BAB II

LANDASAN TEORI

2.1 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.

Seteah 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.

2.2. 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.

2.3. 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.

2.4. kriftografi

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).

2.5. 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).

Pada penelitian ini, RSA digunakan untuk mengamankan data yang dikirimkan melalui jaringan wireless. Sebelum data ditransmisikan, data terlebih dahulu dienkripsi menggunakan kunci publik sehingga berubah menjadi ciphertext. Setelah diterima oleh penerima yang sah, data didekripsi menggunakan kunci privat sehingga kembali menjadi plaintext. Dengan mekanisme tersebut, data yang berhasil ditangkap oleh intruders tidak dapat dibaca tanpa memiliki kunci privat yang sesuai (Irfan et al., 2024).

Tahapan algoritma RSA meliputi:

1. Pembangkitan pasangan kunci (Key Generation).
2. Proses enkripsi menggunakan kunci publik.
3. Pengiriman data melalui jaringan wireless.
4. Proses dekripsi menggunakan kunci privat.

Keterangan:

1. Tahap pertama adalah pembangkitan pasangan kunci yang terdiri atas kunci publik dan kunci privat. Proses ini diawali dengan memilih dua bilangan prima yang berbeda, yaitu p dan q. Kedua bilangan tersebut kemudian digunakan untuk menghitung nilai modulus n, yang selanjutnya menjadi bagian dari kunci publik maupun kunci privat.

Nilai modulus dihitung menggunakan persamaan berikut.

Penjelasan:

- **p** = bilangan prima pertama.

- **q** = bilangan prima kedua.
- **n** = hasil perkalian kedua bilangan prima yang digunakan sebagai modulus.

Selanjutnya dihitung nilai fungsi Euler menggunakan persamaan berikut.

Nilai $\varphi(n)$digunakan untuk menentukan pasangan kunci publik dan kunci privat. Setelah itu dipilih nilai **e** sebagai kunci publik dengan syarat relatif prima terhadap $\varphi(n)$, kemudian dihitung nilai **d** sebagai kunci privat menggunakan persamaan berikut.

Hasil dari proses ini diperoleh dua buah kunci, yaitu:

- **Public Key** = (e, n)
- **Private Key** = (d, n)

Kunci publik digunakan untuk proses enkripsi, sedangkan kunci privat digunakan untuk proses dekripsi

1. Proses enkripsi (encryption)

   Tahap berikutnya adalah proses enkripsi. Pada tahap ini, data asli (plaintext) diubah menjadi data terenkripsi (ciphertext) menggunakan kunci publik. Tujuan proses ini adalah menjaga kerahasiaan data agar tidak dapat dibaca oleh pihak yang tidak memiliki hak akses.

   Proses enkripsi dilakukan menggunakan persamaan berikut.

   Penjelasan:

   - **C** = Ciphertext (data hasil enkripsi).
   - **M** = Plaintext (data asli).
   - **e** = eksponen publik.

- **n** = modulus.

Hasil dari proses ini adalah data dalam bentuk ciphertext yang siap dikirim melalui jaringan wireless.

2. Pengiriman data(transmission)

   Setelah proses enkripsi selesai, data dalam bentuk ciphertext dikirimkan melalui jaringan wireless menuju perangkat penerima. Pada tahap ini, data berpotensi disadap oleh intruders karena media transmisi wireless bersifat terbuka. Namun demikian, data yang berhasil ditangkap oleh pihak yang tidak berwenang tetap berada dalam bentuk ciphertext, sehingga isi informasi tidak dapat dipahami tanpa memiliki kunci privat yang sesuai.

3. Proses dekripsi(decryption)

   Tahap terakhir adalah proses dekripsi. Pada tahap ini, penerima menggunakan kunci privat untuk mengembalikan ciphertext menjadi plaintext. Dengan demikian, informasi yang dikirimkan dapat dibaca kembali oleh penerima yang memiliki hak akses.

   Persamaan dekripsi RSA dituliskan sebagai berikut.

   Penjelasan:

   - **M** = Plaintext.
   - **C** = Ciphertext.
   - **d** = eksponen privat.
   - **n** = modulus.

Melalui proses dekripsi tersebut, data yang sebelumnya tidak dapat dipahami akan kembali menjadi informasi yang dapat dibaca oleh penerima.