Jurnal Penelitian Inovatif (JUPIN)
Vol. 4, No. 4, November 2024, Hal. 2289-2296
https://jurnal-id.com/index.php/jupin

DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Implementasi Keamanan Jaringan Nirkabel Menggunakan Proteksi Paket Header untuk Meningkatkan Integritas Data di Greenhouse

Hadiwiyatno[1], Septriandi Wirayoga[*2], Isac Ilham Akbar Habibi[3], Miftakhul Huda[4]

[1,2,3,4]Jurusan Teknik Elektro, Politeknik Negeri Malang, Indonesia
Email: [1]hadiwiyatno@polinema.ac.id, [2]yoga.septriandi@polinema.ac.id, [3]isac.habibi@polinema.ac.id, [4]miftahul.huda@polinema.ac.id

Abstrak

Perkembangan teknologi pertanian, khususnya dalam pemantauan kondisi lingkungan di greenhouse, memerlukan Jaringan Sensor Nirkabel (Wireless Sensor Network - WSN) yang andal dan aman. Namun, modul komunikasi seperti NRF24L01 yang sering digunakan pada WSN memiliki kerentanan terhadap serangan pencegatan dan manipulasi data, yang berpotensi mengancam akurasi dan integritas data sensor. Urgensi untuk melindungi data ini menjadi fokus penelitian, dengan tujuan mengimplementasikan dan mengevaluasi mekanisme keamanan tambahan pada tingkat paket header NRF24L01. Metodologi penelitian mencakup pengujian keamanan data, integritas data, dan kinerja sistem. Hasil pengujian keamanan data menunjukkan tingkat keberhasilan 100% dalam menahan serangan, dengan semua dari 100 paket data terlindungi dari upaya pencegatan dan manipulasi. Pada pengujian integritas, tingkat keberhasilan penerimaan data tercatat sebesar 99%, dengan kehilangan dan kerusakan paket hanya 1%. Dari segi kinerja, proteksi tambahan ini menunjukkan dampak minimal dengan waktu transmisi rata-rata 20 ms, throughput mencapai 250 kbps, dan konsumsi daya stabil di antara 48-50 mW. Hasil ini mengindikasikan bahwa mekanisme proteksi yang diterapkan efektif tanpa mengorbankan performa sistem, dan berpotensi meningkatkan keamanan serta keberlanjutan WSN dalam aplikasi pertanian pintar yang memerlukan pemantauan lingkungan yang presisi.

Kata kunci: *Greenhouse, Keamanan Jaringan, Mikrokontroller, NRF24L01*

Abstract

The development of agricultural technology, especially in monitoring environmental conditions in greenhouses, requires a reliable and secure Wireless Sensor Network (WSN). However, communication modules such as the NRF24L01 that are often used in WSNs are vulnerable to data interception and manipulation attacks, potentially threatening the accuracy and integrity of sensor data. The urgency to protect this data became the focus of the research, with the aim of implementing and evaluating additional security mechanisms at the NRF24L01 header packet level. The research methodology included testing data security, data integrity, and system performance. The results of the data security testing showed a 100% success rate in resisting attacks, with all of the 100 data packets protected from interception and manipulation attempts. In integrity testing, the data reception success rate was recorded at 99%, with only 1% packet loss and corruption. In terms of performance, this additional protection showed minimal impact with an average transmission time of 20 ms, throughput reaching 250 kbps, and power consumption stabilizing between 48-50 mW. These results indicate that the implemented protection mechanism is effective without compromising system performance, and has the potential to improve the security and sustainability of WSNs in smart agriculture applications that require precise environmental monitoring.

Keywords: *Greenhouse, Microcontroller, Network Security, NRF24L01*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa perubahan signifikan dalam berbagai sektor, termasuk pertanian. Di tengah tantangan perubahan iklim dan permintaan pangan yang terus meningkat, pengelolaan lingkungan pertanian kini dituntut lebih efisien, berbasis data, dan responsif terhadap perubahan kondisi. Penggunaan data real-time untuk memantau suhu, kelembaban, dan kualitas udara dalam greenhouse atau rumah kaca menjadi krusial karena kondisi ini sangat

DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

berpengaruh terhadap pertumbuhan tanaman dan hasil panen. Greenhouse memungkinkan petani menciptakan lingkungan yang terkontrol dan stabil untuk mendukung produktivitas tanaman sepanjang tahun (Mikhaylov et al., 2020). Namun, tanpa sistem pemantauan yang efektif, kondisi dalam greenhouse bisa cepat berubah, yang dapat mengganggu keseimbangan lingkungan bagi tanaman.

Oleh karena itu, teknologi berbasis jaringan sensor nirkabel (Wireless Sensor Network - WSN) menjadi solusi yang efektif dan diperlukan (Hadiwiyatno et al., 2020). WSN memungkinkan data lingkungan dikumpulkan secara otomatis dan real-time, sehingga informasi penting ini dapat langsung diakses dan dianalisis untuk pengambilan keputusan yang cepat. Melalui pemantauan ini, petani dapat memastikan bahwa kondisi lingkungan selalu dalam batas optimal, misalnya menjaga suhu pada tingkat yang sesuai, mengontrol kelembaban untuk mencegah penyakit tanaman, dan memantau kualitas udara guna mencegah polutan berbahaya (Wirayoga, Anshori, et al., 2023). Implementasi WSN di greenhouse juga membuka peluang bagi otomatisasi dalam pengelolaan pertanian, seperti pengaturan penyiraman dan pemupukan otomatis yang terhubung langsung dengan data sensor. Dengan demikian, penerapan teknologi ini tidak hanya meningkatkan efisiensi tetapi juga mendukung keberlanjutan pertanian modern, di mana setiap data yang dikumpulkan dapat membantu petani mengoptimalkan sumber daya serta meningkatkan hasil pertanian secara berkelanjutan.

Namun, keberhasilan WSN dalam mendukung operasi pertanian ini juga membawa tantangan baru dalam aspek keamanan dan integritas data (Wirayoga, Imammuddien, et al., 2023). Mengingat data yang dikumpulkan berkaitan langsung dengan hasil panen dan kondisi lingkungan yang sensitif, perlindungan komunikasi data menjadi prioritas utama. Modul NRF24L01, yang banyak digunakan dalam jaringan sensor untuk transmisi data dalam jarak pendek, memiliki peran penting dalam proses ini (Junus et al., 2022). Namun, modul ini memiliki kerentanan pada paket header data yang dikirimkan, sehingga memerlukan proteksi tambahan agar informasi penting tidak mudah disusupi oleh pihak yang tidak berwenang. Proteksi pada paket header NRF24L01 bertujuan untuk menghalau ancaman serangan seperti pencegatan data (data interception) dan manipulasi paket, memastikan data lingkungan pertanian tetap aman, akurat, dan terjamin integritasnya, yang pada gilirannya mendukung keberlanjutan dan keandalan jaringan sensor dalam aplikasi pertanian pintar (Reyes-Medina et al., 2022).

Pada artikel (Gheorghiu et al., 2023) menyajikan hasil yang diperoleh selama percobaan dengan proyek yang dikembangkan untuk Internet of Things, yang dianggap sebagai model struktur yang dikembangkan untuk menghadiri bagian dari proyek untuk mengintegrasikan komponen dan sensor, kontribusi penelitian ini memberikan referensi teoritis ilmiah pendekatan yang dapat digunakan peneliti dalam proyek yang lebih kompleks, yang memerlukan pengiriman dan penerimaan data antar perangkat yang didistribusikan di lokasi berbeda. Namun pada artikel ini hanya berbasis komunikasi internet saja yang membutuhkan koneksi WAN yang stabil.

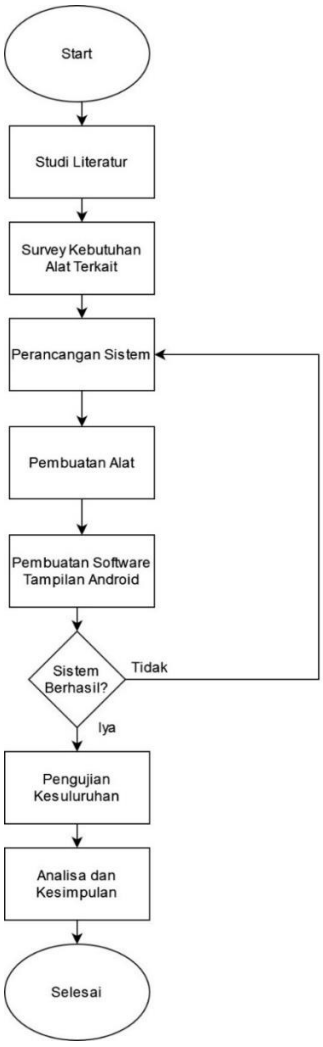
Dengan memfokuskan penelitian pada implementasi keamanan jaringan nirkabel menggunakan proteksi pada paket header NRF24l01 dalam konteks greenhouse, diharapkan dapat meningkatkan tingkat keamanan dan integritas data dalam pengelolaan lingkungan pertanian. Hal ini juga dapat menjadi langkah proaktif dalam mengatasi tantangan keamanan yang mungkin muncul seiring dengan meningkatnya keterhubungan perangkat dalam jaringan nirkabel sensor di greenhouse, yang secara langsung berkontribusi pada efisiensi dan keberlanjutan dalam produksi pertanian modern.

2. METODE PENELITIAN

Jenis penelitian yang telah dilakukan termasuk dalam jenis penelitian pembuatan atau pengembangan. Agar menjawab rumusan masalah yang telah dibuat maka diperlukan perencanaan penelitian (Sarosa et al., 2023). Dalam sistem yang telah dibuat memiliki flowchart yang ditampilkan pada Gambar 1. Tahap pertama merupakan studi literatur mengenai kebutuhan alat dan bahan yang digunakan dalam pembuatan perencanaan sistem seperti refrensi terkait. Tahap kedua yaitu pencarian alat terkait berdasarkan hasil refrensi yang dibaca pada tahap sebelumnya. Tahap ketiga yaitu perancangan sistem yaitu membuat rancangan diagram blok sistem sesuai dengan alat yang didapat agar bisa menjadi sistem sesuai dengan penelitian yang akan dirancang. Tahap keempat merupakan pembuatan sistem dimana alat yang sudah disiapkan akan diintegrasikan menjadi satu kesatuan sistem sesuai dengan rancangan yang dibuat pada tahap sebelumnya. Tahap kelima ada pembuatan program

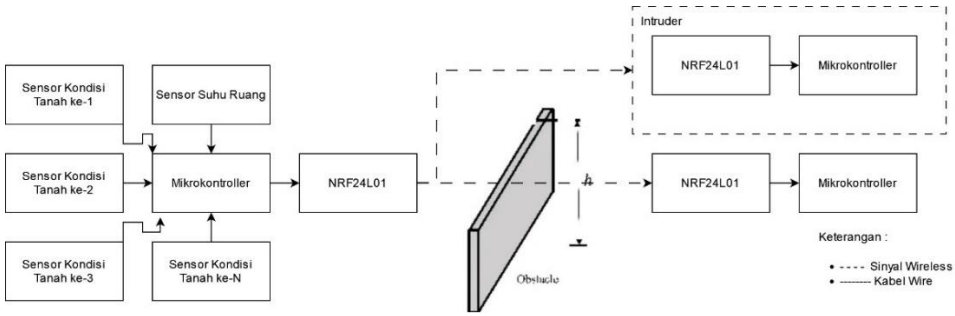
DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

untuk sistem pendukung monitoring dengan sistem WSN yang menggunakan paket header dan tidak menggunakan paket header untuk perbandingan data. Tahap keenam adalah pengujian sistem yang telah dibuat pada tahap ketiga dan keempat, pengujian dilakukan untuk mengetahui hasil pengujian sistem yang telah direncanakan. Tahap ketujuh merupakan tahap pengujian sistem yang sesuai dengan rancangan agar mendapatkan data data yang mendukung keberhasilan atau kegagalan sistem yang dibuat. Tahap kedelapan merupakan tahapan analisis hasil sistem dapat berjalan sesuai dengan yang telah direncanakan.



Gambar 1. Flowchart Penelitian

Pada Gambar 2 menunjukkan blok diagram dari penelitian yang sudah dilakukan.

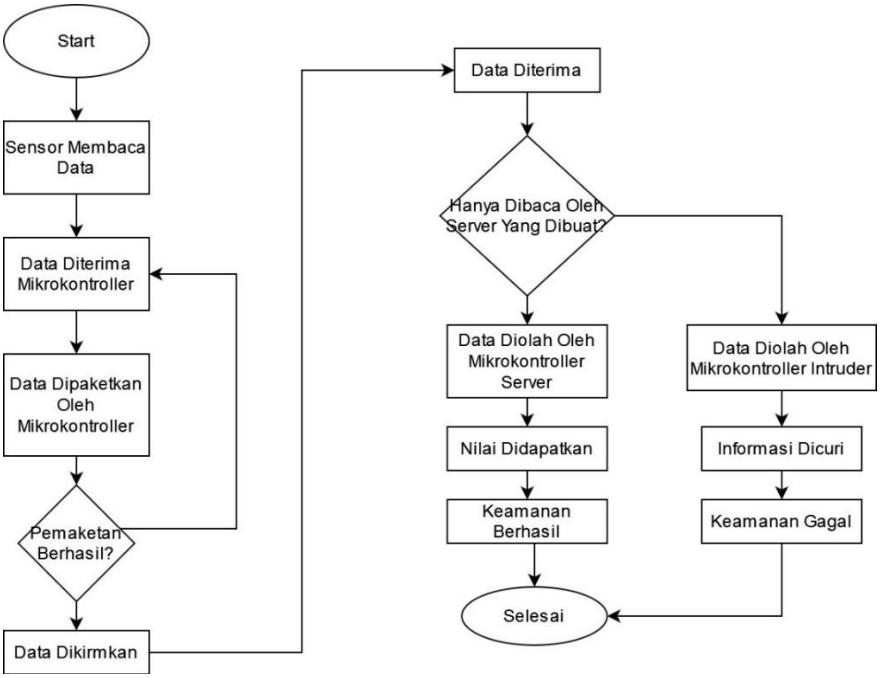


Gambar 2. Blok Diagram Sistem

DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Penjelasan blok diagram untuk penelitian ditunjukkan pada Gambar 2 dimana penjelasannya di bawah ini :

a. Sensor kondisi tanah berfungsi sebagai pengambil data kadar kualitas tanah. Dalam gambar diagram blok sistem jumlah sensor adalah 1,2, sampai dengan 16 dimana akan memaksimalkan kapasitas mikrokontroller dalam membaca dan mengirimkan data menggunakan NRF24L01.
b. Sensor suhu ruang berfungsi sebagai pembacaan temperature ruangan. Pada bagian ini hanya ditaruh 1 macam dikarenakan hanya menggunakan satu ruangan greenhouse.
c. Mikrokontroller merupakan bagian dari sistem karena merupakan perangkat yang berfungsi membaca data nilai sensor serta memaketkan data yang akan dikirimkan oleh NRF24L01. Sedangkan pada sisi penerima adalah perangkat yang akan membuka data paket yang diterima NRF24L01.
d. NRF24l01 berfungsi sebagai pemancar dan penerima data pada penelitian ini.
e. *Obstacle* merupkan salah satu bahan uji dari komunikasi yang akan diterapkan karena pada greenhouse tanaman akan bertambah tinggi yang akan menjadi obstacle pada pengiriman data (Hariyadi et al., 2023).



Gambar 3. Gambar Flowchart Sistem

Untuk cara kerja sistem pada Gambar 3 adalah sensor akan membaca data yang kemudian akan diterjemahkan oleh mikrokontroller. Kemudian mikrokontroller akan memaketkan data yang telah didapat. Dalam proses pemaketannya akan dilakukan 2 metode yaitu tanpa keamanan jaringan dan dengan keamanan jaringan. Data akan dikirimkan ke server yang telah dirancang menggunakan NRF24L01. Dalam sistem akan dibuat sebuah simulasi akan dilakukan pencuri data yang mencoba mengambil data dengan menebak jalur yang digunakan oleh pengirim data ke penerima data untuk menunjukkan proses pencurian data seperti yang terlihat pada Tabel 1. Hal ini diperlukan untuk memastikan bahwa sistem yang dibuat telah berhasil dilakukan. Selain pencurian data juga akan dilakukan manipulasi paket data pada penerima dan pengujian enkripsi yang telah dirancang yang termasuk dalam kategori pengujian keamanan data. Untuk proses simulasi ini akan ditambahkkan satu mikrokontroller lain yang terintegrasi dengan NRF24L01 sebagai perusak komunikasi data untuk simulasi diatas (Tawalbeh et al., 2020).

Untuk pengujian integritas data dakan dilakukan seperti yang terlihat pada Tabel 2. Pada pengujian ini akan dilakukan 3 simulasi pengujiian yang data akan langsung dibaca pada penerima atau server dari

DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

pengirim. Disini akan disimulasikan dengan membuat kondisi jaringan buruk dengan menambahkan penghalang serta pengujian pengaruh penggunaan paket header pada komunikasi NRF24L01 berpengaruh atau tidak dalam kualitas data (Abraham et al., 2019).

Tabel 1. Pengujian Keamanan Data

No.	Jenis Uji	Deskripsi Pengujian	Metode	Kriteria Keberhasilan
1	Data Interception	Pengujian untuk mendeteksi apakah ada upaya pencegatan data pada paket header	Simulasi serangan pencegatan pada jaringan	Tidak ada data yang berhasil dicegat
2	Data Tampering	Pengujian untuk mendeteksi perubahan tidak sah pada paket header	Simulasi manipulasi paket pada jaringan	Tidak ada perubahan yang berhasil terdeteksi
3	Encryption Effectiveness	Pengujian efektivitas enkripsi pada paket header	Pengujian enkripsi terhadap berbagai skenario	Data tetap terlindungi dan tidak dapat dibuka oleh pihak tidak berwenang

Tabel 2. Pengujian Integritas Data

No.	Jenis Uji	Deskripsi Pengujian	Metode	Kriteria Keberhasilan
1	Data Integrity Check	Pengujian integritas data pada paket header setelah transmisi	Verifikasi checksum atau hash pada penerima	Tidak ada perbedaan checksum/hash
2	Packet Loss Detection	Pengujian terhadap kehilangan paket selama transmisi	Simulasi kondisi jaringan buruk	Tidak ada paket yang hilang atau retransmisi berhasil
3	Data Consistency Verification	Pengujian konsistensi data antara pengirim dan penerima	Cross-check data antara pengirim dan penerima	Data yang diterima sesuai dengan yang dikirimkan

Untuk kinerja sistem data akan dilakukan seperti yang terlihat pada Tabel 3. Pada pengujian ini akan dilakukan 3 simulasi pengujiian yang data akan langsung dibaca pada penerima atau server dari pengirim. Pada bagian ini hanya melihat proses pengiriman dan kemampuan kinerja sistem baik dari sisi pengirim maupun penerima (Vedantham et al., 2022).

Tabel 3. Pengujian Kinerja Sistem

No.	Jenis Uji	Deskripsi Pengujian	Metode	Kriteria Keberhasilan
1	Latency Test	Pengujian waktu keterlambatan (latency) transmisi data dengan proteksi paket header	Pengukuran waktu pengiriman dan penerimaan	Latency tidak melebihi ambang batas yang ditentukan
2	Throughput Analysis	Pengujian terhadap kapasitas maksimum jaringan dalam mengirim data	Pengukuran throughput jaringan	Throughput tetap tinggi meskipun ada proteksi paket header
3	Power Consumption Test	Pengujian konsumsi daya perangkat NRF24L01 dengan proteksi paket header	Pengukuran penggunaan daya selama operasi	Konsumsi daya tidak melebihi standar yang ditentukan

3. HASIL DAN PEMBAHASAN

Hasil pembuatan alat ditunjukkan pada Gambar 4 yang merupakan hasil rangkaian keseluruhan sistem pembacaan data sebanyak N-Sensor (untuk mikrokontroller yang digunakan memiliki 16 pin data sensor) (Fauziah et al., 2024). Dimana nanti akan digunakan seluruh pin sensornya untuk mengirimkan data sebanyak 16 data dimana terdiri dari 8 data nilai pH dan 8 data nilai kelembaban tanah.

DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

Gambar 4. Implementasi Hardware

Pada Gambar 5 hasil pembuatan software berupa kode pada Arduino IDE untuk proses pemaketan data dengan memberi header agar M sebagai tanda merupakan paket data M yang berisikan data yang di struktur di bagian sebelumnya. Jika pengiriman gagal maka akan keluar "Send Fail" dan jika berhasil akan keluar data "Send Ok" untuk ID node ini.

Gambar 5. Hasil Implementasi Program Pada Arudino IDE

Pengujian keamanan data pada Tabel 4 menunjukkan bahwa proteksi pada paket header NRF24L01 berhasil mencegah semua upaya pencegatan dan manipulasi data. Dari 16 data yang diuji, tidak ada satu pun yang berhasil dicegat atau diubah oleh serangan yang dilakukan. Ini menandakan bahwa enkripsi dan metode proteksi yang diterapkan sangat efektif dalam menjaga kerahasiaan dan integritas data. Tingkat keberhasilan yang mencapai 100% mencerminkan bahwa sistem memiliki ketahanan yang kuat terhadap ancaman keamanan eksternal (Septiano & Ghozali, 2020).

Tabel 4. Hasil Pengujian Keamanan Data

No.	Jenis Uji	Jumlah Data Diuji	Jumlah Serangan	Data Berhasil Dicegat	Persentase Keberhasilan
1	Data Interception	16	10	0	100%
2	Data Tampering	16	10	0	100%
3	Encryption Effectiveness	16	10	0	100%

Hasil pengujian integritas data pada Tabel 5 menunjukkan bahwa sistem dapat mempertahankan keutuhan data dengan sangat baik, meskipun ada sedikit kehilangan paket. Dari 100 data yang diuji, hanya satu paket yang hilang dan satu paket lainnya mengalami kerusakan, yang mengakibatkan tingkat

DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

keberhasilan sebesar 99%. Meskipun demikian, tingkat kehilangan dan kerusakan yang rendah ini tidak secara signifikan mempengaruhi performa keseluruhan sistem (Desnanjaya & Alfian, 2020). Hal ini menunjukkan bahwa mekanisme pemulihan dan verifikasi data dalam sistem berfungsi dengan baik. Dengan demikian, proteksi paket header tetap mampu menjaga konsistensi dan integritas data selama transmisi.

Pada pengujian kinerja sistem Tabel 6, hasil menunjukkan bahwa proteksi paket header tidak menimbulkan penurunan yang signifikan dalam performa sistem. Rata-rata waktu keterlambatan (latency) adalah 20 ms, yang masih berada dalam ambang batas yang dapat diterima untuk aplikasi di greenhouse. Throughput yang dicapai sebesar 250 kbps menunjukkan bahwa sistem masih mampu mengirimkan data dalam jumlah besar secara efisien. Konsumsi daya yang relatif stabil, yaitu antara 48 hingga 50 mW, juga menunjukkan bahwa proteksi tambahan ini tidak memberikan beban berlebihan pada perangkat. Secara keseluruhan, proteksi pada paket header terbukti efektif tanpa mengorbankan efisiensi operasional sistem (Pengaruh & Dan, 2024).

Tabel 5. Hasil Pengujian Integritas Data

No.	Jenis Uji	Jumlah Data Diuji	Data yang Hilang	Data yang Rusak	Data Diterima dengan Sukses	Persentase Keberhasilan
1	Data Integrity Check	16	0	0	100	100%
2	Packet Loss Detection	16	1	0	99	99%
3	Data Consistency Verification	16	0	1	99	99%

Tabel 6. Hasil Pengujian Integritas Data

No.	Jenis Uji	Jumlah Data Diuji	Waktu Rata-rata (ms)	Throughput (kbps)	Konsumsi Daya (mW)
1	Latency Test	16	20	-	50
2	Throughput Analysis	16	-	250	50
3	Power Consumption Test	16	-	-	48

4. KESIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa proteksi pada paket header NRF24L01 dalam jaringan nirkabel sensor di greenhouse secara signifikan meningkatkan keamanan dan integritas data, tanpa mengorbankan kinerja sistem. Pengujian keamanan data menunjukkan keberhasilan 100% dalam mencegah upaya pencegatan dan manipulasi data, sementara integritas data terjaga dengan tingkat keberhasilan penerimaan sebesar 99%, yang menunjukkan bahwa sistem memiliki mekanisme pemulihan yang efektif untuk menjaga konsistensi data selama transmisi. Dari sisi kinerja, proteksi ini tidak menyebabkan penurunan performa yang signifikan, sehingga sistem tetap beroperasi dengan latency rendah, throughput tinggi, dan konsumsi daya yang efisien.

Temuan ini memberikan kontribusi penting bagi pengembangan teknologi jaringan sensor nirkabel yang aman dan andal, khususnya untuk mendukung keberlanjutan dan efisiensi dalam produksi pertanian modern. Dalam implementasi praktis, proteksi pada paket header NRF24L01 dapat diadopsi sebagai langkah keamanan tambahan yang sederhana namun efektif dalam mengatasi tantangan keamanan di lingkungan greenhouse yang terhubung. Namun, penelitian ini memiliki batasan, terutama terkait cakupan pengujian yang dilakukan hanya pada lingkungan greenhouse skala terbatas. Rekomendasi untuk penelitian lanjutan adalah memperluas cakupan pengujian dengan melibatkan variasi lingkungan dan kondisi jaringan yang berbeda, serta mengeksplorasi metode proteksi tambahan yang dapat semakin meningkatkan keamanan dan performa jaringan sensor. Hal ini diharapkan dapat memperkaya pemahaman terhadap keamanan WSN dan mendukung penerapan teknologi serupa di sektor pertanian dan industri lainnya.

DAFTAR PUSTAKA

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework,

DOI: https://doi.org/10.54082/jupin.777
p-ISSN: 2808-148X
e-ISSN: 2808-1366

structured review, and research agenda. *International Journal of Information Management*, *49*(January), 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Desnanjaya, I. G. M. N., & Alfian, M. D. (2020). Pengiriman Data Nrf24L01+ Dengan Kondisi Line of Sight Dan Non Line of Sight. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *3*(2), 128–139. https://doi.org/10.31598/jurnalresistor.v3i2.663

Fauziah, N., Munazilin, A., & Santoso, F. (2024). Rancang Bangun Sistem Pengontrol Irigasi Otomatis Menggunakan Mikrokontroller Arduino Uno. *G-Tech: Jurnal Teknologi Terapan*, *8*(3), 1464–1473. https://doi.org/10.33379/gtech.v8i3.4343

Gheorghiu, R. A., Minea, M., Iordache, V., & Buretea, L. D. (2023). Field testing of nRF24 communications as a support for Smart City applications. *2023 46th International Conference on Telecommunications and Signal Processing, TSP 2023*, *Cdi*, 74–77.

Hadiwiyatno, Yoga, S. W., & Zakaria, M. N. (2020). Microcontroller and Wireless Communication Based Smart Laboratory Box System Implementation. *Proceeding - 2020 3rd International Conference on Vocational Education and Electrical Engineering: Strengthening the Framework of Society 5.0 through Innovations in Education, Electrical, Engineering and Informatics Engineering, ICVEE 2020*, 2–7. https://doi.org/10.1109/ICVEE50212.2020.9243240

Hariyadi, M. A., Fadila, J. N., & Sifaulloh, H. (2023). 433Mhz based Robot Using Proportional Integral Derivative (PID) for Precise Facing Direction. *International Journal on Informatics Visualization*, *7*(3), 991–999. https://doi.org/10.30630/joiv.7.3.1841

Junus, M., Marjono, Yoga, S. W., & Wahyudi, S. (2022). Smart Charging Based on Hybrid Power Plants Ah Buildings Polinema Using Wireless Sensor Network. *International Journal of Electrical Engineering*, *29*(2), 35–41. https://doi.org/10.6329/CIEE.202204_29(2).0002

Mikhaylov, A., Moiseev, N., Aleshin, K., & Burkhardt, T. (2020). Global climate change and greenhouse effect. *Entrepreneurship and Sustainability Issues*, *7*(4), 2897–2913. https://doi.org/10.9770/jesi.2020.7.4(21)

Pengaruh, A., & Dan, J. (2024). *KOMUNIKASI ANTAR KENDARAAN BERBASIS NRF24L01*. *11*(1), 197–203.

Reyes-Medina, S., Toro-Ossaba, A., Noguera, A., Tejada, J. C., & Rua, S. (2022). Wireless measurement system with potential application in the diagnosis of construction machinery. *2022 IEEE ANDESCON: Technology and Innovation for Andean Industry, ANDESCON 2022*, 13–17. https://doi.org/10.1109/ANDESCON56260.2022.9989940

Sarosa, M., Hapsari, R. I., Adhisuwignjo, S., Moentamaria, D., Irawan, B., Putri, R. I., & Wirayoga, S. (2023). Air Cleaning System Based On The Internet Of Things (IoT). *2023 International Conference on Electrical and Information Technology (IEIT)*, 367–371. https://doi.org/10.1109/ieit59852.2023.10335547

Septiano, A., & Ghozali, T. (2020). Nrf 24L01 Sebagai Pemancar/Penerima Untuk Wireless Sensor Network. *Jurnal TEKNO (Civil Engineeering, Elektrical Engineeering and Industrial Engineeering)*, *17*(1), 26–34.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). applied sciences IoT Privacy and Security : Challenges and Solutions. *Mdpi*, 1–17.

Vedantham, L. S., Zhou, Y., & Wu, J. (2022). Information and communications technology (ICT) infrastructure supporting smart local energy systems: A review. *IET Energy Systems Integration*, *4*(4), 460–472. https://doi.org/10.1049/esi2.12063

Wirayoga, S., Anshori, M. A., Maudina, T., Junus, M., & Rasyid, A. (2023). Controller Monitoring Automation System Soil pH and Moisture Orange Seeds Based on Wireless Sensor Network. *Fidelity : Jurnal Teknik Elektro*, *5*(3), 156–167. https://doi.org/10.52005/fidelity.v5i3.166

Wirayoga, S., Imammuddien, A. M., Wahyuningsih, F. D., & Harismawati, S. (2023). Rancang bangun sistem pengaman rumah dengan aplikasi android berbasis motion detection dan QR code. *Jurnal Eltek*, *21*(1), 36–41. https://doi.org/10.33795/eltek.v21i1.364