

Keamanan Jaringan Pada Wireless Terhadap Serangan Intruders Menggunakan Metode RSA

Kevin Alfareza ¹⁾; RG Guntur Alam ²⁾; A.R. Walad Mahfuzhi ³⁾; Dedy Abdullah ⁴⁾
^{1,2,3,4)}Program Studi Teknik Informatika Fakultas Teknik, Universitas Muhammadiyah Bengkulu
Email: ¹⁾kevinalfareza08@gmail.com

ARTICLE HISTORY

Received [15 Juli 2026]

Revised [19 Oktober 2026]

Accepted [21 Oktober 2026]

KEYWORDS

Network Security, Wireless,
Intruders, Cryptography, RSA.

*This is an open access
article under the [CC-BY-SA](#)
license*



ABSTRAK

Pesatnya perkembangan teknologi jaringan wireless telah memberikan kemudahan dalam komunikasi serta pertukaran informasi secara cepat dan fleksibel. Meskipun demikian, karakteristik media transmisi yang bersifat terbuka menyebabkan jaringan wireless memiliki tingkat kerentanan yang tinggi terhadap berbagai ancaman keamanan, seperti penyadapan (eavesdropping) dan akses oleh pihak yang tidak berwenang (intruders). Ancaman tersebut berpotensi mengakibatkan kebocoran informasi serta mengurangi kerahasiaan data selama proses transmisi. Untuk mengatasi permasalahan tersebut, diperlukan mekanisme pengamanan yang mampu menjaga kerahasiaan informasi ketika data dikirimkan melalui jaringan. Penelitian ini bertujuan untuk mengevaluasi penerapan algoritma RSA sebagai metode kriptografi dalam meningkatkan keamanan jaringan wireless dari serangan intruders. Pendekatan penelitian yang digunakan adalah metode eksperimen (Experimental Research) dengan membangun lingkungan jaringan wireless, mengimplementasikan algoritma RSA pada proses enkripsi dan dekripsi data, kemudian melakukan simulasi serangan untuk menilai tingkat keamanan sistem. Pengujian dilaksanakan pada dua kondisi, yaitu sebelum dan setelah implementasi algoritma RSA, sehingga efektivitas metode yang diterapkan dapat dibandingkan secara objektif. Evaluasi dilakukan dengan memperhatikan beberapa indikator, meliputi kerahasiaan data (confidentiality), integritas data (integrity), kemampuan sistem dalam mencegah akses tidak sah, serta pengaruh penerapan algoritma RSA terhadap performa jaringan. Hasil penelitian diharapkan menunjukkan bahwa penggunaan algoritma RSA mampu meningkatkan tingkat keamanan jaringan wireless melalui proses transformasi data dari bentuk plaintext menjadi ciphertext. Dengan demikian, data yang berhasil diperoleh oleh pihak yang tidak berwenang tidak dapat dipahami tanpa kunci privat yang sesuai. Berdasarkan hasil tersebut, algoritma RSA dapat dijadikan sebagai salah satu alternatif solusi untuk memperkuat perlindungan data pada jaringan wireless terhadap ancaman penyadapan maupun akses yang tidak sah.

ABSTRACT

The rapid development of wireless network technology has provided ease in communication and exchange of information quickly and flexibly. However, the characteristics of open transmission media cause wireless networks to have a high level of vulnerability to various security threats, such as eavesdropping and access by unauthorized parties (intruders). The threat has the potential to cause information leakage and reduce data confidentiality during the transmission process. To overcome these problems, a security mechanism is needed that is able to maintain the confidentiality of information when data is transmitted over the network. This study aims to evaluate the application of RSA algorithm as a cryptographic method in improving the security of wireless networks from intruders. The research approach used is an experimental Research method by building a wireless network environment, implementing the RSA algorithm in the process of encryption and decryption of data, then perform a simulation attack to assess the level of system security. The tests were carried out in two conditions, before and after the implementation of the RSA algorithm, so that the effectiveness of the applied methods can be objectively compared. The evaluation was conducted by taking into account several indicators, including data confidentiality, data integrity, the ability of the system to prevent unauthorized access, and the effect of the application of the RSA algorithm on network performance. The results are expected to show that the use of RSA algorithm is able to increase the level of wireless network security through the process of data transformation from plaintext to ciphertext. Thus, the data successfully obtained by unauthorized parties cannot be understood without the corresponding private key. Based on these results, the RSA algorithm can be used as an alternative solution to strengthen data protection on wireless networks against the threat of eavesdropping and unauthorized access.

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah mendorong terjadinya berbagai perubahan dalam kehidupan masyarakat, khususnya dalam cara memperoleh dan bertukar informasi. Salah satu teknologi yang berkembang pesat adalah jaringan nirkabel (*wireless*), yaitu teknologi komunikasi yang memungkinkan perangkat terhubung ke jaringan internet tanpa memerlukan media kabel sebagai penghubung. (Alodat, 2022). Jaringan wireless banyak digunakan di berbagai tempat, seperti rumah, sekolah, kampus, perkantoran, hingga tempat umum karena memberikan kemudahan dalam mengakses informasi dan berkomunikasi (Hamdi Putra, 2025)

Meskipun memiliki banyak kelebihan, penggunaan jaringan *wireless* juga memiliki berbagai risiko keamanan. Data yang dikirim melalui jaringan *wireless* dapat menjadi sasaran pihak yang tidak bertanggung jawab. Salah satu ancaman yang sering terjadi adalah adanya intruders, yaitu pihak yang mencoba masuk ke dalam jaringan tanpa izin untuk mengakses, mencuri, mengubah, atau merusak data yang ada. Kondisi ini dapat menyebabkan kerugian bagi pengguna maupun pengelola jaringan, terutama jika data yang disalahgunakan bersifat penting dan rahasia (PINONTOAN, 2024).

Keamanan jaringan menjadi aspek yang sangat penting untuk diperhatikan guna melindungi data dan informasi dari berbagai ancaman. Salah satu cara yang dapat digunakan untuk meningkatkan keamanan jaringan adalah dengan menerapkan teknologi kriptografi (Rafael et al., 2025). Kriptografi merupakan teknik yang digunakan untuk mengamankan data dengan cara mengubah informasi asli menjadi bentuk yang sulit dipahami oleh pihak yang tidak memiliki hak akses (Selvi et al., 2025).

Salah satu algoritma kriptografi yang banyak digunakan adalah RSA (*Rivest-Shamir-Adleman*). RSA merupakan algoritma kriptografi asimetris yang menggunakan dua kunci, yaitu kunci publik untuk proses *enkripsi* dan kunci privat untuk proses dekripsi (Mulyanto et al., 2022). Dengan metode ini, data yang dikirim melalui jaringan *wireless* dapat dienkripsi terlebih dahulu sehingga tidak dapat dibaca oleh pihak yang melakukan penyadapan atau akses tanpa izin (Walle, 2024).

TINJAUAN PUSTAKA

Keamanan jaringan merupakan serangkaian upaya yang dilakukan untuk melindungi jaringan komputer, data, serta perangkat yang terhubung di dalamnya dari berbagai ancaman dan serangan. Tujuan utama keamanan jaringan adalah menjaga agar informasi yang dikirim dan diterima melalui jaringan tetap aman, tidak dapat diakses oleh pihak yang tidak berwenang, serta terhindar dari kerusakan atau penyalahgunaan (Puttaswamy & Shivaprasad, 2024).

Dalam sebuah jaringan, keamanan sangat penting karena data yang ditransmisikan rentan terhadap berbagai ancaman, seperti penyadapan, pencurian data, peretasan, dan serangan *malware*. Maka, diperlukan mekanisme keamanan yang mampu melindungi sistem dan informasi yang terdapat dalam jaringan (Satria Galang Saputra et al., 2023).

Keamanan jaringan memiliki tiga aspek utama, yaitu:

1. Kerahasiaan (*Confidentiality*), yaitu menjaga agar informasi hanya dapat diakses oleh pihak yang memiliki hak akses.
2. Integritas (*Integrity*), yaitu memastikan bahwa data yang dikirim atau disimpan tidak mengalami perubahan tanpa izin.
3. Ketersediaan (*Availability*), yaitu menjamin bahwa data dan layanan jaringan dapat digunakan oleh pengguna yang berhak ketika dibutuhkan.

Dengan adanya keamanan jaringan yang baik, risiko terjadinya pencurian data, akses ilegal, dan gangguan terhadap sistem dapat diminimalkan sehingga aktivitas komunikasi dan pertukaran informasi melalui jaringan dapat berjalan dengan aman dan lancar.

Penelitian yang dilakukan oleh Yogendra Kumar dan Vijay Kumar (2023) dengan judul "*A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications*" membahas berbagai jenis serangan yang terjadi pada jaringan *wireless* serta penerapan sistem deteksi intrusi (*Intrusion Detection System/IDS*) sebagai solusi keamanan. Hasil penelitian menunjukkan bahwa ancaman seperti akses tidak sah, penyadapan data, dan berbagai bentuk intrusi masih menjadi tantangan utama dalam pengelolaan jaringan *wireless*. Penelitian ini juga menekankan pentingnya pengembangan sistem keamanan yang mampu melindungi jaringan dari aktivitas *intruders*.

Kemudian penelitian yang dilakukan oleh Firdaus (2024) dengan judul "*Development of Network Security Systems Using Computer-Based Encryption and Authentication Techniques*" membahas pengembangan sistem keamanan jaringan menggunakan teknik enkripsi dan autentikasi berbasis algoritma RSA. Hasil penelitian menunjukkan bahwa kombinasi enkripsi RSA dan autentikasi mampu meningkatkan keamanan jaringan secara signifikan serta mengurangi risiko kebocoran data dan akses yang tidak sah. Penelitian ini menunjukkan bahwa algoritma RSA memiliki peran penting dalam menjaga kerahasiaan informasi yang ditransmisikan melalui jaringan.

Selanjutnya Penelitian yang dilakukan oleh Manesh Thankappan, Helena Rifà-Pous, dan Carles Garrigues (2024) dengan judul "*A Distributed and Cooperative Signature-Based Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks*" mengembangkan sistem deteksi intrusi untuk menghadapi serangan *Man-in-the-Middle* pada jaringan *Wi-Fi*. Hasil penelitian menunjukkan bahwa sistem yang dikembangkan mampu mendeteksi aktivitas serangan secara efektif sehingga dapat meningkatkan keamanan jaringan *wireless*. Penelitian ini

membuktikan bahwa ancaman *intruders* pada jaringan *Wi-Fi* masih menjadi permasalahan yang memerlukan perhatian khusus.

Setelah itu Penelitian yang dilakukan oleh Moh. Rafael Kamil Ardiansyah dan Radhitya Dwi Akmal Purnomo (2025) dengan judul "*Security and Privacy Challenges in Wireless Sensor Networks: A Systematic Literature Review of Threat Mitigation Strategies*" membahas berbagai bentuk ancaman keamanan yang berpotensi menyerang jaringan *nirkabel*, di antaranya serangan *blackhole*, *sinkhole*, *wormhole*, *Sybil*, *Denial of Service (DoS)*, dan *Man-in-the-Middle Attack*.

Penelitian ini menemukan bahwa berbagai serangan tersebut dapat mengancam aspek-aspek fundamental keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data dalam jaringan. Selain itu, penelitian ini mengemukakan bahwa penerapan teknik kriptografi, mekanisme autentikasi, serta sistem deteksi intrusi merupakan strategi yang efektif dalam meningkatkan keamanan jaringan dan meminimalkan risiko serangan pada lingkungan jaringan *wireless*.

Selanjutnya, Penelitian yang dilakukan oleh Habiburrahman dan Ubaidillah Hamdi Putra (2025) dengan judul "Analisis Peran dan Tantangan Keamanan Jaringan pada *Wireless Sensor Network (WSN)*" mengkaji peran penting keamanan jaringan dalam menjamin kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan autentikasi data pada sistem *Wireless Sensor Network*.

Berdasarkan hasil penelitian, diketahui bahwa *WSN* memiliki tingkat kerentanan yang cukup tinggi terhadap berbagai ancaman keamanan, seperti serangan intrusi, penyadapan informasi, manipulasi paket data, serta serangan *Denial of Service (DoS)*. Berdasarkan temuan tersebut, penelitian ini menegaskan bahwa penerapan teknik enkripsi dan mekanisme keamanan yang efektif sangat diperlukan untuk melindungi data selama proses transmisi pada jaringan *wireless* serta meminimalkan risiko yang ditimbulkan oleh berbagai ancaman keamanan.

Berdasarkan berbagai penelitian terdahulu, dapat disimpulkan bahwa keamanan jaringan *wireless* merupakan aspek yang sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data dari berbagai ancaman keamanan. Beragam serangan, seperti intrusi, penyadapan, dan manipulasi data, dapat mengganggu proses komunikasi serta membahayakan informasi yang ditransmisikan melalui jaringan.

Hasil kajian terdahulu menyatakan bahwa menunjukkan bahwa penerapan algoritma kriptografi, khususnya RSA, efektif dalam meningkatkan tingkat keamanan data selama proses transmisi. Oleh karena itu, penelitian mengenai Keamanan Jaringan pada *Wireless* terhadap Serangan Intruders Menggunakan Metode RSA dilakukan untuk mengimplementasikan algoritma RSA sebagai mekanisme pengamanan data guna mencegah akses tidak sah dan melindungi jaringan *wireless* dari berbagai bentuk serangan yang dilakukan oleh pihak yang tidak berwenang.

Jaringan Wireless

Jaringan *wireless* merupakan jaringan komunikasi yang menggunakan media gelombang radio untuk melakukan pertukaran data tanpa menggunakan kabel sebagai media transmisi. Penggunaan jaringan *wireless* memberikan kemudahan dalam mobilitas pengguna karena perangkat dapat saling terhubung selama masih berada dalam jangkauan sinyal. Teknologi ini banyak diterapkan pada lingkungan pendidikan, perkantoran, industri, maupun rumah tangga karena proses instalasinya lebih sederhana dibandingkan jaringan kabel (Januari et al., 2026).

Meskipun memiliki berbagai keunggulan, jaringan *wireless* juga memiliki tingkat kerentanan yang lebih tinggi terhadap ancaman keamanan. Hal tersebut disebabkan media transmisi yang digunakan bersifat terbuka sehingga sinyal dapat diterima oleh perangkat lain yang berada dalam jangkauan jaringan. Kondisi ini memungkinkan terjadinya penyadapan data, pencurian informasi, hingga akses tidak sah yang dilakukan oleh pihak lain.

Intruders

Intruders merupakan individu atau pihak yang berusaha memperoleh akses ke suatu sistem atau jaringan tanpa memiliki hak atau izin dari pemilik sistem. Tujuan utama *intruders* dapat berupa memperoleh informasi penting, mencuri data, mengubah informasi, ataupun mengganggu kinerja jaringan (Voyiatzis & Serpanos, 2007).

Dalam jaringan *wireless*, *intruders* dapat melakukan berbagai jenis serangan, seperti *packet sniffing*, *eavesdropping*, *spoofing*, *Man-in-the-Middle Attack*, maupun *Denial of Service (DoS)*. Ancaman tersebut dapat menyebabkan kebocoran data, hilangnya integritas informasi, dan terganggunya layanan jaringan apabila tidak diantisipasi dengan mekanisme keamanan yang memadai.

Kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik pengamanan informasi dengan cara mengubah data asli (plaintext) menjadi bentuk yang tidak dapat dipahami (ciphertext). Tujuan utama kriptografi adalah menjaga kerahasiaan, integritas, autentikasi, dan keaslian data selama proses penyimpanan maupun transmisi (Hamdi Putra, 2025).

Secara umum, algoritma kriptografi dibagi menjadi dua kelompok, yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan algoritma asimetris menggunakan dua kunci yang berbeda, yaitu kunci publik (public key) dan kunci privat (private key).

Algoritma RSA

Algoritma RSA (*Rivest-Shamir-Adleman) merupakan salah satu metode kriptografi asimetris yang diperkenalkan oleh Ronald Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1977. Berbeda dengan kriptografi simetris yang menggunakan satu kunci, RSA memanfaatkan sepasang kunci yang saling berkaitan, yaitu kunci publik (public key) untuk melakukan proses enkripsi serta kunci privat (private key) yang berfungsi untuk mengembalikan data terenkripsi ke bentuk aslinya melalui proses dekripsi (Irfan et al., 2024).

METODE PENELITIAN

Metode penelitian

Pendekatan penelitian yang digunakan adalah metode eksperimen (Experimental Research) dengan membangun lingkungan jaringan wireless, mengimplementasikan algoritma RSA pada proses enkripsi dan dekripsi data, kemudian melakukan simulasi serangan untuk menilai tingkat keamanan sistem. Pengujian dilaksanakan pada dua kondisi, yaitu sebelum dan setelah implementasi algoritma RSA, sehingga efektivitas metode yang diterapkan dapat dibandingkan secara objektif. Evaluasi dilakukan dengan memperhatikan beberapa indikator, meliputi kerahasiaan data (confidentiality), integritas data (integrity), kemampuan sistem dalam mencegah akses tidak sah, serta pengaruh penerapan algoritma RSA terhadap performa jaringan.

Model Pengembangan System (RPL)

Algoritma yang digunakan dalam penelitian ini adalah algoritma RSA yang menggunakan bahasa pemrograman java dan Sistem perancangan menggunakan model Rapid application development (RAD). Menurut Sandy Kosasi (2015) Metode RAD (Rapid Application Development) menggunakan metode iteratif (berulang) dalam mengembangkan sistem dimana model bekerja sistem dikonstruksikan di awal tahap pengembangan dengan tujuan menetapkan kebutuhan pengguna.

Berikut adalah langkah pendekatan Rapid application development (RAD):

Bussines modeling

Langkah ini digunakan untuk perancangan dasar dari suatu system, analisis keamanan yang lengkap dilakukan untuk menganamankan jaringan yang penting bagi pengguna, bagaimana serangan itu bias terjadi, kapan dan bagaimana cara algoritma RSA menangani serangan tersebut.

Data modeling

Langkah ini digunakan untuk menganalisis informasi ataupun data yang sudah dikumpulkan dari langkah bussines modeling. Semua data yang dikumpulkan diidentifikasi secara rinci untuk mencari model bisnis yang tepat

1. Proses modeling

Untuk menentukan arus bagaimana cara mengamankan jaringan dan untuk mencapai hasil pengamanan yang sesuai dengan model keamanan.

2. Application generation

Fase ini untuk system yang sebenarnya dibangun dan pengkodean dilakukan dengan menggunakan alat otomatis untuk mengubah model proses yang akurat.

3. Testing and turn over

Untuk pengujian keseluruhan system yang dibangun oleh semua komponen yang perlu diuji secara menyeluruh dengan uji yang lengkap agar bias menghindari resiko cacat system.

HASIL DAN PEMBAHASAN

Hasil

Hasil penelitian diharapkan menunjukkan bahwa penggunaan algoritma RSA mampu meningkatkan tingkat keamanan jaringan wireless melalui proses transformasi data dari bentuk plaintext menjadi ciphertext. Dengan demikian, data yang berhasil diperoleh oleh pihak yang tidak berwenang tidak dapat dipahami tanpa kunci privat yang sesuai. Berdasarkan hasil tersebut, algoritma RSA dapat dijadikan sebagai salah satu alternatif solusi untuk memperkuat perlindungan data pada jaringan wireless terhadap ancaman penyadapan maupun akses yang tidak sah.

Pembahasan

Enkripsi dan deskripsi metode RSA

Langkah-langkah dalam mengenkripsi atau mendeskripsi RSA Adalah sebagai berikut:

1. Pilih 2 buah bilangan prima p dan q .
2. Hitung nilai $n = p * q$, (usahakan agar setidaknya $n > 255$ agar dapat mewakili seluruh karakter ASCII).
3. Hitung nilai $m = (p-1) * (q-1)$.
4. Cari nilai e , dimana e merupakan relatif prima dari m .
5. Cari nilai d , yang memenuhi persamaan $ed \equiv 1 \text{ mod } m$ atau $d = e^{-1} \text{ mod } m$.
6. Kunci public (e, n) dan kunci private (d, n).
7. Fungsi enkripsi $\rightarrow E(ta) = t^e \text{ mod } n$; dimana t merupakan karakter ke- a dari message (pesan) yang akan dienkripsi.
8. Fungsi dekripsi $\rightarrow D(ca) = c^d \text{ mod } n$; dimana c merupakan karakter ke- a dari ciphertext yang akan didekripsikan

Penerapan metode RSA

Implementasi metode RSA pada sistem yang dikembangkan dalam penelitian ini diawali ketika pengguna, misalnya Endang, akan mengirimkan pesan kepada Server. Pada tahap tersebut, sistem akan meminta Server sebagai penerima pesan untuk menghasilkan sepasang kunci kriptografi, yaitu kunci publik (public key) dan kunci privat (private key). Sesuai dengan mekanisme algoritma RSA, proses pembangkitan kunci dilakukan oleh pihak penerima sehingga kunci privat tetap tersimpan di server dan tidak pernah dikirimkan kepada pihak lain. Sebaliknya, kunci publik didistribusikan kepada komputer pengirim agar dapat digunakan untuk mengenkripsi pesan sebelum proses pengiriman dilakukan. Dengan mekanisme tersebut, hanya pihak penerima yang memiliki kunci privat yang dapat mendekripsi dan membaca isi pesan yang telah dienkripsi.

KESIMPULAN

Dari hasil perancangan, pengujian dan implementasi program yang telah dilakukan terhadap sistem keamanan jaringan pada Wireless terhadap serangan Intruder menggunakan metode RSA, dapat disimpulkan sebagai berikut :

1. Dari hasil pengujian sistem, ukuran 1024 Bit berhasil digunakan sedangkan dengan ukuran lebih dari 1024 Bit enkripsi tidak dapat berhasil pada sistem yang dibuat,
2. Data enkripsi angka dan huruf berhasil sedangkan data gambar tidak dapat di enkripsi. Dalam kondisi koneksi internet mati dan hidup sistem tetap dapat digunakan lain halnya dengan koneksi jaringan ketika koneksi jaringan terhubung sistem dapat digunakan akan tetapi jika koneksi terputus sistem tidak dapat digunakan. Adapun penggunaan sistem ini hanya dapat digunakan maksimal 10 orang. Dan Jarak lokasi penggunaan sistem antar pengguna ketika dalam satu jaringan Maksimal 10 Meter.

DAFTAR PUSTAKA

- Alodat, I. (2022). Wireless Networks Encryption by Simulation of Attacks. *International Journal of Electrical and Electronic Engineering and Telecommunications*, 11(5), 351–355. <https://doi.org/10.18178/ijeetc.11.5.351-355>
- Hamdi Putra, U. (2025). Analisis Peran dan Tantangan Keamanan Jaringan pada Wireless Sensor Network (WSN). *Karapan Network Journal*, 1, No.1(1). <http://creativecommons.org/licenses/by/4.0/>

- Irfan, A., Nusri, A. Z., Rachmat, Z., & Wulandari, S. (2024). Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS). *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, 7(1), 110–119. <https://doi.org/10.57093/jisti.v7i1.195>
- Januari, N., Moly, A. H., Mau, S. D. I., & Ledi, D. F. (2026). Analisis Keamanan Jaringan Komputer Menggunakan Metode Penetration Testing dikelola oleh Universitas Andalas untuk mengumpulkan , mengelola , mendokumentasikan , dan Permasalahan utama pada situs Repository Universitas Andalas adalah masih digunakannya pr. (November 2025).
- Mulyanto, Y., Herfandi, & Candra Kirana, R. (2022). 1528-Article Text-4037-1-10-20220219. *JINTEKS (Jurnal Informatika Teknologi Dan Sains)*, 4(1), 26–35.
- PINONTOAN. (2024). *Skripsi keamanan jaringan berbasis intrusion detection system*.
- Puttaswamy, C., & Shivaprasad, N. P. K. (2024). Enhancing wireless sensor network security with optimized cluster head selection and hybrid public-key encryption. *International Journal of Electrical and Computer Engineering*, 14(3), 2976–2987. <https://doi.org/10.11591/ijece.v14i3.pp2976-2987>
- Rafael, M., Ardiansyah, K., Dwi, R., & Purnomo, A. (2025). Security and Privacy Challenges in Wireless Sensor Networks: A Systematic Literature Review of Threat Mitigation Strategies. *Karapan Network Journal*, 1, No.1(1). <http://creativecommons.org/licenses/by/4.0/>
- Satria Galang Saputra, Parga Zen, B., & Abdurahman. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). *Jurnal Sistem Informasi Galuh*, 1(2), 43–51. <https://doi.org/10.25157/jsig.v1i2.3152>
- Selvi, M., Santhosh Kumar, S. V. N., Thangaramya, K., & Abdul Gaffar, H. (2025). Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks. *Scientific Reports*, 15(1). <https://doi.org/10.1038/s41598-025-03558-8>
- Voyiatzis, A. G., & Serpanos, D. N. (2007). Wireless Sensor Networks. *Network Security: Current Status and Future Directions*, 375–390. <https://doi.org/10.1002/9780470099742.ch21>
- Walle, Y. M. (2024). Hybrid RSA–AES-Based Software-Defined Network to Improve the Security of MANET. *Open Information Science*, 8(1). <https://doi.org/10.1515/opis-2024-0001>
- Yogesh Suryawanshi, E. al. (2023). Chinese Remainder Theorem based Performance Analysis of RSA Cryptosystem. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(8), 523–526. <https://doi.org/10.17762/ijritcc.v11i8.9559>