KEAMANAN *WIRELESS SENSOR NETWORK* PENDETEKSI KEBAKARAN HUTAN MENGGUNAKAN ALGORITMA AES PADA MEDIA KOMUNIKASI LORA

(*Wireless Sensor Network Security for Forest Fire Detection Using Aes Algorithm on Lora Communication Media*)

Abdul Rahman[1)], Muhammad Sya'ban Nugroho[2*)]

[1,2)]Universitas Multi Data Palembang
e-mail: arahman@mdp.ac.id, abanaban6@mhs.mdp.ac.id
[*)] penulis korespondensi

Abstract. Indonesia has a vast forest area reaching 120.3 million ha in 2020. Forest fires (karhutla) in Indonesia are a problem that is often faced every year during the dry season. The development of the Wireless Sensor Network (WSN) makes it possible to place fire detection sensors in forest areas, also supported by Longe Range (LoRa) communication technology so that the range of WSN is very far. The security of data sent by sensors via WSN is essential to prevent parties from manipulating the sensor data sent. This study developed a security system for data transmitted from WSN to LoRa gateway using a 128-bit AES security system. AES is symmetric encryption, and its computational complexity is relatively tiny, so it is very suitable to be implemented in WSN. The results of this study indicate that the data read by the sensor via WSN with 128-bit AES encryption and sent to the LoRa gateway can be appropriately read using the same encryption key as the key installed on the WSN; meanwhile, if the key used is not the same, sensor data sent from WSN cannot be displayed correctly.

Keywords: AES, Forest fires, Wireless Sensor Network, LoRa, Security

1. Pendahuluan

Indonesia mempunyai kawasan hutan yang cukup luas, yaitu 120,3 juta ha pada tahun 2020 [17]. Permasalahan yang sering terjadi pada kawasan hutan di Indonesia adalah sering terjadinya kebakaran hutan dan lahan (karhutla). Pada sepanjang tahun 2021 luas area yang terjadi karhutla mengalami peningkatan jika dibandingkan dengan karhutla pada tahun 2020, data dari kementerian lingkungan hidup dan kehutanan (KLHK) mencatat bahwa di Indonesia luas hutan dan lahan yang terbakar mencapai 354,582 ha, dimana jumlah ini mengalami peningkatan sebesar 19,4 % dibandingkan karhutla tahun 2020 [7]. Karhutla di Indonesia tidak hanya menjadi perhatian di dalam negeri tetapi juga menjadi perhatian negara-negara lain, sehingga dampak karhutla di Indonesia menjadi perhatian tidak hanya lokal, nasional bahkan menjadi perhatian secara global [9]. Lahan gambut yang terbakar mengeluarkan lebih banyak kabut dibandingkan dengan tanah mineral, diperkirakan total emisi dari karhutla di Indonesia pada tahun 2015 adalah setara dengan 1,2 miliar ton CO_2 [12].

Pemanfaatan teknologi telah dikembangkan untuk penanganan karhutla, diantaranya: implementasi algoritma *Naïve Bayes* untuk deteksi titik api [16], *fuzzy time series*

digunakan untuk memprediksi jumlah kemunculan titik api [6], algoritma *K-Means* digunakan untuk menentukan daerah rawan titik api di provinsi Riau [27], pemanfaatan kamera untuk mendeteksi munculnya titik api dengan notifikasi menggunakan *sms gateway* [8].

Perkembangan teknologi *Internet of Thing* (IoT), penggunaan *Wireless Sensor Network* (*WSN*) menjadi kebutuhan untuk menempatkan sensor yang dapat dipantau jarak jauh. *WSN* merupakan sebuah sistem terdistribusi yang terdiri dari node dengan kemampuan untuk memperoleh informasi tentang kondisi lingkungan dan mengirimkannya secara nirkabel ke stasiun pangkalan (*base station*) untuk dilakukan proses selanjutnya [6, 30a]. Gangguan keamanan *WSN* memerlukan aktivitas fisik di dekat *WSN* untuk menambahkan node berbahaya ke jaringan yang ada atau untuk memblokir atau menangkap data yang dikirimkan. *WSN* yang terhubung ke jaringan internet memungkinkan penyerang dari seluruh dunia untuk melakukan aktivitas kejahatan pada jaringan ini [29, 11]. Media komunikasi menggunakan *LoRa (Long Range)* merupakan teknologi yang dapat digunakan pada implementasi *IoT* dengan melibatkan *WSN* sebagai data masukan. Jaringan *LoRa* menyediakan enkripsi data untuk transmisi *end-to-end* dari perangkat akhir ke *server* jaringan dengan menggunakan *Network Session Key* (*NwkSKey*) dan dari perangkat akhir ke *server* aplikasi dengan memanfaatkan *Application Session Key* (*AppSKey*) [28].

Advanced Encryption Standard (*AES*) adalah algoritma *block cipher* yang banyak digunakan [10], dan juga merupakan salah satu metode enkripsi yang paling umum digunakan pada perangkat *IoT* [28]. *AES* adalah enkripsi simetris, dan kompleksitas komputasinya relatif kecil dibandingkan dengan enkripsi asimetris lainnya. Oleh karena itu lebih cocok untuk perangkat *IoT* yang memiliki kemampuan komputasi yang sederhana [4, 13, 32].

Sensor deteksi kebakaran hutan menggunakan *WSN* dapat digunakan untuk mendeteksi lebih dini terjadinya kebakaran hutan. Data deteksi kebakaran hutan menggunakan *WSN* ini dikirimkan melalui jaringan *wireless* dengan media komunikasi *LoRA* sangat rawan disusupi oleh pihak-pihak yang tidak bertanggung jawab, yang menyebabkan data yang dikirimkan oleh *WSN* dapat di manipulasi. Oleh sebab itu pada penelitian ini dibuat sistem keamanan data pada *WSN* dengan menerapkan algoritma *AES* untuk mengamankan data yang dikirimkan *WSN* untuk mendeteksi terjadinya karhutla.

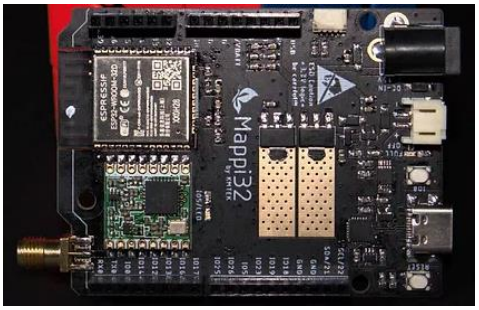
A. *Wireless Sensor Network* (*WSN*)

Kemajuan terbaru dalam komunikasi *wireless*, dan komputer serta perkembangan teknologi mikroelektronik telah memungkinkan berkembangnya sensor-sensor dengan ukuran yang kecil, murah, dan multifungsi. Sensor ini biasanya digunakan di area target melalui cara acak untuk memantau fitur fisik lingkungan seperti suhu, kelembaban, dan tekanan. Data yang dipantau biasanya diteruskan ke pengumpul data (*sink*) menggunakan

metode kooperatif (umumnya multihop) dan mengirimkan data ke *server* data untuk selanjutnya dilakukan analisis data. Selain itu, sensor dapat mengatur diri sendiri berdasarkan kolaborasi lokal mereka untuk membentuk *Wireless Sensor Network* (*WSN*) [19, 31, 33]. Kombinasi teknologi *IoT* dan *WSN* telah banyak di implementasi dalam sistem pemantauan dan pendeteksian jarak jauh, seperti pemantau kualitas air [25], pemantauan hasil panen [5, 23, 18], sistem informasi pengangkutan sampah [25], deteksi kebocoran gas dan pemadam kebakaran [26].

B. *Long Range* (*LoRa*)

LoRa merupakan sebuah teknik modulasi *spread spectrum* yang berasal dari teknologi *chirp spread spectrum* (CSS). Teknik modulasi yang digunakan dalam *LoRa* membuatnya kuat untuk menyalurkan *noise* karena seluruh *bandwidth* yang dialokasikan digunakan untuk menyiarkan sinyal berupa informasi atau data. Selain itu, keamanan pada sistem *LoRa* dapat terjamin karena transmisi tersebar secara *pseudo-random* yang muncul seperti *noise*, oleh karena itu teknik modulasi telah memberikan keamanan dasar untuk sistem *LoRa* [1]. Selain itu, *LoRa* merupakan pilihan terbaik untuk mendukung implementasi *IoT* yang membutuhkan komunikasi data jarak jauh dengan penggunaan daya yang sangat kecil [34]. *LoRa* dapat beroperasi pada rentang frekuensi 434-928 MHz, hal ini bergantung terhadap regulasi penggunaan frekuensi di berbagai Negara. Untuk *LoRa* di Indonesia berada pada rentang frekuensi 920-923 MHz [14, 15].



Gambar 1. *Mappi32 Development Board* [2]

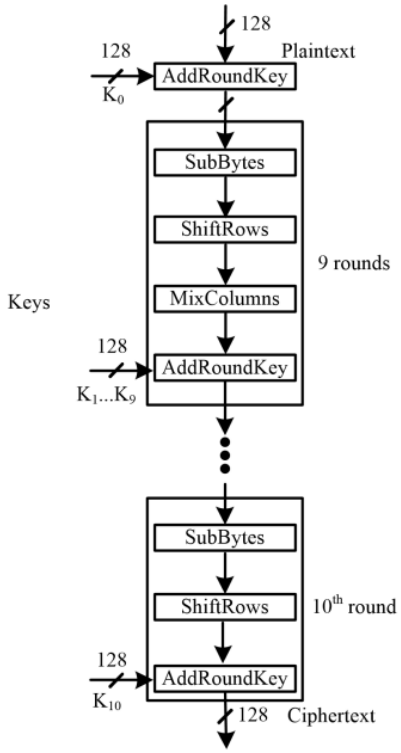
C. Mappi32

Mappi32 merupakan sebuah *development board* IoT yang dikeluarkan oleh KMTek (Karya Merapi Teknologi) Indonesia. Dalam sebuah *development board* ini sudah tertanam langsung *chip LoRa* dan *development board* ini dapat juga dipergunakan layaknya penggunaan Arduino. Mappi32 menggunakan frekuensi radio dalam melakukan pengiriman informasi, modul ini beroperasi pada rentan frekuensi 920-923 MHz yang dimana frekuensi ini merupakan frekuensi yang legal digunakan untuk penerapan *LoRa* di Indonesia. Frekuensi antara Mappi32 dengan LoRa *gateway* tentulah harus sama, sehingga komunikasi antar kedua *device* dapat dilakukan. Apabila ada perbedaan pada frekuensi pada salah *device*, maka data tidak akan dapat diterima maupun di kirim dari

sisi Mappi32 dan *LoRa gateway* [2]. Gambar 1 merupakan bentuk dari Mappi32 yang digunakan untuk *WSN* dan *LoRa gateway*.

D. *Advanced Encryption Standard* (*AES*)

AES digunakan untuk enkripsi dan dekripsi data, enkripsi mengambil data input dan mengubahnya menjadi *ciphertext*, dekripsi mengubah *ciphertext* kembali menjadi teks biasa dari input sebelumnya. Struktur *AES* didasarkan pada jaringan substitusi-permutasi, hal ini menjadikan proses bisa lebih cepat pada kedua perangkat keras dan perangkat lunak. *AES* memiliki ukuran kunci 128, 192 dan 256bit untuk enkripsi dan dekripsi data [3]. *AES* merupakan *chipher* simetris yang berarti bahwa *AES* akan menggunakan kunci yang sama untuk enkripsi dan dekripsi, oleh karena itu pengirim dan penerima harus mengetahui kunci rahasia yang sama. Algoritma enkripsi mendefinisikan sejumlah transformasi yang akan dilakukan pada *plaintext* [26].



Gambar 2. Diagram Alir Algoritma AES [26]

Pada algoritma *AES* 128-bit akan menggunakan 10 putaran (*round)* seperti diagram alir Gambar 2, dimana setiap putaran menggunakan kunci yang dihasilkan dari penjadwalan kunci. Pada putaran terakhir sedikit berbeda dari yang lain karena tidak menyertakan langkah *MixColumns.* Cara kerja *chipher* ini dapat dibagi menjadi dua bagian, yaitu: komputasi putaran (*round computation*) dan penjadwalan kunci (*key scheduling*) [26].

A. Komputasi Putaran

128-bit *plaintext* disimpan dalam *state-register* menggunakan matriks 4×4, dimana masing-masing menyimpan satu *byte*. Setiap bagian akan menjalani tiga langkah berikut:

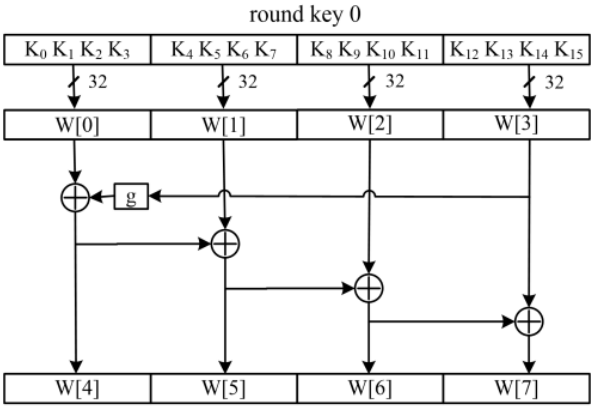
1. *Substitution Bytes*: pada langkah ini merupakan bagian paling kritis dari algoritma karena menghabiskan daya dan area terbesar. Setiap *byte* dalam *state-register* diganti dengan beberapa nilai yang telah ditentukan sebelumnya yang diperoleh setelah melakukan beberapa aritmatika bidang hingga di bidang Galois, GF (2^8).

2. *ShiftRows*: pada langkah ini melibatkan pergeseran siklus dari 3 baris terakhir dengan 1, 2 dan 3 tempat di *state-register*.

3. *MixColumns*: pada langkah ini dilakukan operasi pada *state* matriks dengan kolom demi kolom, dan melibatkan perkalian matriks dengan elemen matriks yang telah ditentukan.

B. Penjadwalan Kunci

Setiap putaran dalam desain akan menggunakan sebuah kunci yang diperoleh dari kunci sandi yang disepakati oleh kedua pihak yang berkomunikasi. Kunci putaran k1, k2, ... k10 dievaluasi dalam berbagai cara tergantung pada persyaratan dalam fungsi putaran. Hal ini biasanya diambil setiap kali putaran yang sesuai dimulai. Arsitektur internal dari penjadwalan kunci (*key-scheduler*) ditampilkan pada Gambar 3.



Gambar 3. Arsitektur Penjadwalan Kunci(*Key-Scheduler*)[8][26]

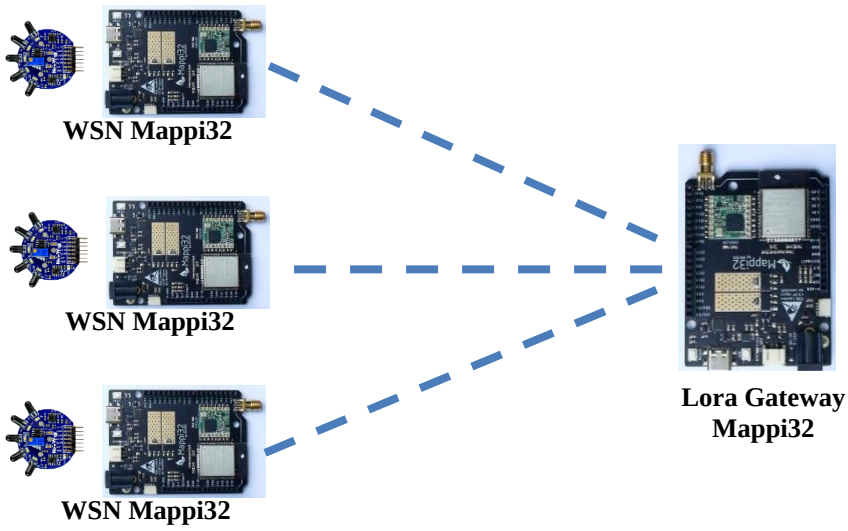
2. Metodologi

Pada penelitian ini dibagi menjadi dua tahapan, yaitu: perancangan perangkat keras untuk simulasi *WSN* deteksi kebakaran hutan dan perancangan perangkat lunak untuk

implementasi algoritma *AES*.

A. Perancangan Perangkat Keras

Pada penelitian ini perancangan perangkat keras yang dilakukan adalah membuat rancangan simulasi *WSN* untuk deteksi kebakaran menggunakan komunikasi *LoRa*. *Development kit* yang digunakan untuk *WSN* dan *LoRa gateway*, digunakan Mappi32 dengan sensor-sensor yang terpasang pada masing-masing node *WSN* terdiri dari sensor deteksi api modul *infrared IR flame* 5 *channel*, dan sensor deteksi suhu dan kelembaban menggunakan DHT11. Rancangan sistem simulasi *WSN* dengan komunikasi *LoRa* ditunjukkan pada Gambar 4.



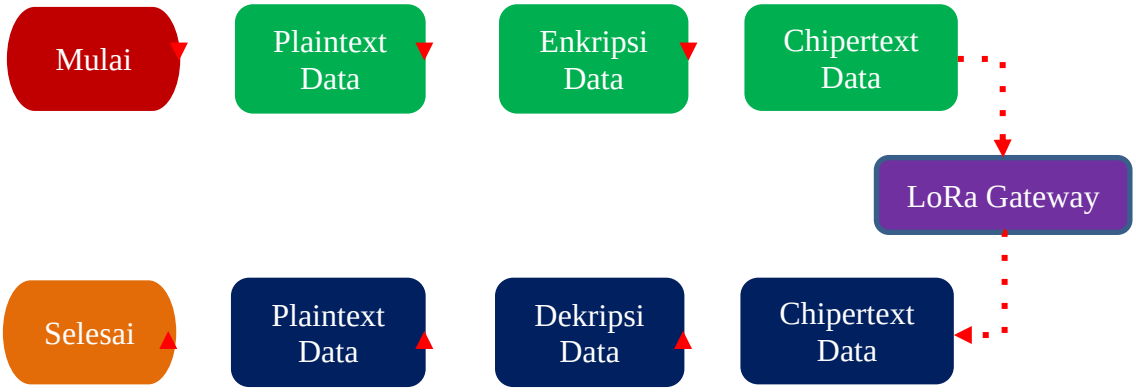
Gambar 4. Rancangan Simulasi WSN Deteksi Kebakaran Hutan

B. Perancangan Perangkat Lunak

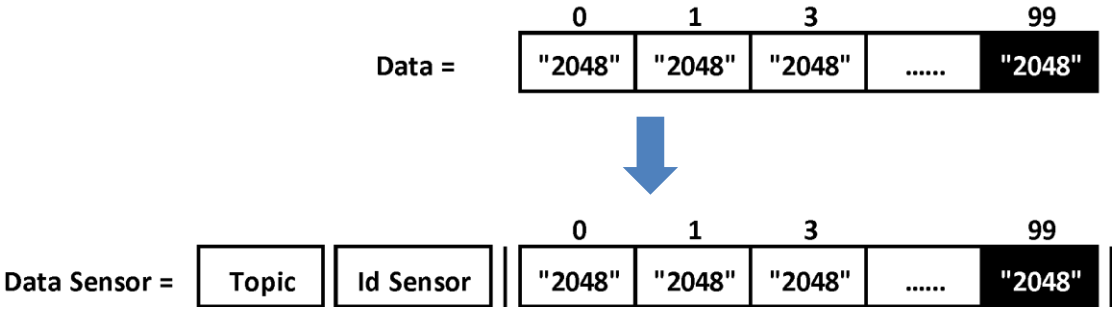
Diagram alir data mekanisme *end-to-end security* pada sistem secara umum dapat dilihat pada Gambar 5. Data sensor sebelum ditransmisikan ke *LoRa gateway* terlebih dahulu data di proses menggunakan algoritma *AES* dengan kunci 128-bit membentuk *chiphertext*. Hasil dari *chiphertext* ditransmisikan menggunakan media transmisi *LoRa*. Data yang diterima oleh *LoRa gateway* akan menjalankan proses dekripsi dengan cara menyamakan kunci *AES* yang ada pada node sensor dan *LoRa gateway*. Setelah itu data akan di dekripsi kembali menjadi *plaintext*.

Node sensor merekam data *sensor* yang menghasilkan beberapa jumlah data. Data tersebut berupa *list* dan akan dibagi ke dalam beberapa bentuk data untuk setiap transmisi untuk selanjutnya di enkripsi menggunakan algoritma *AES*. Pembagian data tersebut bertujuan untuk memaksimalkan ukuran *payload* yang dapat ditampung *LoRa* yaitu sekitar 256 *bytes* dalam satu kali transmisi, ilustrasi pembagian data dapat dilihat pada Gambar 6.

Payload yang diterima *gateway* akan diverifikasi dengan cara menyamakan kunci enkripsi dan dekripsi yang terdapat pada *node sensor* dan *gateway*. Jika kedua kunci tersebut sama/cocok, *chiphertext* dapat di dekripsi menjadi data yang dapat dibaca (*plaintext*). Proses ini dilakukan bertujuan untuk mengautentifikasi pesan yang masuk pada *gateway*.

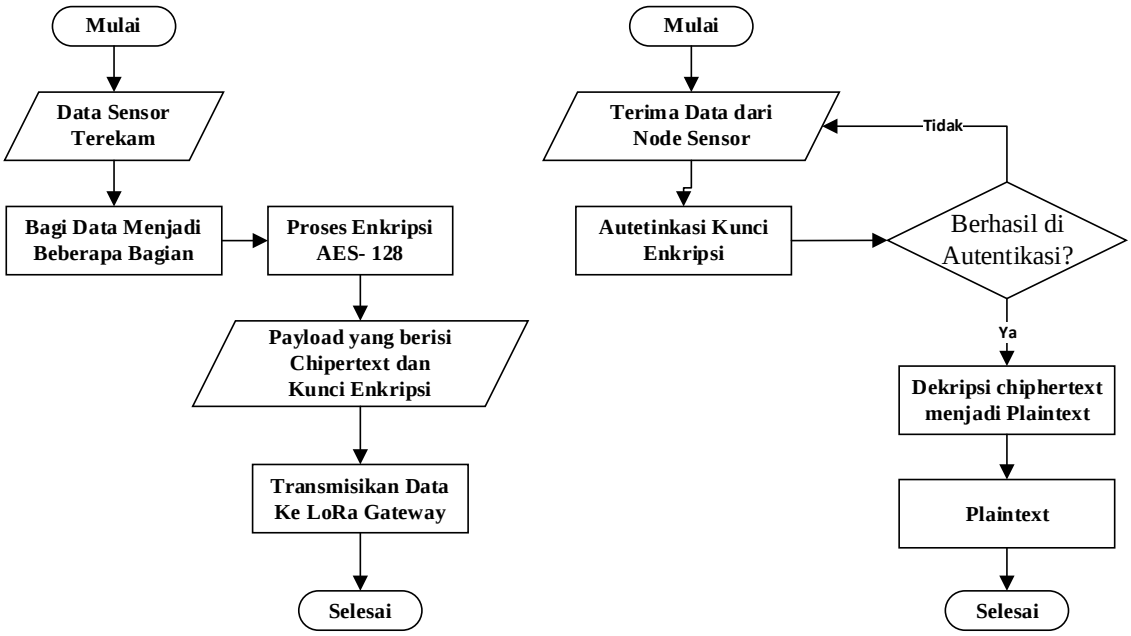


Gambar 5. Diagram Alir Mekanisme *End-to-End Security*



Gambar 6. Ilustrasi Pembagian Data

Tahapan implementasi perangkat lunak berdasarkan perancangan sistem yang telah ditentukan pada tahap sebelumnya dapat dilihat pada Gambar 7. Tahapan ini akan dimulai pada proses inisialisasi sensor terlebih dahulu, setelah itu sensor akan melakukan pembacaan kondisi lingkungan. Data yang didapat dari *node sensor* yang masih bersifat *plaintext* akan di enkripsi menjadi *chiphertext*, setelah melakukan proses enkripsi data menjadi *chiphertext* data ini selanjutnya di transmisikan ke *gateway* pada gelombang frekuensi *LoRa* 923 MHz menggunakan perangkat Mappi32, jika *gateway* menerima transmisi data dari sensor maka akan dilakukan proses dekripsi *chiphertext* kembali ke *plaintext* dengan menggunakan kunci deksripsi yang sama dengan kunci enkripsi dan menampilkan data pada *serial monitor*. Jika *gateway* belum menerima transmisi data dari node sensor maka node sensor akan mentransmisikan ulang data tersebut ke *gateway*.



Gambar 7. Diagram Alir Transmisi Data Sensor dari *Node* Sensor ke *LoRa Gateway*

3. Hasil dan Pembahasan

Proses implementasi enkripsi dan dekripsi pada data sensor yang ditransmisikan dari *WSN* ke *LoRa gateway* dilakukan secara bertahap dan sistematis hingga semua proses pendeteksi dapat dilakukan.

3.1 Pengujian Perangkat Keras

Pengujian perangkat keras pada penelitian ini dilakukan untuk memastikan rancangan sensor pendeteksi karhutla menggunakan *WSN* dapat terhubung dengan baik ke *LoRa gateway*. Pengujian dilakukan untuk mengetahui pengaruh *Line of Sight* (*LOS*) dan *None-Line of Sight* (*NLOS*) pada sistem pendeteksi karhutla yang dirancang, serta melakukan pengujian pada sensor deteksi api, sensor suhu, dan kelembaban. *LOS* merupakan teknik dalam melakukan transmisi sinyal antar dua stasiun yang saling terhubung dan benar-benar tidak ada objek yang menghalangi (bebas pandang) sehingga sinyal dari stasiun pengirim dapat langsung diterima oleh sisi stasiun penerima, sedangkan *NLOS* merupakan suatu kondisi dimana pandangan terhalang sebuah obyek sepenuhnya. Pada saat kondisi ini terjadi maka koneksi antara dua stasiun akan terhambat bahkan terputus.

Pengujian *LOS* dan *NLOS* untuk mengetahui kinerja teknologi *LoRa* dalam upaya mentransmisikan sebuah data yang berasal *node sensor* 1 dan *node sensor* 2 ke *gateway*. Pengujian dilakukan pada jarak antara 50 meter hingga 150 meter pada masing-masing *node sensor*. Jarak antara *node sensor 1* dan *node sensor 2* pada saat dilakukan pengujian

sekitar 5m hal ini dilakukan untuk mengurangi interferensi terhadap *node senor 1* dan *node sensor 2*. Lokasi pengujian dilakukan pada lokasi padat penduduk dan tempat terbuka. Pengujian ini dilakukan untuk melihat nilai *delay* dan kekuatan sinyal *(RSSI)* pada saat pengiriman data *node sensor* hingga data tersebut diterima oleh *gateway*. *Delay* merupakan waktu tunda suatu paket sebagai akibat dari proses transmisi yang terjadi melalui satu titik ke titik lain sebagai tujuannya. Hal-hal yang mempengaruhi nilai *delay* yaitu: jarak, media fisik, kongesti atau juga waktu proses yang lama. *RSSI*(*Received Signal Strength Indicator*) indikator untuk mengukur kekuatan sinyal, diamana semakin jauh jarak trasnmisinya, sinyal yang diterima akan semakin kecil yang berdampak pada pengiriman data yang semakin lama. Faktor-faktor yang mempengaruhi nilai RSSI adalah *noise, multi-path fading, power transmit,* dan hal-hal yang fluktuatif pada kekuatan yang diterima. Jika nilai RSSI mendekati 0 (nol), maka sinyal yang diterima akan bagus.

Tabel 1. Hasil Pengujian Node Sensor Pada Tempat Padat Penduduk (*NLOS*)

Jarak (meter)	***Delay* (detik)**		***RSSI* (dBm)**		**Status**	
	Node Sensor 1	**Node Sensor 2**	**Node Sensor 1**	**Node Sensor 2**	**Node Sensor 1**	**Node Sensor 2**
50	1	1	-44	-39	Terkirim	Terkirim
75	2	2	-56	-54	Terkirim	Terkirim
100	6	5	-64	-61	Terkirim	Terkirim
125	9	8	-71	-68	Terkirim	Terkirim
150	-	-	-	-	Tidak Terkirim	Tidak Terkirim
175	-	-	-	-	Tidak Terkirim	Tidak Terkirim

Tabel 2. Hasil Pengujian Node Sensor Pada Tempat Terbuka (*LOS*)

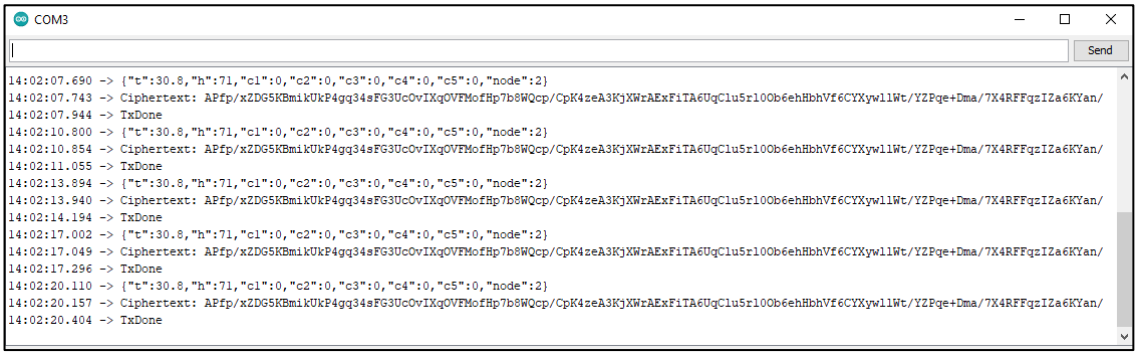
Jarak (meter)	***Delay* (detik)**		***RSSI* (dBm)**		**Status**	
	Node Sensor 1	**Node Sensor 2**	**Node Sensor 1**	**Node Sensor 2**	**Node Sensor 1**	**Node Sensor 2**
50	0	0	-34	-25	Terkirim	Terkirim
75	0	1	-48	-33	Terkirim	Terkirim
100	1	2	-53	-40	Terkirim	Terkirim
125	2	3	-67	-46	Terkirim	Terkirim
150	4	4	-71	-55	Terkirim	Terkirim
175	-	-	-	-	Tidak Terkirim	Tidak Terkirim

Berdasarkan hasil pengujian node sensor untuk lokasi padat penduduk (*NLOS*) pada tabel 1, terlihat bahwa baik node sensor 1 dan node sensor 2 masih dapat mengirimkan data pada jarak 125 meter. Pada node sensor 1 sinyal terkecil (*RSSI*) yang terdeteksi pada jarak 125m sebesar -71 dBm dan *delay* mencapai 9 detik, sedangkan pada node sensor 2 sinyal terkecil yang terdeteksi pada jarak 125m sebesar -68 dBm dan *delay* 8 detik. Pada pengujian node sensor untuk lokasi tempat terbuka (*LOS*) sesuai Tabel 2, hasilnya menunjukkan bahwa node sensor 1 dan node sensor 2 masih dapat mengirimkan data pada jarak 150 meter. Pada node sensor 1 sinyal terkecil yang terdeteksi pada jarak 150m

sebesar -71 dBm dan *delay* mencapai 4 detik, sedangkan pada node sensor 2 sinyal terkecil yang terdeteksi mencapai -55 dBm dengan *delay* sebesar 4 detik.

3.2 Pengujian Fungsional Sistem

Pengujian fungsional sistem dilakukan untuk mengetahui konsistensi fungsi-fungsi yang ada dari hasil perancangan serta implementasi *AES* pada *WSN* untuk sistem deteksi kahutla menggunakan komunikasi *LoRa*. Pada Gambar 8 hasil pembacaan data yang dilakukan oleh node sensor *WSN* dari sensor api dan sensor suhu masih dalam bentuk *plaintext*. Data dalam bentuk *plaintext* ini dilakukan proses enkripsi *AES* 128-bit menjadi *chiphertext*, setelah menjadi *chiphertext* data ditransmisikan ke *LoRa gateway*. Pada Gambar 9 menunjukkan bahwa pada *LoRa gateway* berhasil menerima data yang ditransmisikan dari node sensor *WSN*. Data yang diterima oleh *LoRa gateway* masih berbentuk *chiphertext*, kemudian di *LoRa gateway* dilakukan proses enkripsi menjadi *plaintext* agar data yang dikirim oleh node sensor *WSN* dapat dibaca kembali.



Gambar 8. Hasil Pengujian Proses Enkripsi Data pada Node Sensor *WSN*

Gambar 9. Hasil Pengujian Proses Dekripsi Data pada *LoRa Gateway*

Pada Gambar 10 menunjukkan proses pengujian dekripsi data yang diterima pada *LoRa gateway* dengan menggunakan kunci dekripsi yang berbeda dengan kunci enkripsi yang digunakan. Hasilnya menunjukkan data sensor dalam bentuk *chiphertext* yang diterima

di *LoRa gateway* tidak dapat dilakukan proses dekripsi menjadi *plaintext* dikarenakan kunci enkripsi yang berbeda antara sensor node *WSN* dan *LoRa gateway*.

Gambar 10. Hasil Pengujian untuk Kunci Enkripsi yang berbeda pada *LoRa Gateway*

Untuk menguji waktu yang dibutuhkan untuk proses enkripsi dan dekripsi menggunakan *AES* 128-bit, dilakukan pengujian proses enkripsi di node sensor dan proses dekripsi di *LoRa gateway*. Hasil pengujian didapatkan waktu yang dibutuhkan untuk proses enkripsi dan dekripsi *AES* 128-bit ditunjukkan pada Tabel 3. Pada Tabel 3, untuk proses enkripsi dari 10 kali transmisi data yang dilakukan proses enkripsi, didapatkan rata-rata waktu enkripsi adalah 0,0506 detik, sedangkan untuk proses dekripsi pada *LoRa gateway* dibutuhkan rata-rata waktu proses adalah 0,1236 detik. Hasil ini menunjukkan proses enkripsi AES 128-bit lebih cepat dari pada proses deskripsinya.

Tabel 3. Pengujian Waktu Proses Enkripsi dan Dekripsi

No	Urutan Data	Waktu Proses (detik)	
		Enkripsi	Dekripsi
1	Transmisi Data ke-1	0,053	0,147
2	Transmisi Data ke-2	0,054	0,1
3	Transmisi Data ke-3	0,046	0,1
4	Transmisi Data ke-4	0,047	0,147
5	Transmisi Data ke-5	0,047	0,132
6	Transmisi Data ke-6	0,055	0,131
7	Transmisi Data ke-7	0,055	0,1
8	Transmisi Data ke-8	0,049	0,147
9	Transmisi Data ke-9	0,048	0,132
10	Transmisi Data ke-10	0,052	0,1
Rata-rata		**0,0506**	**0,1236**

4. Kesimpulan

Pada penelitian ini, keamanan data sensor *WSN* menggunakan *AES* 128-bit pada komunikasi menggunakan *LoRa gateway* dapat diimplementasikan dengan baik. Data sensor dari *WSN* yang telah di enkripsi dapat dibaca di *LoRa gateway* jika kunci yang digunakan sama dengan kunci enkripsi, sebaliknya data sensor tidak dapat dibaca jika kunci yang digunakan berbeda. Komputasi *AES* 128-bit pada *WSN* yang dalam penelitian ini menggunakan Mappi32 sangat kecil, sehingga tidak membebani proses pengiriman data sensor yang telah terenkripsi dari *WSN* ke *LoRa gateway*. Proses enkripsi dan dekripsi menggunakan *AES* 128-bit yang dilakukan oleh Mappi32 membutuhkan waktu rata-rata 0,0506 detik untuk proses enkripsi dan 0,1236 detik untuk proses dekripsi. Penggunaan media komunikasi *LoRa gateway* sangat baik di implementasikan pada *WSN* untuk mendeteksi kebakaran hutan karena jangkauan sinyal trasnmisi bisa cukup hingga mencapai jarak 150m pada daerah *LOS* dan jarak 125m pada daerah *NLOS*.

Daftar Pustaka

[1] LoRa Physical Layer & RF Interface, *electronics-notes.com*. https://www.electronics-notes.com/articles/connectivity/lora/radio-rf-interface-physical-layer.php

[2] Mappi32 Development Board, *https://www.kmtech.id/*. https://www.kmtech.id/generalboard

[3] Ahamed, J., Zahid, M., Omar, M., Ahmad, K., (2019), AES and MQTT based security system in the internet of things, *J. Discret. Math. Sci. Cryptogr.*, **22(8)**, 1589–1598. doi: 10.1080/09720529.2019.1696553

[4] Bui, D., Puschini, D., Bacles-Min, S., Beigné, E., Tran, X., (2016), Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications, *2016 International Conference on IC Design and Technology (ICICDT)*, 1–4. doi: 10.1109/ICICDT.2016.7542076

[5] Caicedo-Ortiz, J.G., De-la-Hoz-Franco, E., Ortega, R.M., Piñeres-Espitia, G., Combita-Niño, H., Estévez, F., Cama-Pinto, A., (2018), Monitoring System for Agronomic Variables Based in WSN Technology on Cassava Crops, *Comput. Electron. Agric.*, **145**, 275–281. https://doi.org/10.1016/j.compag.2018.01.004

[6] Chauhan, A., Semwal, S., Chawhan, R., (2013), Artificial neural network-based forest fire detection system using wireless sensor network, *2013 Annual IEEE India Conference (INDICON)*, 1-6. doi: 10.1109/INDCON.2013.6725913

[7] Dihni, V.A., (2022), "Luas Kebakaran Hutan dan Lahan RI Bertambah 19% pada 2021," *databoks*. https://databoks.katadata.co.id/datapublish/2022/01/11/luas-kebakaran-hutan-dan-lahan-ri-bertambah-19-pada-2021#:~:text=Luas areal kebakaran hutan dan lahan (karhutla) di Indonesia sepanjang,dibandingkan 296.942 ha pada 2020 (diakses Feb 25, 2022)

[8] Dworkin, M., dkk., (2001), Advanced Encryption Standard (AES). Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD. doi: https://doi.org/10.6028/NIST.FIPS.197

[9] Edwards, S.A. & Heiduk, F., (2015), Hazy Days: Forest Fires and the Politics of Environmental Security in Indonesia, *J. Curr. Southeast Asian Aff.*, **34(3)**, 65–94. doi: 10.1177/186810341503400303

[10] FIPS Publication 197, (2001), Advanced Encryption Standard (AES), *U.S. DoC/NIST (https://www.nist.gov/)* https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf (diakses Apr 23, 2022)

[11] Gulati, K., Kumar Boddu, R.S., Kapila, D., Bangare, S.L., Chandnani, N., Saravanan, G., (2022), A review paper on wireless sensor network techniques in Internet of Things (IoT), *Mater. Today Proc.*, **51**, 161–165. https://doi.org/10.1016/j.matpr.2021.05.067

[12] Huijnen, V., Wooster, M., Kaiser, J., dkk., Fire carbon emissions over maritime southeast Asia in 2015 largest since 1997, (2016), *Sci Rep* **6**, 26886. https://doi.org/10.1038/srep26886

[13] Hung, C.-W. & Hsu, W.-T., (2018) Power Consumption and Calculation Requirement Analysis of AES for WSN IoT, *Sensors*, **18(6)**, 1675. doi: 10.3390/s18061675

[14] Kementerian Komunikasi dan Informatika RI, (2019), *Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 1 Tahun 2019 Tentang Penggunaan Spektrum Frekuensi Radio Berdasarkan Izin Kelas*.

[15] Kementerian Komunikasi dan Informatika RI, (2019), *Peraturan Direktur Jenderal Sumber Daya dan Perangkat Pos dan Informatika Nomor 3 Tahun 2019 Tentang Persyaratan Teknis Alat dan /atau Perangkat Telekomunikasi Low Power Wide Area*.

[16] Misfaul, M., Dana, M., Kurniawan, W., Fitriyah, H., (2018), Rancang Bangun Sistem Deteksi Titik Kebakaran Dengan Metode Naive Bayes Menggunakan Sensor Suhu dan Sensor Api Berbasis Arduino, *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, **2(9)**, 3384–3390.

[17] Nurbaya, S., (2020), *The State of Indonesia's Forest 2020*. Ministry of Environment and Forestry Republic of Indonesia.

[18] Núñez V, J.M., Fonthal R, F., Quezada L, Y.M., Design and Implementation of WSN and IoT for Precision Agriculture in Tomato Crops, *2018 IEEE ANDESCON*, 1–5. doi: 10.1109/ANDESCON.2018.8564674

[19] Pan, J.S., Kong, L., Sung, T.W., Tsai, P.W., Snášel, V., (2018), A-Fraction First Strategy for Hierarchical Model in Wireless Sensor Networks, *Journal of Internet Technology*, **19**, 1717–1726. doi: 10.3966/160792642018111906009 (19)

[20] Pambudi, R.A., Setiawan, B.D., Wijoyo, S.H., (2018), Implementasi Fuzzy Time Series untuk Memprediksi Jumlah Kemunculan Titik Api, *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, **2(11)**, 4767–4776. (6)

[21] Pradana, S.Y., Utaminingrum, F., Kurniawan, W., (2018), Deteksi Titik Api Terpusat Menggunakan Kamera dengan Notifikasi Berbasis SMS Gateway pada Raspberry Pi, *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, **2(12)**, 7183–7191. (8)

[22] Rathinam, D.D.K., Surendran, D., Shilpa, A., Grace, A.D., Sherin, J., (2019), Modern Agriculture Using Wireless Sensor Network (WSN), *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 515–519. doi: 10.1109/ICACCS.2019.8728284 (23)

[23] Salameh, H.B., Dhainat, M., Benkhelifa, E., (2019), A Survey On Wireless Sensor Network-Based IoT Designs for Gas Leakage Detection and Fire-Fighting Applications, *JJCIT*, **5(2)**, 60–73. doi: 10.5455/jjcit.71-1550235278 (26)

[24] Satria, D., Zulfan, Munawir, Hidayat, T., (2019), Implementation of Wireless Sensor Network (WSN) on Garbage Transport Warning Information System Using GSM Module," *J. Phys. Conf. Ser.*, **1175**, 12054. doi: 10.1088/1742-6596/1175/1/012054

[25] Simitha. K.M. & Subodh, R.M.S., IoT and WSN Based Water Quality Monitoring System, *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, 205–210. doi: 10.1109/ICECA.2019.8821859

[26] Singha, T.B., Palathinkal, R.P., Ahamed, S.R., (2020), Implementation of AES Using Composite Field Arithmetic for IoT Applications, *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, 115–121. doi: 10.1109/ISEA-ISAP49340.2020.235009

[27] Sukamto, S., Id, I.D., Angraini, T.R., Penentuan Daerah Rawan Titik Api di Provinsi Riau Menggunakan Clustering Algoritma K-Means, *JUITA J. Inform.*, **6(2)**, 137-147. doi: 10.30595/juita.v6i2.3172

[28] Tsai, K., Huang, Y., Leu, F., You, I., Huang, Y., Tsai, C., (2018), AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments, *IEEE Access*, **6**, 45325–45334. doi: 10.1109/ACCESS.2018.2852563

[29] Van Rooy, D., Bus, J., (2010), Trust and privacy in the future internet—a research perspective, *Identity Inf. Soc.*, **3(2)**, 397–404. doi: 10.1007/s12394-010-0058-7

[30] Varela, N., Díaz-Martinez, J.L., Ospino, A., Zelaya, N.A.L., (2020), Wireless sensor network for forest fire detection, *Procedia Comput. Sci.*, **175**, 435–440. doi: 10.1016/j.procs.2020.07.061

[31] Wang, J., Gao, Y., Liu, W., Sangaiah, A.K., Kim, H.J., (2019), Energy efficient routing algorithm with mobile sink support for wireless sensor networks, *Sensors (Switzerland)*, **19(7)**, 1–19. doi: 10.3390/s19071494

[32] Yu, W. & Köse, S., (2017), A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks, *IEEE Trans. Circuits Syst. I Regul. Pap.*, **64(11)**, 2934–2944. doi: 10.1109/TCSI.2017.2702098

[33] Zeng, D., Dai, Y., Li, F., Sherratt, R.A., Wang, J., (2018), Adversarial learning for distant supervised relation extraction, *Comput. Mater. Contin.*, **55(1)**, 121–136. doi: 10.3970/cmc.2018.055.121

[34] Zourmand, A., Kun Hing, A.L., Wai Hung, C., Abdulrehman, M., (2019), Internet of Things (IoT) using LoRa technology, *2019 IEEE Int. Conf. Autom. Control Intell. Syst. I2CACIS 2019 - Proc.*, 324–330. doi: 10.1109/ I2CACIS.2019.8825008