

# Meningkatkan Keamanan Jaringan Wireless-Lan Dengan Penerapan Multi-Ssid Dan Segmentasi Vlan Menggunakan Perangkat Ruijie Wireless Pada PT. XYZ

Akrom<sup>1\*</sup>, Leni Susanti<sup>1</sup>

<sup>1,2</sup>Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia

Email: <sup>1\*</sup>[dosen02613@unpam.ac.id](mailto:dosen02613@unpam.ac.id), <sup>2</sup>[dosen02617@unpam.ac.id](mailto:dosen02617@unpam.ac.id)

(\* : coresponding author)

**Abstrak** – Keamanan jaringan *Wireless Local Area Network* (WLAN) merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data pada lingkungan perusahaan. PT. XYZ masih menerapkan *single Service Set Identifier* (SSID) yang digunakan secara bersamaan oleh karyawan dan tamu, sehingga meningkatkan risiko akses tidak sah, penyebaran *malware*, dan kebocoran data. Penelitian ini bertujuan untuk meningkatkan keamanan jaringan *Wireless-LAN* melalui implementasi *Multi-Service Set Identifier* (Multi-SSID) dan segmentasi *Virtual Local Area Network* (VLAN) menggunakan perangkat Ruijie Wireless. Metode penelitian yang digunakan meliputi analisis kebutuhan jaringan, perancangan topologi, implementasi konfigurasi *Multi-SSID* dan *VLAN*, serta pengujian konektivitas dan keamanan jaringan. Hasil penelitian menunjukkan bahwa implementasi dua SSID yang dipetakan ke VLAN berbeda berhasil memisahkan akses jaringan antara karyawan dan tamu. Perangkat pada SSID Staff dapat mengakses jaringan internal dan internet, sedangkan perangkat pada SSID Guest hanya memperoleh akses internet tanpa dapat mengakses server maupun perangkat internal perusahaan. Implementasi tersebut mampu meningkatkan keamanan jaringan, mempermudah pengelolaan hak akses pengguna, serta mengurangi potensi ancaman keamanan pada jaringan *Wireless-LAN* perusahaan.

**Kata Kunci:** Wireless-LAN; Multi-SSID; VLAN; Ruijie Wireless; Keamanan Jaringan

**Abstract** – *Wireless Local Area Network* (WLAN) security plays an important role in maintaining the confidentiality, integrity, and availability of organizational data. PT. XYZ currently employs a single *Service Set Identifier* (SSID) shared by employees and guests, increasing the risk of unauthorized access, malware propagation, and data leakage. This study aims to improve WLAN security by implementing *Multi-Service Set Identifier* (Multi-SSID) and *Virtual Local Area Network* (VLAN) segmentation using Ruijie Wireless devices. The research method consists of network requirement analysis, network topology design, implementation of *Multi-SSID* and *VLAN* configurations, followed by connectivity and security testing. The implementation results demonstrate that separating employee and guest networks into different VLANs successfully isolates network access according to user roles. Devices connected to the Staff SSID can access internal network resources and the Internet, while devices connected to the Guest SSID are restricted to Internet access only and cannot communicate with internal servers or corporate resources. The proposed implementation enhances WLAN security, simplifies network access management, and reduces potential cyber threats within the enterprise wireless infrastructure. **Keywords:** Wireless LAN; Multi-SSID; VLAN; Ruijie Wireless; Network Security .

**Keywords:** Wireless LAN; Multi-SSID; VLAN; Ruijie Wireless; Network Security .

## 1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong hampir seluruh perusahaan untuk mengandalkan jaringan komputer sebagai infrastruktur utama dalam mendukung aktivitas operasional. Salah satu teknologi yang banyak digunakan adalah *Wireless Local Area Network* (WLAN) karena mampu memberikan fleksibilitas mobilitas pengguna, kemudahan instalasi, serta efisiensi biaya dibandingkan jaringan berbasis kabel. Penggunaan *wireless* memungkinkan perangkat seperti laptop, telepon pintar, dan tablet terhubung ke jaringan perusahaan tanpa dibatasi oleh lokasi fisik. Namun, semakin luas penggunaan *WLAN*, semakin besar pula potensi ancaman terhadap keamanan jaringan, terutama apabila seluruh pengguna menggunakan satu jaringan *wireless* yang sama [1].

PT. XYZ merupakan perusahaan manufaktur multinasional yang memanfaatkan jaringan *Wireless-LAN* sebagai media utama untuk mendukung aktivitas bisnis sehari-hari. Selain digunakan oleh karyawan, jaringan *wireless* perusahaan juga sering dimanfaatkan oleh tamu yang

membutuhkan akses internet selama berada di lingkungan perusahaan. Kondisi tersebut menyebabkan seluruh perangkat, baik milik karyawan maupun tamu, berada pada segmen jaringan yang sama sehingga meningkatkan risiko terjadinya penyebaran *malware*, pencurian data, maupun akses tidak sah terhadap sumber daya jaringan perusahaan. Penggunaan *single Service Set Identifier (SSID)* pada jaringan *wireless* juga menyulitkan administrator dalam melakukan pengendalian akses berdasarkan kategori pengguna [2].

Berbagai penelitian sebelumnya telah membahas peningkatan keamanan jaringan *Wireless-LAN*. Mulyanto et al. (2022) menerapkan metode *penetration testing* untuk menganalisis tingkat kerentanan jaringan *wireless* terhadap serangan *brute force*. Sementara itu, Setiawan (2023) merancang jaringan *Wireless Local Area Network* menggunakan perangkat MikroTik untuk meningkatkan kualitas layanan jaringan. Penelitian lainnya oleh Hermawan dan Rahmatia (2024) mengimplementasikan metode *heatmap* dalam menentukan posisi *access point* sehingga cakupan sinyal menjadi lebih optimal. Meskipun demikian, sebagian besar penelitian tersebut masih berfokus pada analisis keamanan, kualitas sinyal, maupun pengujian jaringan, sedangkan implementasi pemisahan akses antara pengguna internal dan tamu menggunakan kombinasi *Multi-SSID* dan segmentasi *Virtual Local Area Network (VLAN)* pada perangkat Ruijie Wireless masih relatif terbatas [3].

Berdasarkan permasalahan tersebut, penelitian ini menawarkan solusi berupa penerapan *Multi-SSID* yang dipadukan dengan segmentasi *VLAN* pada perangkat Ruijie Wireless. Melalui pendekatan ini, jaringan *wireless* dipisahkan menjadi dua kelompok layanan, yaitu *SSID* khusus karyawan dan *SSID* khusus tamu. Setiap *SSID* dihubungkan dengan *VLAN* yang berbeda sehingga perangkat tamu hanya memperoleh akses internet tanpa dapat mengakses jaringan internal perusahaan. Penerapan segmentasi jaringan ini diharapkan mampu meningkatkan keamanan jaringan, mengurangi risiko penyebaran virus, serta mempermudah pengelolaan hak akses pengguna [4].

Metode penelitian diawali dengan analisis kebutuhan jaringan, identifikasi permasalahan pada infrastruktur *Wireless-LAN*, perancangan topologi jaringan menggunakan *Multi-SSID* dan *VLAN*, implementasi konfigurasi pada perangkat Ruijie Wireless, serta pengujian konektivitas dan keamanan jaringan setelah implementasi dilakukan. Hasil pengujian kemudian dianalisis untuk mengetahui efektivitas penerapan segmentasi jaringan dalam meningkatkan keamanan akses *wireless* [5].

Tujuan penelitian ini adalah mengimplementasikan *Multi-SSID* dan segmentasi *VLAN* pada jaringan *Wireless-LAN* PT. XYZ untuk memisahkan akses jaringan karyawan dan tamu sehingga keamanan jaringan perusahaan dapat ditingkatkan. Hasil penelitian diharapkan dapat menjadi referensi bagi organisasi atau perusahaan yang ingin membangun infrastruktur *Wireless-LAN* yang lebih aman, terstruktur, dan mudah dikelola [6].

## **2. METODE**

### **2.1 Tahapan Penelitian**

Penelitian ini menggunakan metode implementasi (*implementation research*) yang bertujuan untuk meningkatkan keamanan jaringan *Wireless Local Area Network (WLAN)* melalui penerapan *Multi-Service Set Identifier (Multi-SSID)* dan segmentasi *Virtual Local Area Network (VLAN)* menggunakan perangkat Ruijie Wireless pada PT. XYZ. Tahapan penelitian dilakukan secara sistematis mulai dari identifikasi kebutuhan jaringan hingga pengujian hasil implementasi.

Tahapan penelitian yang dilakukan terdiri atas lima langkah utama sebagai berikut [7].

#### **a. Analisis Kebutuhan Jaringan**

Tahap awal dilakukan dengan mengidentifikasi kondisi jaringan *Wireless-LAN* yang sedang digunakan di PT. XYZ. Analisis difokuskan pada penggunaan *single SSID* yang digunakan secara bersamaan oleh karyawan dan tamu sehingga menimbulkan potensi ancaman keamanan jaringan [8].

#### **b. Perancangan Topologi Jaringan**

Berdasarkan hasil analisis kebutuhan, dilakukan perancangan topologi jaringan menggunakan dua *SSID*, yaitu *SSID Staff* dan *SSID Guest*. Masing-masing *SSID* dipetakan ke *VLAN* yang berbeda sehingga setiap kelompok pengguna memperoleh hak akses sesuai kebutuhannya.

#### **c. Implementasi Multi-SSID dan VLAN**

Implementasi dilakukan pada perangkat Ruijie Wireless dengan membuat dua *SSID* yang berbeda. Selanjutnya dilakukan konfigurasi *VLAN*, pengalamatan IP, konfigurasi *routing*, dan pengaturan *gateway* agar jaringan tamu hanya dapat mengakses internet tanpa memperoleh akses ke jaringan internal perusahaan.

#### **d. Pengujian Sistem**

Setelah konfigurasi selesai dilakukan, dilakukan pengujian konektivitas terhadap masing-masing *SSID*, pengujian komunikasi antar-*VLAN*, serta pengujian akses menuju server internal perusahaan.

#### **e. Analisis Hasil**

Tahap terakhir adalah menganalisis hasil implementasi berdasarkan keberhasilan segmentasi jaringan, keamanan akses pengguna, dan kemampuan sistem dalam membatasi akses perangkat tamu terhadap jaringan internal perusahaan. Secara umum tahapan penelitian ditunjukkan pada Gambar 1.



**Gambar 1. Tahapan Penelitian**

### **2.2. Implementasi Multi-SSID dan Segmentasi VLAN**

Implementasi dilakukan menggunakan perangkat Ruijie Wireless Access Point, Ruijie Switch, dan Internet Gateway. Konfigurasi jaringan dirancang dengan memisahkan jaringan berdasarkan kategori pengguna menggunakan teknologi *Multi-SSID* dan *Virtual Local Area Network (VLAN)*.

SSID pertama digunakan sebagai jaringan khusus karyawan (*SSID Staff*) yang dihubungkan dengan VLAN 10, sedangkan SSID kedua digunakan sebagai jaringan tamu (*SSID Guest*) yang dihubungkan dengan VLAN 20 [9]. Dengan pendekatan tersebut, perangkat tamu hanya memperoleh akses menuju internet tanpa dapat mengakses server maupun perangkat milik perusahaan. Konfigurasi perangkat yang digunakan dalam penelitian ditunjukkan pada Tabel 1.

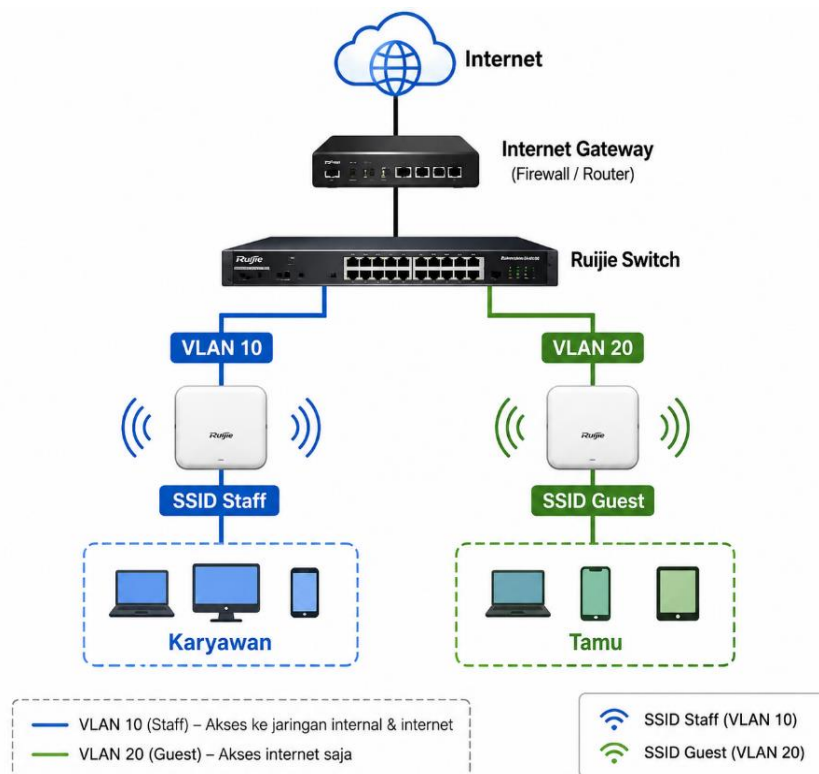
**Tabel 1.** Konfigurasi Segmentasi Jaringan

| SSID  | VLAN ID | Pengguna | Hak Akses                    |
|-------|---------|----------|------------------------------|
| Staff | 10      | Karyawan | Internet dan Server Internal |
| Guest | 20      | Tamu     | Internet saja                |

Pengujian dilakukan untuk memastikan bahwa setiap perangkat memperoleh alamat IP sesuai dengan VLAN masing-masing serta memastikan tidak terdapat komunikasi langsung antara jaringan tamu dan jaringan internal perusahaan [10]. Keberhasilan implementasi diukur berdasarkan beberapa parameter sebagai berikut.

- Perangkat karyawan dapat mengakses seluruh layanan jaringan internal.
- Perangkat tamu hanya dapat mengakses internet.
- Perangkat tamu tidak dapat melakukan *ping* maupun akses ke server internal.
- Segmentasi jaringan berjalan sesuai konfigurasi VLAN.

Arsitektur implementasi jaringan diperlihatkan pada Gambar 2.



**Gambar 2.** Arsitektur Implementasi Multi-SSID dan VLAN

Keberhasilan segmentasi jaringan dapat dianalisis menggunakan persentase keberhasilan pengujian sebagai berikut.

$$\text{Persentase Keberhasilan} = \frac{\text{Jumlah Pengujian Berhasil}}{\text{Jumlah Seluruh Pengujian}} \times 100\% \quad (1)$$

Sedangkan tingkat kegagalan pengujian dihitung menggunakan Persamaan (2).

$$\text{Persentase Kegagalan} = \frac{\text{Jumlah Pengujian Gagal}}{\text{Jumlah Seluruh Pengujian}} \times 100\% \quad (2)$$

Nilai persentase tersebut digunakan untuk mengevaluasi efektivitas penerapan *Multi-SSID* dan segmentasi *VLAN* dalam meningkatkan keamanan jaringan *Wireless-LAN* pada PT. XYZ.

### 3. ANALISA DAN PEMBAHASAN

Bagian ini membahas hasil implementasi *Multi-Service Set Identifier (Multi-SSID)* dan segmentasi *Virtual Local Area Network (VLAN)* pada jaringan *Wireless Local Area Network (WLAN)* PT. XYZ. Implementasi dilakukan menggunakan perangkat Ruijie Wireless dengan tujuan meningkatkan keamanan jaringan melalui pemisahan akses antara pengguna internal (karyawan) dan pengguna eksternal (tamu). Hasil penelitian dianalisis berdasarkan keberhasilan konfigurasi jaringan, segmentasi *VLAN*, serta hasil pengujian konektivitas.

#### 3.1 Implementasi Multi-SSID dan Segmentasi VLAN

Implementasi dilakukan dengan membuat dua buah *Service Set Identifier (SSID)* pada perangkat Ruijie Wireless, yaitu SSID Staff dan SSID Guest. Kedua SSID tersebut dipisahkan menggunakan teknologi *Virtual Local Area Network (VLAN)* sehingga setiap pengguna memperoleh hak akses yang berbeda sesuai kebutuhan perusahaan.

Tahapan implementasi meliputi:

- a. Membuat SSID Staff sebagai jaringan khusus karyawan.
- b. Membuat SSID Guest sebagai jaringan tamu.
- c. Menghubungkan masing-masing SSID dengan VLAN yang berbeda, yaitu:
  1. VLAN 10 digunakan untuk jaringan karyawan.
  2. VLAN 20 digunakan untuk jaringan tamu.

Selanjutnya dilakukan konfigurasi *routing*, *gateway*, serta *IP Address* agar perangkat yang berada pada VLAN berbeda tidak dapat saling berkomunikasi secara langsung. Dengan konfigurasi tersebut, perangkat tamu hanya memperoleh akses menuju internet tanpa dapat mengakses jaringan internal perusahaan. Konfigurasi jaringan yang diterapkan ditunjukkan pada Tabel 2.

**Tabel 2.** Konfigurasi Segmentasi Jaringan

| SSID       | VLAN | Pengguna | Hak Akses                    |
|------------|------|----------|------------------------------|
| SSID Staff | 10   | Karyawan | Internet dan Server Internal |
| SSID Guest | 20   | Tamu     | Internet Saja                |

##### 3.1.1 Hasil Pengujian Sistem

Setelah konfigurasi selesai dilakukan, tahap berikutnya adalah pengujian terhadap seluruh layanan jaringan untuk memastikan bahwa segmentasi jaringan berjalan sesuai dengan rancangan. Pengujian dilakukan terhadap beberapa skenario, antara lain:

- a. Pengujian koneksi perangkat karyawan ke jaringan internal.
- b. Pengujian koneksi perangkat tamu ke internet.
- c. Pengujian komunikasi antar-VLAN.

d. Pengujian akses menuju server perusahaan.

Hasil pengujian menunjukkan bahwa seluruh konfigurasi berhasil diterapkan sesuai dengan rancangan penelitian. Perangkat yang terhubung pada SSID Staff memperoleh alamat IP dari VLAN 10 dan dapat mengakses server maupun internet. Sebaliknya, perangkat pada SSID Guest memperoleh alamat IP dari VLAN 20 dan hanya dapat mengakses internet tanpa dapat melakukan komunikasi dengan perangkat pada jaringan internal. Hasil pengujian ditunjukkan pada Tabel 3.

**Tabel 3.** Hasil Pengujian Implementasi

| Pengujian                  | SSID Staff | SSID Guest | Status   |
|----------------------------|------------|------------|----------|
| Mendapatkan IP Address     | ✓          | ✓          | Berhasil |
| Akses Internet             | ✓          | ✓          | Berhasil |
| Akses Server Internal      | ✓          | ✗          | Berhasil |
| Ping ke Perangkat Internal | ✓          | ✗          | Berhasil |
| Komunikasi Antar VLAN      | ✗          | ✗          | Berhasil |

Berdasarkan hasil pengujian tersebut dapat diketahui bahwa segmentasi jaringan menggunakan *Multi-SSID* dan *VLAN* berhasil meningkatkan keamanan jaringan. Perangkat tamu tidak lagi memiliki akses menuju sumber daya internal perusahaan sehingga risiko penyebaran *malware*, pencurian data, maupun akses tidak sah dapat diminimalkan. Selain meningkatkan keamanan, implementasi ini juga mempermudah administrator jaringan dalam melakukan pengelolaan hak akses pengguna. Setiap kelompok pengguna memiliki jalur komunikasi yang terpisah sehingga proses pemantauan jaringan menjadi lebih mudah dan lebih aman dibandingkan penggunaan *single SSID*. Secara keseluruhan, implementasi *Multi-SSID* dan segmentasi *VLAN* pada perangkat Ruijie Wireless berhasil memenuhi tujuan penelitian, yaitu memisahkan jaringan karyawan dan tamu tanpa mengurangi kualitas layanan internet yang diterima oleh masing-masing pengguna.

## 4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa penerapan Multi-Service Set Identifier (Multi-SSID) dan segmentasi Virtual Local Area Network (VLAN) menggunakan perangkat Ruijie Wireless berhasil meningkatkan keamanan jaringan *Wireless Local Area Network (WLAN)* pada PT. XYZ. Implementasi dua SSID yang dipisahkan ke dalam VLAN berbeda mampu memisahkan akses jaringan antara pengguna internal (karyawan) dan pengguna eksternal (tamu), sehingga perangkat tamu tidak dapat mengakses server maupun sumber daya jaringan internal perusahaan. Hasil pengujian menunjukkan bahwa SSID Staff yang terhubung ke VLAN 10 dapat mengakses jaringan internal dan internet sesuai dengan hak akses yang diberikan, sedangkan SSID Guest yang terhubung ke VLAN 20 hanya memperoleh akses internet tanpa dapat berkomunikasi dengan perangkat pada jaringan internal. Dengan demikian, penerapan segmentasi jaringan berhasil mengurangi potensi penyebaran *malware*, akses tidak sah, serta risiko kebocoran data yang sebelumnya dapat terjadi akibat penggunaan *single SSID*.

Penelitian selanjutnya dapat dikembangkan dengan mengintegrasikan mekanisme keamanan yang lebih komprehensif, seperti Network Access Control (NAC), 802.1X Authentication, RADIUS Server, atau Firewall Policy berbasis VLAN untuk meningkatkan proses autentikasi dan pengendalian akses pengguna. Selain itu, penelitian berikutnya dapat melakukan evaluasi performa jaringan menggunakan parameter Quality of Service (QoS), seperti *throughput*, *delay*, *packet loss*, dan *jitter*, sehingga tidak hanya aspek keamanan yang dianalisis, tetapi juga kualitas layanan jaringan setelah implementasi *Multi-SSID* dan segmentasi *VLAN*.



## REFERENCES

- [1] Sonny Rumlatur, "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong Sonny Rumlatur," *Tek. Elektro*, vol. 19, no. 100, 2014.
- [2] R. Rachman, "ANALISIS KEAMANAN JARINGAN WIRELESS LAN (WLAN) DENGAN METODE PENETRATION TESTING PADA PT.PLN (PERSERO) SEKTOR PENGENDALIAN PEMBANGKITAN PEKANBARU," *Natl. Multidiscip. Sci.*, vol. 1, 2022.
- [3] G. Aryo *et al.*, "Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing di SMK Xyz Tana Toraja," *Anal. Keamanan Jar. Wirel. Menggunakan Metod. Penetration Test. di SMK Xyz Tana Toraja*, vol. 2, no. 2, 2022.
- [4] M. A. Rozan *et al.*, "Implementasi Web Proxy Pada Mikrotik Untuk Mengoptimalkan Keamanan Jaringan Wireless Lan," *J. Pendidik. Teknol. Inf.*, vol. 7, no. 1, 2024.
- [5] M. A. Rozan *et al.*, "IMPLEMENTASI WEB PROXY PADA MIKROTIK UNTUK MENGOPTIMALKAN KEAMANAN JARINGAN WIRELESS LAN DI LINGKUNGAN SEKOLAH MAN 1 GRESIK," *J. Pendidik. Teknol. Inf.*, vol. 7, no. 1, 2024.
- [6] Jamaludin, "Teknik Keamanan Jaringan Wireless LAN Pada Warnet Salsabila Computer Net," *J. Penelit. Tek. Inform.*, vol. 1, 2016.
- [7] A. Maharani, M. Tahir, D. Sangka Buana, S. Muidatul Fauziah, W. Rotama Putra, and M. Akmal Hasan, "PENERAPAN WEB PROXY PADA MIKROTIK UNTUK OPTIMALISASI KEAMANAN JARINGAN WIRELESS LAN DI SMKN 1 BANGKALAN," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 4, 2025.
- [8] M. Noviansyah and H. Saiyar, "PEMANFAATAN WEB PROXY SEBAGAI PENGOPTIMAL KEAMANAN JARINGAN WIRELESS LAN," *J. Khatulistiwa Inform.*, vol. 8, no. 1, 2020.
- [9] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r)," *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 5, no. 2, 2022.
- [10] S. Rumlatur, "ANALISIS KEAMANAN JARINGAN WIRELESS LAN (WLAN) PADA PT. PLN (PERSERO) WILAYAH P2B AREA SORONG," *Electro Luceat*, vol. 1, no. 1, 2015.