JURNAL ELTEK
Vol. 23, No. 1, April 2025, hal. 24~31
p-ISSN: 1693 – 4024 | e-ISSN: 2355-0740
DOI: 10.33795/eltek.v23i1.6910

Implementasi algoritma elgamal untuk pengamanan data pada *wireless sensor network*

M. Nanak Zakaria[1], Yoyok Heru Prasetyo Isnomo[2] , Junaedi Adi Prasetyo[3] , Dwinnar Rosyidan[4]
e-mail: [1]**nanakzach@polinema.ac.id**, [2]**urehkoyoy@polinema.ac.id**, [3]**junaedi.prasetyo@poliwangi.ac.id**, [4]**didanrosyidan@gmail.com**
[1,2,4]Jurusan Teknik Elektro, Politeknik Negeri Malang, Indonesia
[3]Jurusan Bisnis dan Informatika, Politeknik Negeri Banyuwangi, Indonesia

Informasi Artikel

Riwayat Artikel

Diterima 17 Februari 2025
Direvisi 24 April 2025
Diterbitkan 25 April 2025

Kata kunci:

Algoritma ElGamal
Jaringan Sensor Nirkabel
Keamanan Data

ABSTRAK

Perkembangan teknologi informasi menimbulkan tantangan keamanan data, terutama pada *Wireless Sensor Network* (WSN) yang rentan terhadap penyadapan. LoRa (Long Range) sering digunakan dalam WSN, tetapi memiliki kelemahan dalam keamanan komunikasi antar node. Untuk mengatasi hal ini, diperlukan sistem autentikasi yang kuat, seperti manajemen kunci. Algoritma ElGamal dipilih karena keamanannya berbasis logaritma diskret dan fleksibilitasnya dalam pengaturan ukuran kunci. Penelitian ini mengimplementasikan Algoritma ElGamal pada WSN dengan LoRa sebagai media transmisi. Perangkat yang digunakan adalah ESP32 Devkit V1 dan LoRa Ra-2 SX1278 pada node master, serta sensor HC-SR04 dan Flame Sensor pada node slave. Hasil menunjukkan Algoritma ElGamal mencapai ketepatan 100% dalam pengiriman data dengan delay 0,289 detik. Daya tahan baterai mencapai 2 jam 58 menit 38 detik. Pengujian intrusi membuktikan Algoritma ElGamal mampu mengamankan data melalui enkripsi dan dekripsi. Kesimpulannya, implementasi Algoritma ElGamal berhasil menjaga keamanan komunikasi dalam WSN, memastikan keaslian pesan, serta menjaga kinerja perangkat selama proses pengiriman dan penerimaan data.

Keywords:

Data Security
Elgamal Algorithm
Wireless Sensor Network

ABSTRACT

The advancement of information technology presents data security challenges, especially in Wireless Sensor Networks (WSN), which are vulnerable to eavesdropping. LoRa (Long Range) is commonly used in WSN but has weaknesses in securing node communication. To address this, a strong authentication system is required, such as key management. The ElGamal algorithm is chosen for its security based on discrete logarithms and flexibility in key size configuration. This study implements the ElGamal algorithm in a WSN system using LoRa as the transmission medium. Devices used include the ESP32 Devkit V1 and LoRa Ra-2 SX1278 on the master node, along with the HC-SR04 sensor and Flame Sensor on the slave node. Results show that the ElGamal algorithm achieves 100% accuracy in data transmission with a delay of 0.289 seconds. The battery lasts for 2 hours, 58 minutes, and 38 seconds. Intrusion testing proves that the ElGamal algorithm secures data through encryption and decryption. In conclusion, implementing the ElGamal algorithm successfully ensures secure communication in WSN, maintains message authenticity, and sustains device performance during data transmission and reception.

Penulis Korespondensi:
Muhammad Nanak Zakaria,
Jurusan Teknik Elektro,
Politeknik Negeri Malang,
Jl. Soekarno Hatta No. 9, Malang, Jawa Timur, Indonesia.
Email: nanakzach@politeknik.ac.id

1. PENDAHULUAN

Penggunaan perangkat teknologi informasi di semua bidang kehidupan saat ini menimbulkan permasalahan baru yang pada intinya terkait dengan masalah keamanan data. Keamanan data menjadi sangat penting untuk diperhatikan, karena saat data yang dikirimkan, dari satu perangkat ke perangkat lain, dapat diakses oleh orang yang tidak berkepentingan, maka data tersebut bisa jadi akan disalahgunakan, sehingga menyebabkan kerugian [1]. Permasalahan keamanan data ini dihadapi oleh teknologi *Wireless Sensor Network* (WSN). Keamanan data pada Wireless Sensor Network (WSN) menjadi lebih krusial mengingat data yang dikirimkan melalui jaringan nirkabel rentan terhadap penyadapan dan serangan dari pihak yang tidak bertanggung jawab. Salah satu teknologi yang sering digunakan untuk mendukung komunikasi dalam WSN adalah LoRa *(Long Range)*.

LoRa memiliki jangkauan yang lebih dari 1 km (tanpa hambatan) dan menggunakan daya atau sumber tenaga yang rendah. Dengan kelebihan ini menjadikan LoRa pasangan yang tepat bagi WSN. Terdapat banyak jenis LoRa, penelitian ini menggunakan LoRa SX1278 yang memiliki jangkauan hingga mencapai ± 5 km. [2] Meskipun LoRa mempunyai kelebihan, terdapat beberapa potensi kelemahan yang perlu untuk diselesaikan. Kelemahan tersebut adalah rentannya terhadap penyadapan dan pencurian data. Kelemahan ini terjadi pada komunikasi antar node dengan menggunakan LoRa [3]. Hal ini akan menjadi ancaman keamanan pada sistem. Penyusup bisa menjadi node tidak valid dan mengirimkan data yang salah atau menghalangi jalannya penerimaan data yang seharusnya. Seperti penelitian yang dilakukan oleh John Thomas dan rekannya mengenai serangan *Man In The Middle* yang dapat terjadi pada komunikasi antar LoRa. *Man In The Middle* adalah serangan dalam komunikasi LoRa dimana penyerang menyisipkan dirinya diantara komunikasi antar LoRa, sehingga penyerang dapat mengambil, mengubah, dan mencegat data yang dikirimkan pada komunikasi antar LoRa yang terjadi [4]. Untuk mengatasi permasalahan ini diperlukan sistem autentikasi. Sistem autentikasi yang disarankan menggunakan pendekatan manajemen kunci. Manajemen kunci adalah penggunaan kunci untuk mengontrol proses kriptografi untuk melakukan proses keamanan seperti autentikasi dan enkripsi.

Salah satu contoh algoritma kriptografi asimetris yang umum digunakan adalah Algoritma Elgamal. Algoritma ElGamal dipilih karena beberapa alasan utama dalam kriptografi. Pertama-tama, keamanannya yang kuat didasarkan pada kesulitan permasalahan logaritma diskret, yang membuatnya menjadi pilihan yang aman untuk enkripsi dan tanda tangan digital. Kemudian, ElGamal memiliki fleksibilitas yang tinggi dalam hal ukuran kunci dan implementasi, memungkinkan pengguna untuk menyesuaikan tingkat keamanan dan kinerja sesuai kebutuhan mereka. Kelebihan lain dari algoritma ElGamal adalah proses enkripsi pada plainteks yang sama diperoleh cipherteks yang berbeda-beda, namun pada proses dekripsi diperoleh plainteks yang sama [5]. Selain itu, sebagai algoritma kriptografi kunci publik, ElGamal memfasilitasi pertukaran kunci yang aman dan memungkinkan komunikasi rahasia di lingkungan yang tidak terpercaya. Kelebihan utama ElGamal adalah kombinasi antara keamanan yang kuat dan fleksibilitas, yang menjadikannya pilihan yang menonjol dalam berbagai aplikasi kriptografi, mulai dari komunikasi aman hingga otentikasi digital [6].

Untuk memberikan pengamanan dalam pengiriman data sensor pada WSN menggunakan Algoritma ElGamal maka penulis melakukan penelitian dengan judul "Implementasi Algoritma ElGamal Untuk Pengaman Data Sensor Pada WSN".

2. METODE PENELITIAN

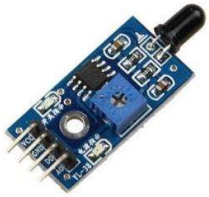
Penelitian ini mengembangkan teknologi yang sudah ada sebelumnya yaitu WSN dan dikombinasikan dengan Algoritma ElGamal sebagai metode untuk pengamanan data pada penelitian ini. Dalam Penelitian ini menggunakan komponen-kombonen sebagai berikut:

Gambar 1. ESP32 Devkit V1[7]

Mikrokontroler ESP32 merupakan mikrokontroler SoC (System on Chip) terpadu dengan dilengkapi WiFi 802.11 b/g/n, Bluetooth versi 4.2, dan berbagai peripheral. ESP32 adalah chip yang cukup lengkap, terdapat prosesor, penyimpanan dan akses pada GPIO (General Purpose Input Output). ESP32 bisa digunakan untuk rangkaian pengganti pada Arduino, ESP32 memiliki kemampuan untuk mendukung terkoneksi ke WI-FI secara langsung [8]. Pada penelitian ini ESP32 Devkit V1 digunakan sebagai Mikrokontroler yang akan mengontrol komponen-komponen lain.

Gambar 2. LoRa Ra-2 SX1278 [9]

LORA SX1278 merupakan sebuah modul LORA yang menyediakan jangkauan penyebaran spektrum ultra long dan memiliki interferensi tinggi untuk meminimalkan konsumsi daya. Menggunakan Teknik modulasi LoRa yang dipatenkan Semtech, SX1278 dapat mencapai sensitivitas lebih dari -148 dBm menggunakan bahan kristal dengan biaya rendah dan bill ofmaterial. Sensitivitas tinggi yang dikombinasikan dengan penguat daya +20 dBm terintegrasi menghasilkan link budget yang menjadikannya optimal untuk aplikasi apa pun yang membutuhkan jarak jangkau yang jauh. LoRa ini memberikan keuntungan yang signifikan dalam pemblokiran dan selektivitas atas teknik modulasi konvensional, memecahkan masalah jarak jangkau, gangguan kekebalan dan konsumsi energi [10]. Pada penelitian ini LoRa Ra-2 SX1278 akan digunakan sebagai media transmisi antara Node Master dan Node Slave.



Gambar 3. Flame Sensor [11]

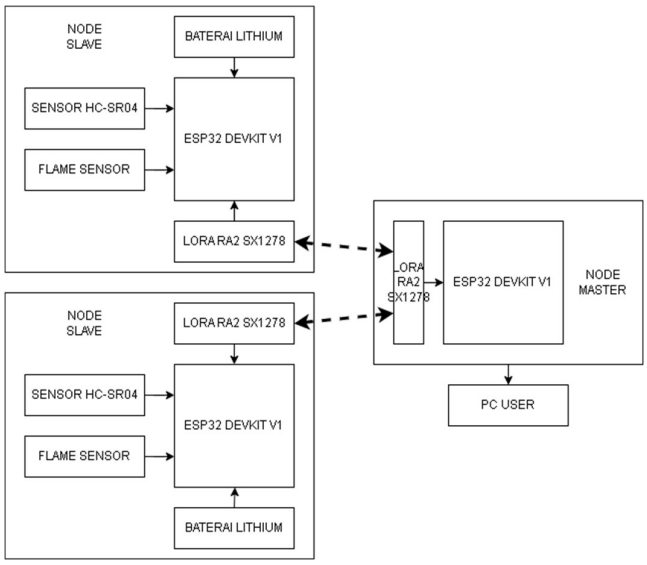
Flame sensor merupakan sensor yang mempunyai fungsi sebagai pendeteksi nyala api yangdimana api tersebut memiliki panjang gelombang antara 760nm – 1100nm. Sensor ini menggunakan infrared sebagai tranduser dalam mendeteksi kondisi nyala api [12].

Gambar 4. Sensor HC-SR04 [13]

Sensor ultrasonik tipe HCSR04 merupakan perangkat yang digunakan untuk mengukur jarak dari suatu objek. Kisaran jarak yang dapat diukur sekitar 2-450 cm. Perangkat ini menggunakan dua pin digital untuk mengkomunikasikan jarak yang terbaca. Prinsip kerja sensor ultrasonik ini bekerja dengan mengirimkan pulsa ultrasonik sekitar 40 KHz, kemudian dapat memantulkan pulsa echo kembali, dan menghitung waktu yang diambil dalam mikrodetik [14]. Pada penelitian ini Sensor HC-SR04 digunakan sebagai pengukur jarak api

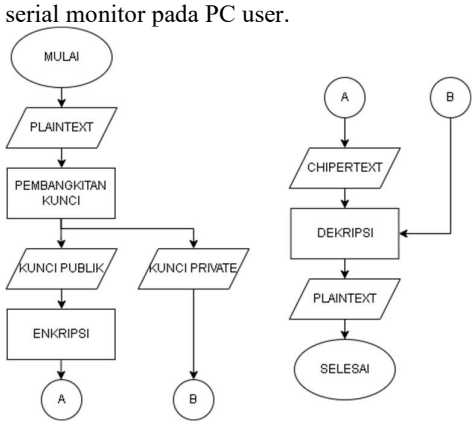
Gambar 5. Baterai Lithium[15]

Baterai lithium-ion merupakan salah satu jenis baterai sekunder rechargeable battery) yang dapat diisi ulang dan merupakan baterai yang ramah lingkungan karena tidak mengandung bahan yang berbahaya seperti baterai-baterai yg berkembang lebih dahulu yaitu baterai NI-Cd dan Ni-MH. Baterai ini memiliki kelebihan dibandingkan baterai sekunder jenis lain, yaitu memiliki stabilitas penyimpanan energi yang sangat baik (daya tahan sampai 10 tahun atau lebih) [16]. Pada penilitian ini Baterai akan menjadi sumber daya untuk Node Slave.



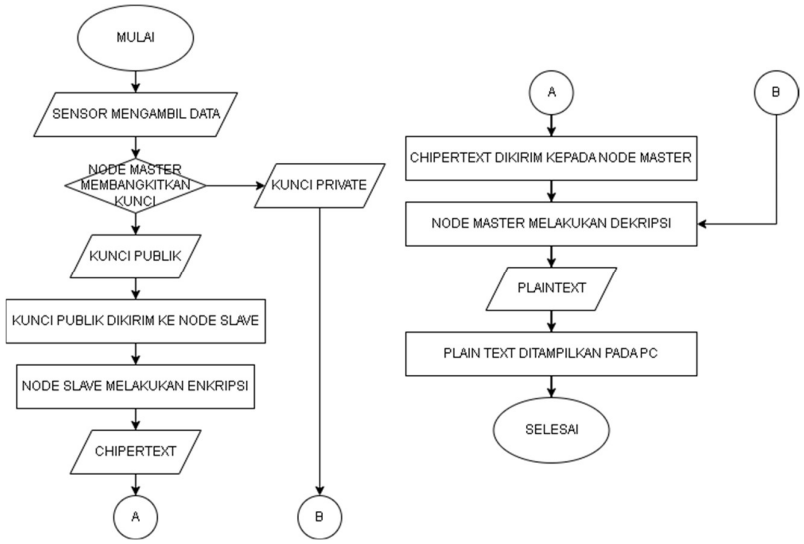
Gambar 6. Perancangan Sistem

Pada penelitian ini sistem diawali dengan Flame sensor dan sensor HC-SR04 yang terdapat pada node slave mengambil data. Data (plaintext) tersebut diteruskan menuju ESP32 Devkit V1 pada node slave. Kemudian node master melakukan pembangkitan kunci untuk membuat kunci publik (y) untuk enkripsi dan kunci private (x) untuk dekripsi. Setelah pembangkitan kunci berhasil, kunci publik dikirim dari node master menuju node slave melalui media transmisi LoRa Ra-2 SX1278. Setelah kunci publik diterima, data (plaintext) yang telah diterima node slave dari sensor di enkripsi menggunakan kunci publik (y) yang diterima dari node master yang menghasilkan data terenkripsi (chipertext). Setelah data terenkripsi (chipertext), data tersebut dikirim menuju node master melalui LoRa Ra-2 SX1278. Selanjutnya node master melakukan proses dekripsi terhadap data terenkripsi (chipertext) menggunakan kunci private (x) yang sudah dibangkitkan sebelumnya. Sehingga data terenkripsi (chipertext) menjadi data terdekripsi (plaintext). Selanjutnya data terdekripsi (plaintext) ditampilkan melalui serial monitor pada PC user.



Gambar 7. Flowchart Algoritma ElGamal

Algoritma ElGamal merupakan bagian dari kriptografi asimetris yang pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit [17]. Dengan memanfaatkan bilangan prima yang besar serta masalah logaritma diskrit yang cukup menyulitkan, maka keamanan kuncinya lebih terjamin [18]. Proses enkripsi ElGamal dari plaintext ke dalam bentuk ciphertext didahului pembentukan kunci oleh penerima pesan, dua macam pasangan kunci yaitu kunci public dan kunci private. Kunci public untuk disebarluaskan sedangkan kunci private untuk diri sendiri. Untuk membuat sebuah pesan rahasia dalam bentuk ciphertext, pesan rahasia harus dikonversikan terlebih dahulu dalam bilangan bulat kemudian dikodekan berdasarkan kode ASCII(American Standart for Information Interchange). Pesan dalam bentuk ciphertext didekripsi menggunakan kunci private untuk dikembalikan menjadi pesan yang sebenarnya [19].



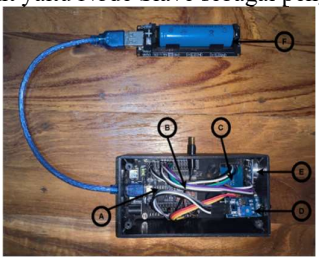
Gambar 8. Flowchart Sistem

Sistem diawali dengan Flame sensor dan sensor HC-SR04 yang terdapat pada node slave mengambil data. Data (plaintext) tersebut diteruskan menuju ESP32 Devkit V1 pada node slave. Kemudian node master melakukan pembangkitan kunci untuk membuat kunci publik (y) untuk enkripsi dan kunci private (x) untuk dekripsi. Setelah pembangkitan kunci berhasil, kunci publik dikirim dari node master menuju node slave melalui media transmisi LoRa Ra-2 SX1278. Setelah kunci publik diterima, data (plaintext) yang telah diterima node slave dari sensor di enkripsi menggunakan kunci publik (y) yang diterima dari node master yang menghasilkan data terenkripsi (chipertext). Setelah data terenkripsi (chipertext), data tersebut dikirim menuju node master melalui LoRa Ra-2 SX1278. Selanjutnya node master melakukan proses dekripsi terhadap data terenkripsi (chipertext) menggunakan kunci private (x) yang sudah dibangkitkan sebelumnya. Sehingga data terenkripsi (chipertext) menjadi data terdekripsi (plaintext). Selanjutnya data terdekripsi (plaintext) ditampilkan melalui serial monitor pada PC user.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Pembuatan Alat

Pada bagian ini menyajikan hasil pengembangan perangkat yang digunakan untuk implementasi algoritma ElGamal pada jaringan sensor nirkabel (WSN). Perangkat ini terdiri dari dua node: node master dan node slave. Node master dilengkapi dengan ESP32 DevKit V1, ESP32 Shield, dan modul LoRa SX1278. Node slave menggunakan ESP32 DevKit V1, ESP32 Shield, modul LoRa SX1278, sensor HC-SR04 (untuk mengukur jarak), dan sensor flame (untuk mendeteksi api). Kedua node terhubung melalui jaringan LoRa untuk pengiriman data terenkripsi menggunakan algoritma ElGamal. Pada Gambar 7 berikut merupakan hasil pembuatan alat yang telah selesai dirakit yaitu Node Slave sebagai pengirim.

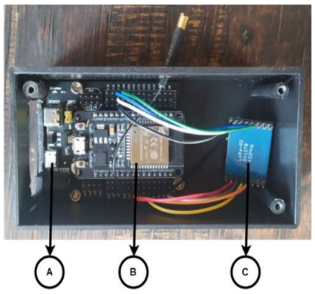


Gambar 7. Node Slave

Keterangan :

A. ESP32 Shield sebagai papan mikrokontroler tambahan untuk memperbanyak pin yang akan digunakan
B. ESP32 Devkit V1 sebagai mikrokontroler
C. LoRa Ra-2 SX1278 sebagai modul transmisi nirkabel
D. Flame Sensor sebagai sensor pendeteksi api
E. Sensor HC-SR04 sebagai sensor pengukur jarak benda
F. Baterai Lithium sebagai sumber daya energi

Pada Gambar 8 berikut merupakan hasil pembuuatan alat yang telah selesai dirakit yaitu Node Masyer sebagai penerima.



Gambar 8. Node Master

Keterangan :

A. ESP32 Shield sebagai papan mikrokontroler tambahan untuk memperbanyak pin yang akan digunakan
B. ESP32 Devkit V1 sebagai mikrokontroler
C. LoRa Ra-2 SX1278 sebagai modul transmisi nirkabel

3.2. Hasil Pengujian

Berikutnya adalah pengujian penggunaan sistem yang terdiri dari 5 bagian yaitu, pengujian keberhasilan pengiriman dan penerimaan pesan, pengujian jarak jangkauan, pengujian delay pengiriman dan penerimaan pesan, pengujian daya tahan baterai, dan pengujian intrusi. Berikut merupakan penjelasan lebih lanjut untuk Hasil Pengujian.

3.2.1 Pengujian Keberhasilan Pengiriman dan Penerimaan Pesan

Pada bagian ini dilakukan proses pengujian ketepatan antara pesan yang dikirim dan pesan yang diterima dengan menggunakan Algoritma ElGamal dan tanpa menggunakan Algoritma ElGamal. Pengujian dilakukan dengan mengecek kesamaan pesan yang dikirim oleh node slave dan pesan yang diterima oleh node master melalui serial monitor. Hasil dari pengujian ini didapatkan ketepatan 100% untuk pengujian tanpa menggunakan Algoritma ElGamal dan 100% untuk pengujian dengan menggunakan Algoritma ElGamal. Pengujian ini sangat penting karena ketepatan data merupakan faktor krusial dalam sistem komunikasi, sebagaimana yang diungkapkan dalam beberapa penelitian yang menunjukkan pentingnya menjaga integritas data dalam jaringan nirkabel, termasuk pada sistem berbasis LoRa [20]. Hasil pengujian ini mendukung klaim bahwa ElGamal dapat digunakan dengan baik dalam menjaga ketepatan pesan yang dikirim, seperti yang juga tercatat dalam penelitian tentang penggunaan ElGamal pada jaringan sensor nirkabel [21].

3.2.2 Pengujian Jarak Jangkauan

Pada bagian ini dilakukan pengujian jangkauan komunikasi LoRa dalam pengiriman dan penerimaan pesan. Pengujian dilakukan dengan menyesuaikan jarak antara node master dan node slave serta mengubah posisi antena pada kedua node. Pengujian ini dilakukan untuk mengetahui sejauh mana jangkauan komunikasi LoRa, baik tanpa halangan maupun dengan halangan. Hasil pengujian menunjukkan jarak sejauh 30 m baik dengan maupun tanpa Algoritma ElGamal. LoRa memang telah dikenal memiliki jangkauan yang cukup baik untuk komunikasi jarak jauh, meskipun penggunaan enkripsi dapat mempengaruhi sedikit jangkauan yang dicapai. Sebuah studi tentang komunikasi LoRa dalam aplikasi IoT menunjukkan bahwa meskipun ada sedikit penurunan performa dalam hal jangkauan karena enkripsi, jangkauan LoRa tetap cukup memadai [22]. Penelitian lebih lanjut juga menyoroti bahwa LoRa dapat digunakan dengan baik dalam pengaturan jaringan sensor nirkabel meskipun terdapat beberapa halangan [23].

3.2.3 Pengujian Delay Pengiriman dan Penerimaan Pesan

Pada bagian ini melakukan proses pengujian delay antara pesan yang dikirim dan pesan yang diterima dengan menggunakan Algoritma ElGamal dan tanpa menggunakan Algoritma ElGamal. Pengujian dilakukan dengan membandingkan waktu pengiriman dan penerimaan pesan pada dua kondisi, yaitu dengan menggunakan Algoritma ElGamal dan tanpa menggunakan Algoritma ElGamal. Pengujian ini dilakukan untuk mengevaluasi kinerja Algoritma ElGamal pada sistem dalam kecepatan pengiriman pesan dan penerimaan pesan. Hasil dari pengujian ini didapatkan nilai delay sebesar 0,064 detik tanpa menggunakan Algoritma ElGamal dan mendapatkan nilai delay sebesar 0,289 detik dengan menggunakan Algoritma ElGamal

3.2.4 Pengujian Daya Tahan Baterai

Pada bagian ini melakukan proses pengujian daya tahan baterai dalam menjalankan alat tanpa Algoritma ElGamal dan dengan Algoritma ElGamal. Pengujian dilakukan dengan menjalankan alat dengan menggunakan baterai hingga baterai habis. Selama alat menyala, setiap 20 menit sekali dilakukan pengukuran tegangan baterai. Pengujian ini dilakukan untuk mengetahui seberapa besar peningkatan daya yang diakibatkan oleh Algoritma ElGamal, yang secara tidak langsung berdampak pada daya tahan baterai perangkat. Hasil dari

pengujian alat tanpa Algoritma ElGamal dapat bertahan selama 3 jam 2 menit 57 detik dan pengujian dengan Algoritma ElGamal dapat bertahan selama 2 jam 58 menit 23 detik

3.2.5 Pengujian Intrusi

Pada bagian ini dilakukan pengujian alat apabila terdapat intruder di antara komunikasi antar LoRa. Pengujian dilakukan dengan menjalankan alat untuk melakukan pengiriman dan penerimaan pesan tanpa Algoritma ElGamal dan dengan Algoritma ElGamal, kemudian disisipkan satu node penyusup yang mencoba mengambil pesan yang dikirim. Hasilnya menunjukkan bahwa tanpa Algoritma ElGamal penyusup dapat membaca pesan, sedangkan ketika Algoritma ElGamal diaktifkan, pesan tetap terlindungi. Temuan ini sejalan dengan riset terkini yang menekankan bahwa peningkatan lapisan kriptografi—ditambah skema agregasi data yang dirancang khusus untuk menjaga kerahasiaan muatan—mampu meminimalkan peluang pembedahan paket oleh pihak tak berwenang [25].

Berikut merupakan hasil dari pengujian dan harapan penulis pada sistemyang telah dirancang dalam penelitian ini

Tabel 1. Hasil Pengujian Sistem

Kegiatan	Hasil yang diharapkan	Hasil pengujian	Hasil	
			Berhasil	Tidak Berhasil
Keberhasilan pengiriman dan penerimaan pesan	Pesan terenkripsi dapat dikirim oleh node slave dan dapat diterima oleh node master kemudian di dekripsi sehingga mendapatkan pesan yang sama dengan yang dikirim sebelumnya	Pesan terenkripsi dapat dikirim oleh node slave dan dapat diterima oleh node master kemudian di dekripsi sehingga mendapatkan pesan yang sama dengan yang dikirim sebelumnya	**10 pengujian**	-
Jarak jangkauan komunikasi antara node master dengan node slave	Dapat mencapai jarak 100 meter	Dapat mencapai jarak 30 meter	-	**10 pengujian**
Delay dalam pengiriman dan penerimaan pesan pada node	Mendapatkan nilai delay sebesar kurang dari 1 detik	Mendapatkan nilai delay sebesar kurang dari 1 detik	**10 pengujian**	-
Daya tahan baterai dalam menjalankan sistem	Mendapatkan ketahanan selama 3 jam	Mendapatkan ketahanan selama 3 jam	**2 pengujian**	-
Melakukan intrusi dengan adanya node pihak ketiga dengan menggunakan metode MITM	Dapat menggagalkan intrusi dari luar	Dapat menggagalkan intrusi dari luar	**10 pengujian**	-

4. KESIMPULAN

Penelitian ini mengembangkan sistem Wireless Sensor Network (WSN) dengan tiga node, terdiri dari dua node slave sebagai pengirim dan satu node master sebagai penerima. Node slave menggunakan ESP32 Devkit V1 dengan sensor HC-SR04, Flame sensor, dan modul LoRa Ra-2 SX1278 untuk transmisi data, sedangkan node master berfungsi menerima data menggunakan LoRa Ra-2 SX1278.

Hasil pengujian menunjukkan bahwa penggunaan Algoritma ElGamal berhasil menjaga integritas pesan dengan tingkat ketepatan 100%, meskipun menyebabkan peningkatan delay dari 0,064 detik menjadi 0,289 detik akibat kompleksitas enkripsi dan dekripsi. Selain itu, daya tahan baterai berkurang dari 3 jam 10 menit 40 detik menjadi 2 jam 58 menit 23 detik. Faktor jarak dan hambatan juga memengaruhi kualitas sinyal, dengan transmisi gagal pada jarak lebih dari 30 meter atau adanya penghalang.

Algoritma ElGamal terbukti meningkatkan keamanan pesan, mencegah penyadapan oleh pihak tidak berwenang, sehingga pesan tetap terlindungi. Dengan demikian, meskipun Algoritma ElGamal berdampak pada efisiensi energi dan keterlambatan transmisi, penggunaannya memberikan perlindungan yang signifikan terhadap keamanan data dalam sistem WSN.

5. DAFTAR PUSTAKA

[1] Syariful e Risa, “Penerapan Keamanan WSN Berbasis Algoritma RSA 2048 dan SHA-3 pada Pemantauan Suhu,” *Jurnal Nasional Teknologi dan Sistem Informasi ,* vol. 6, nº 3, pp. 150-157, 2020.

[2] Prihadi, Sunu e Abdul, “Feasibility of LoRa for Communication Networks in Water Management Systems at Politeknik Negeri Samarinda,” *JTE UNIBA,* vol. 6, nº 1, pp. 175-179, 2021.

[3] A. F. Septano, A. Kusyanti e R. A. Siregar, "Implementation of Feige-Fiat-Shamir Identification Scheme for Authentication between Node and Gateway on LoRa Module," *Journal of Information Technology and Computer Science Development,* vol. 5, nº 7, pp. 2961-2967, 2021.

[4] J. Thomas, S. Cherian, S. Chandran e V. Pavithran, "Man in the Middle Attack Mitigation in LoRaWAN," *Proceedings of the Fifth International Conference on Inventive Computation Technologies (ICICT-2020),* pp. 353-359, 2020.

[5] T. M. Danang, "Elgamal Algorithm In Securing Secret Messages," *Journal of Bandung Institute of Technology,* 2009.

[6] F. A. Anshori E E. Aribowo, "Implementasi Algoritma Kriptografi Kunci Publik Elgamal Untuk Proses Enkripsi Dan Dekripsi Guna Pengamanan File Data," *Jurnal Informatika,* 2014.

[7] F. Husaini, A. M. H. Pardede e I. Gultom, "Application of Encryption Using the ElGamal Method to Enhance the Security of Text and Image Data," *Journal of Computer and Informatics,* vol. 4, nº 1, pp. 67-73, 2022.

[8] M. Nizam, H. Yuana e Z. Wulansari, "ESP32 Microcontroller as a Web-Based Door Monitoring Tool," *Journal of Informatics Engineering Students,* vol. 6, nº 2, pp. 767-772, 2022.

[9] A. Rahman e M. S. Nugroho, " Keamanan Wireless Sensor Network Pendeteksi Kebakaran Hutan Menggunakan Algoritma AES Pada Media Komunikasi LORA," *Seminar Nasional Matematika, Geometri, Statistika, dan Komputas,* 2022.

[10] A. N. Fadillah, A. D. Almazazi e M. T. Ir. Morlan Pardede, "Design and Development of Communication Device Between Smartphones via LoRa Multi-Hop Wireless Network," *National Conference on Social and Engineering at Politeknik Negeri Medan,* pp. 908-916, 2022.

[11] I. Ramadhana e B. Sujatmiko, "Pengembangan Aplikasi Kamus Bahasa Pemrograman C++ Berbasis Android Untuk Meningkatkan Kompetensi Kognitif Mata Kuliahstruktur Data," *Jurnal IT-EDU,* vol. 3, no 1, 2018.

[12] H. D. Cahyadi, Y. Mirza e E. Laila, "Design and Development of a Fire Detection Device Using a Flame Sensor and Smoke Sensor Based on Arduino," *Final Report Journal of Computer Engineering,* vol. 2, nº 1, pp. 60-70, 2022.

[13] S. P. Santoso e F. Wijayanto, "Rancang Bangun Akses Pintu Dengan Sensor Suhu Dan Handsanitizer Otomatis Berbasis Arduino," *Jurnal Elektro ,* vol. 10, no 1, pp. 20-31, 2022.

[14] M. Fadli, D. Suhendri e F. Taufik, "Implementation of Inductive Proximity Sensor in a Metal Waste Sorting System Using the Counter Method Based on Arduino," *Journal of Computer Systems TGD,* vol. 2, nº 4, pp. 229-235, 2023.

[15] M. M. Kurniawan, K. Amron e R. A. Siregar, "Analisis Karakteristik Transmisi LoRa pada Wilayah Perkotaan," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* vol. 6, nº 8, pp. 3977-3986, 2022.

[16] F. A. Perdana, "Lithium Battery," *INKUIRI: Journal of Science Education,* vol. 9, nº 2, pp. 103-109, 2020.

[17] A. Widyatmoko, S. R. Akbar e R. Primananda, "Implementation of Wireless Sensor Network Using OLSR Protocol on Arduino Pro Mini and NRF24L01," *Journal of Information Technology and Computer Science Development,* vol. 2, nº 11, pp. 4750-4759, 2018.

[18] N. Rochmat, R. Isnanto e M. Somantri, "Implementation Of Elgamal Cryptography Algorithm For Message Security," *Scientific Journal of Electrical Engineering,* vol. 1, nº 3, 2012.

[19] Z. Arief, P. H. Trisnawan e A. Basuki, "Implementasi Komunikasi Multi-Hop Menggunakan Metode Controlled Flooding Pada Wireless Sensor Network Berbasis LoRa," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* vol. 4, nº 7, pp. 2154-2162, 2020.

[20] I. G. W. Sanjaya, A. Bhawiyuga e R. A. Siregar, "Implementasi Metode Ephemeral Diffie Hellman Over Cose (EDHOC) pada Wireless Sensor Network (WSN) sebagai Mekanisme Autentikasi berbasis Modul Komunikasi LoRa," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* vol. 5, nº 4, pp. 1423-1434, 2021.

[21] S. Reegan e V. Kabila, "Highly Secured Cluster Based WSN Using Novel FCM and Enhanced ECC-ElGamal Encryption in IoT," *Wireless Personal Communications,* vol. 118, pp. 1313-1329, 2021.

[22] M. Mohan, M. Kavithadevi e J. P. V, "Improved ElGamal Cryptosystem for Secure Data Transfer in IoT Networks," *Fourth International Conference on I-SMAC,* 2020.

[23] A. H. Hamza e S. M. K. Al-Alak, "Evaluation key generator of Multiple Asymmetric methods in Wireless Sensor Network (WSNs)," *Journal of Physics,* pp. 1-10, 2021.

[24] V. Kumar, S. Ray e D. Sadukhan, "ECC, Enhanced pairing-free identity-based broadcast authentication protocol in WSN using ElGamal," *Journal Security and Privacy,* 2022.

[25] Murugheswari, A. Sabantini, L. Jose e Padmapriya, "Effective Data Aggregation in WSN for Enhanced Security and Data Privacy," *Journal of Cryptpgraphy and Security,* pp. 1-10, 2023.