima. Selanjutnya hasil *plaintext* tersebut disimpan di SD card dalam bentuk file datalog.txt dan ditampilkan pada OLED *display*. Berikut hasil *plaintext* yang disimpan dalam file DATALOG.txt pada Gambar 17 dan Gambar 18 merupakan tampilan *output* pada OLED display 128x64 .



Gambar 17. Hasil Plaintext Pada DATALOG.txt

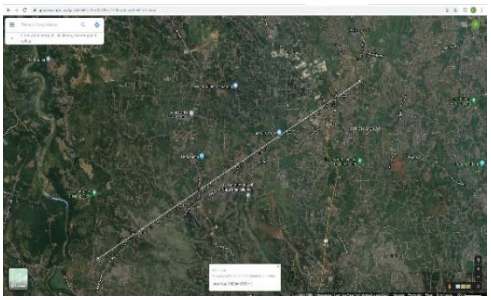
Gambar 18. Tampilan *output* pada OLED display 128x64

4.2. *Performance Testing*

Performance testing bertujuan untuk menguji tingkat keberhasilan dan mengukur performa pada prototipe yang dibangun dari beberapa parameter seperti jarak maksimal yang dicapai dalam berkomunikasi, nilai ADC (getaran), RSSI (*Receive Signal Strength*), dan kecepatan transmisi. Pengujian ini dilakukan dengan dua skema yaitu sistem tanpa AES dan sistem dengan AES. Masing-masing skema terdapat dua kondisi yaitu LOS dan NLOS. Pengujian dilakukan sebanyak 10 kali di setiap lokasi. Waktu pengujian selama dua hari pada tanggal 03 Juli 2021 dan 10 Juli 2021.

a. LOS (*Line of Sight*)

LOS merupakan kondisi dimana antara *transmitter* (TX) dan *receiver* (RX) tidak memiliki hambatan atau halangan. Terdapat 8 lokasi yang dilakukan dalam pengujian dengan jarak maksimal 9600 M. Lokasi perangkat *transmitter* di kampus PoltekSSN sedangkan perangkat *receiver* di kantor Pusdiklat BSSN, Bogor dapat dilihat pada Gambar 19.



Gambar 19. Lokasi Perangkat Jarak 9600 Meter dalam *Google Maps*

Hasil pengujian terbagi menjadi dua skema yaitu sistem tanpa AES dan dengan AES. Berikut hasil pengujian sistem tanpa AES pada Tabel 1 dan sistem dengan AES pada Tabel 2.

Tabel 1. Hasil Rata-Rata Pengujian Kondisi LOS Tanpa AES

Jarak (Meter)	Nilai ADC (Getaran)	RSSI (dBm)	Kecepatan Transmisi (ms)
500	842	-88,8	466,7
1500	846,7	-96,5	965,9
3000	835,6	-113,2	1088,4
4500	824	-97,6	930,9
6000	849,3	-118,5	1308
7000	851,4	-119,8	1513,2
7500	837,6	-120,4	1546,9
9600	843,9	-98	1039,5

Tabel 2. Hasil Rata-Rata Pengujian Kondisi LOS Dengan AES

Jarak (Meter)	Nilai ADC (Getaran)	RSSI (dBm)	Kecepatan Transmisi (ms)
500	845,3	-89,1	479,7
1500	815,5	-97,7	977,6
3000	837,4	-114,7	1113
4500	818,8	-100,1	964
6000	839	-119	1344,7
7000	846,6	-120,3	1539,9
7500	857,3	-121,6	1595,5
9600	833,5	-100,7	1198,4

b. NLOS (Non Line of Sight)

NLOS merupakan kondisi dimana antara *transmitter* (TX) dan *receiver* (RX) memiliki memiliki hambatan atau halangan seperti bangunan, pohon, dan benda lainnya. Terdapat 5 lokasi yang dilakukan dalam pengujian dengan jarak maksimal 6000 Meter. Lokasi perangkat *transmitter* di kampus PoltekSSN sedangkan perangkat *receiver* di jalan Parung Panjang, Sukasari, Rumpin, Bogor dapat dilihat pada Gambar 20.

Gambar 20. Lokasi Perangkat Jarak 6000 Meter dalam *Google Maps*

Hasil pengujian terbagi menjadi dua skema yaitu sistem tanpa AES dan dengan AES. Berikut hasil pengujian sistem tanpa AES pada Tabel 3 dan sistem dengan AES pada Tabel 4.

Tabel 3. Hasil Rata-Rata Pengujian Kondisi NLOS Tanpa AES

Jarak (Meter)	Nilai ADC (Getaran)	RSSI (dBm)	Kecepatan Transmisi (ms)
500	854,9	-92,3	663,9
1500	843	-105,5	1032,4
3000	849,9	-118,1	1218,8
4500	841,7	-102,1	981,4
6000	890,8	-121,7	1547,9

Tabel 2. Hasil Rata-Rata Pengujian Kondisi NLOS Dengan AES

Jarak (Meter)	Nilai ADC (Getaran)	RSSI (dBm)	Kecepatan Transmisi (ms)
500	860,4	-93,2	789,4
1500	820,3	-109,9	1067,1
3000	831,3	-118,8	1228,3
4500	842,6	-108,7	1024,6
6000	857,3	-123,7	1621

5. KESIMPULAN

Sistem pemantauan getaran gempa bumi yang mengimplementasi algoritme AES-25 mengunakan perangkat LoRa berhasil dibangun sesuai yang diharapkan dan berjalan dengan baik. Berdasarkan hasil *perfomance testing* menunjukkan jarak maksimal yang dicapai dalam berkomunikasi pada kondisi LOS adalah 9600 Meter sedangkan kondisi NLOS mencapai 6000 Meter. Nilai ADC (getaran) tertinggi pada jarak 1500 Meter kondisi LOS dengan AES adalah 815,5 sedangkan nilai terendah pada jarak 6000 Meter kondisi NLOS tanpa AES. Hasil rata-rata nilai RSSI tertinggi pada jarak 500 Meter kondisi LOS tanpa AES adalah -88,8 dBm sedangkan nilai terendah pada jarak 6000 Meter kondisi NLOS dengan AES adalah -123,7 dBm. Hasil rata-rata kecepatan transmisi tercepat pada jarak 500 M kondisi LOS tanpa AES adalah 466,7 ms sedangkan rata-rata kecepatan transmisi terlama pada jarak 6000 M kondisi NLOS dengan AES adalah 1621 ms.

Dari hasil pengujian bahwa sistem dengan AES memiliki kecepatan transmisi lebih lambat dibandingkan dengan sistem tanpa AES. Hal ini disebabkan sistem dengan AES terdapat proses enkripsi dan dekripsi data. Berdasarkan hasil tersebut disimpulkan bahwa prototipe berhasil melakukan proses kirim terima data dengan baik.

REFERENSI

[1] BMKG, *Katalog Gempabumi Signifikan dan Dirasakan*. Jakarta: BMKG, 2018

[2] J. F. Saputra, M. Rosmiati, and M. I. Sari, "Pembangunan Prototype Sistem Monitoring Getaran Gempa Menggunakan Sensor Module SW-420," *e-Proceding Appl. Sci.*, vol. 4, no. 3, pp. 2055–2068, 2018.

[3] P. Boccadoro, B. Montaruli, and L. A. Grieco, "QuakeSense, a LoRa-compliant Earthquake Monitoring Open System," *Proc. - 2019 IEEE/ACM 23rd Int. Symp. Distrib. Simul. Real Time Appl. DS-RT 2019*, pp. 1–8, 2019, doi: 10.1109/DS-RT47707.2019.8958675.

[4] R. P. Centelles, F. Freitag, R. Meseguer, L. Navarro, S. F. Ochoa, and R. M. Santos, "A LoRa-Based Communication System for Coordinated Response in an Earthquake Aftermath," *Proceedings*, vol. 31, no. 1, p. 73, 2019, doi: 10.3390/proceedings2019031073.

[5] A. Lavric, "LoRa (long-range) high-density sensors for internet of things," *J. Sensors*, vol. 2019, 2019, doi: 10.1155/2019/3502987.

[6] L. Sciullo, F. Fossemó, A. Trotta, and M. Di Felice, "LOCATE: A LoRa-based mObile emergenCy mAnagement sysTEm," *2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc.*, pp. 1–7, 2018, doi: 10.1109/GLOCOM.2018.8647177.

[7] P. Ragam and D. S. Nimaje, "Performance evaluation of LoRa LPWAN technology for IoT-based blast-induced ground vibration system," *J. Meas. Eng.*, vol. 7, no. 3, pp. 119–133, 2019, doi: 10.21595/jme.2019.20586.

[8] M. Saari, A. Muzaffar Bin Baharudin, P. Sillberg, S. Hyrynsalmi, and W. Yan, "LoRa - A survey of recent research trends," *2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc.*, pp. 872–877, 2018, doi: 10.23919/MIPRO.2018.8400161.

[9] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring The Security Vulnerabilities of LoRa," *IEEE Int. Conf. Cybern.*, 2017, doi: 10.1109/CYBConf.2017.7985777.

[10] A. Jamaluddin, N. N. Mohamed, and H. Hashim, "Securing RF communication using AES-256 symmetric encryption: A performance evaluation," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 217–222, 2018, doi: 10.14419/ijet.v7i4.11.20810.

[11] A. M. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," *Cryptogr. Netw. Secur.*, 2017.

[12] S. Wadehra, S. Goel, and N. Sengar, "AES Algorithm : Encryption and Decryption," *Int. J. Trend Sci. Res. Dev. (IJTSRD)*, pp. 1075–1077, 2018.

[13] M. Rizal, E. M. Zamzami, and M. Zarlis, "Cryptographic Symmetry Analysis with AES Algorithm for Safeguarding Data at Government Agencies," *Int. J. Inf. Syst. Technol.*, vol. 3, no. 1, pp. 131–139, 2019.

[14] E. P. Nugroho, R. R. J. Putra, and I. M. Ramadhan, "SMS Authentication Code Generated by Advance Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account," *Int. Conf. Sci. Inf. Technol.*, pp. 175–180, 2016.

[15] "Semtech LoRa Technology Overview." https://www.semtech.com (accessed Nov. 16, 2020).

[16] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A Study of LoRa : Long Range & Low Power Networks for the Internet of Things," *J. Sensors*, pp. 1–18, 2016, doi: 10.3390/s16091466.

[17] S. Sagir, I. Kaya, C. Sisman, Y. Baltaci, and S. Unal, "Evaluation of Low-Power Long Distance Radio Communication in Urban Areas : LoRa and Impact of Spreading Factor," *IEEE*, pp. 68–71, 2019.

[18] "SX127X Mini Dev featuring LoRa® technology." https://www.dragino.com/products/lora/item/126-lora-mini-dev.html (accessed Nov. 16, 2020).

[19] A. Raj, "Interfacing SX1278 (Ra-02) LoRa Module with Arduino." https://circuitdigest.com/microcontroller-projects/arduino-lora-sx1278-interfacing-tutorial (accessed Mar. 02, 2021).

[20] "SW-420 Vibration Sensor Module," *Components 101*, 2020. https://components101.com/sensors/sw-420-vibration-sensor-module (accessed Dec. 20, 2020).

[21] U. Antenna, "A Review on Recent Ternds and Developments in the Design and Application A Review on Recent Ternds and Developments in the Design and Application of Yagi Uda Antenna," no. September, 2015, doi: 10.9790/2834-10522834.

[22] M. Abdulhamid, "ANALYSIS AND DESIGN OF 10-ELEMENT YAGI-UDA ANTENNA," *JOURNSL RADIO Electron.*, pp. 1–11, 2020, doi: 10.30898/1684-1719.2020.3.10.

[23] A. Dennis, B. H. Wixom, and R. M. Roth, "System Analysis and Design 5th Edition," USA: John Wiley & Sons, lnc., 2015.