Kerangka Evaluasi Keamanan Wi-Fi Pada Institusi Pendidikan Tinggi Xyz Menggunakan Iso 27001

Rut Ramayanti Hutomo[1a)], Roy Rudolf Huizen [1b)], Dandy Pramana Hostiadi [1c)]
[1)] Magister Sistem Informasi, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia
e-mail: [a)]232012020@stikom-bali.ac.id, [b)]Roy@stikom-bali.ac.id, [c)]dandy@stikom-bali.ac.id

Abstrak

Pengelolaan akses Wi-Fi Universitas XYZ masih berisiko karena kredensial berpotensi tersebar luas dan lingkungan kampus yang terbuka memungkinkan sniffing, sehingga diperlukan evaluasi keamanan berbasis ISO 27001 untuk memetakan dan memitigasi risiko secara terstruktur. Penelitian ini bertujuan untuk menganalisis risiko serangan sniffing pada jaringan Wi-Fi, mengukur tingkat keamanan jaringan Wi-Fi terhadap aktivitas sniffing dengan menggunakan pendekatan ISO 27001, serta memberikan rekomendasi langkah-langkah mitigasi yang efektif dalam mengurangi risiko sniffing pada jaringan Wi-Fi. Penelitian ini menggunakan metode kuantitatif pada infrastruktur Wi-Fi yang digunakan di organisasi atau tempat umum. Teknik pengambilan sampel dalam penelitian ini adalah purposive sampling dengan kriteria responden merupakan pengguna Wi-Fi publik yang memiliki pemahaman dasar tentang keamanan jaringan. Penetapan jumlah sampel pada penelitian ini menggunakan formula rumus Slovin menghasilkan 158 responden. Hasil penelitian menunjukkan bahwa meskipun sebagian besar aspek keamanan jaringan Wi-Fi Universitas XYZ berada pada kategori baik, beberapa indikator, khususnya pada manajemen risiko jaringan serta kinerja dan stabilitas teknologi Wi-Fi, masih berada pada kategori cukup sehingga risiko sniffing belum dapat dikategorikan rendah. Pengukuran menggunakan pendekatan ISO 27001 menunjukkan bahwa kemungkinan terjadinya serangan sniffing berada pada tingkat sedang dengan dampak yang berpotensi tinggi, sehingga tingkat risiko secara keseluruhan berada pada kategori sedang hingga tinggi.

Kata kunci: *ISO 27001, Keamanan Wi-Fi, Sniffing.*

1. Pendahuluan

Perkembangan penggunaan jaringan Wi-Fi yang semakin luas memungkinkan masyarakat mengakses internet di berbagai ruang publik, seperti kafe, bandara, pusat perbelanjaan, dan institusi pendidikan [1]. Kemudahan akses ini memberikan manfaat yang besar, tetapi pada saat yang sama menghadirkan risiko keamanan yang tidak dapat diabaikan. Banyak jaringan Wi-Fi publik beroperasi tanpa mekanisme perlindungan yang memadai, sehingga data yang dikirimkan melalui jaringan tersebut berpotensi diakses oleh pihak yang tidak berwenang [2], [3].

Salah satu ancaman keamanan yang paling umum pada jaringan Wi-Fi adalah *sniffing*. Teknik ini digunakan untuk menyadap lalu lintas data yang melintas di jaringan, sehingga penyerang dapat memperoleh informasi sensitif. Data yang berisiko dicuri melalui metode ini mencakup kata sandi, informasi perbankan, hingga identitas pribadi pengguna. Kondisi ini menjadi semakin berbahaya ketika komunikasi data tidak dilindungi oleh enkripsi yang kuat [4].

Perangkat pengguna umumnya secara otomatis mengirimkan permintaan Wi-Fi probe untuk mencari dan terhubung dengan jaringan yang tersedia. Penyerang dapat memanfaatkan pola permintaan ini untuk melacak keberadaan perangkat serta menganalisis aktivitas lalu lintas data [5]. Hasil ini mengindikasikan adanya celah keamanan pada teknologi Wi-Fi yang dapat dimanfaatkan untuk melakukan *sniffing* dan mencuri data pribadi. Risiko tersebut meningkat karena sebagian pengguna belum memiliki kesadaran yang memadai mengenai pentingnya perlindungan data saat mengakses Wi-Fi publik [5].

Lalu lintas Wi-Fi yang tidak terenkripsi sering kali menyertakan informasi tambahan, seperti kekuatan sinyal atau *Received Signal Strength Indicator* (RSSI). Informasi ini dapat dimanfaatkan untuk mengidentifikasi keberadaan perangkat dalam jaringan publik [1]. Dalam kondisi tertentu, teknik *sniffing* memungkinkan pelacakan lokasi pengguna serta pengumpulan data strategis yang berpotensi digunakan dalam serangan lanjutan. Keterbatasan lapisan keamanan pada jaringan Wi-Fi membuat penyerang relatif mudah menyusup dan membaca informasi yang dikirimkan tanpa izin [6], [7].

Dalam konteks mitigasi risiko, standar ISO 27001 dapat dijadikan kerangka kerja sistem manajemen keamanan informasi yang komprehensif untuk mengelola ancaman *sniffing* pada infrastruktur Wi-Fi [8]. Standar ini menyediakan panduan sistematis dalam mengidentifikasi, menilai, dan

mengendalikan risiko keamanan informasi, termasuk risiko yang timbul dari penyadapan lalu lintas jaringan. Penerapan pendekatan berbasis ISO 27001 memungkinkan organisasi mengenali kelemahan pada sistem jaringan yang digunakan dan merancang langkah mitigasi yang lebih terstruktur untuk meningkatkan perlindungan data [9], [10].

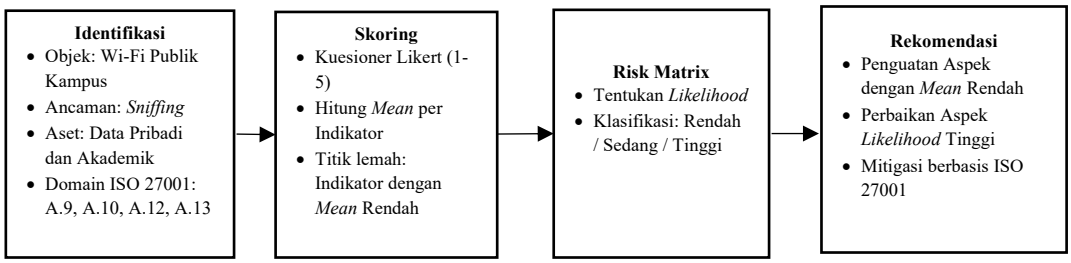
Universitas XYZ sangat bergantung pada jaringan Wi-Fi untuk mendukung aktivitas akademik dan administrasi, seperti akses LMS, sistem informasi akademik, email institusi, repositori digital, hingga layanan konferensi daring. Tingginya mobilitas pengguna oleh mahasiswa, dosen, dan tenaga kependidikan membuat jaringan Wi-Fi kampus digunakan secara masif di berbagai area, namun tidak selalu diikuti dengan standar keamanan perangkat yang seragam. Kondisi ini terlihat dari kebiasaan sebagian pengguna yang belum memperbarui sistem operasi secara berkala, kurang menerapkan perlindungan perangkat, serta melakukan aktivitas sensitif melalui Wi-Fi kampus tanpa memperhatikan keamanan koneksi.

Pengelolaan kontrol akses jaringan di Universitas XYZ masih menghadapi tantangan, seperti kemungkinan kredensial Wi-Fi yang dibagikan secara luas sehingga identitas pengguna sulit ditelusuri ketika muncul aktivitas mencurigakan. Lingkungan kampus yang terbuka juga meningkatkan potensi penyusup berada dalam jaringan yang sama dan memanfaatkan celah keamanan untuk melakukan sniffing terhadap lalu lintas data. Oleh karena itu, diperlukan evaluasi keamanan Wi-Fi yang tidak hanya menilai aspek teknis, tetapi juga mencakup kebijakan, pengelolaan akses, kontrol keamanan, dan perilaku pengguna melalui kerangka ISO 27001 agar risiko sniffing dapat dipetakan dan dimitigasi secara terstruktur.

Penelitian mengenai keamanan Wi-Fi pada umumnya menitikberatkan perhatian pada aspek teknis serangan *sniffing*, seperti pencurian paket data, kelemahan mekanisme autentikasi, dan eksploitasi protokol nirkabel [1], [4], [11]–[14]. Fokus tersebut menghasilkan pemahaman teknis yang kuat, tetapi belum banyak penelitian yang membahas ancaman *sniffing* melalui pendekatan manajemen keamanan informasi secara menyeluruh. Kebaruan penelitian ini muncul dari upaya mengintegrasikan analisis *sniffing* dengan kerangka kerja ISO 27001, sehingga evaluasi keamanan tidak hanya menilai aspek teknis jaringan, tetapi juga mencakup proses identifikasi aset, analisis ancaman, evaluasi kerentanan, serta pengukuran tingkat risiko berdasarkan standar internasional. Kebaruan lain terletak pada pengembangan instrumen kuesioner multi-domain yang disusun berdasarkan standar ISO 27001. Instrumen ini tidak hanya menilai aspek teknis, tetapi juga mencakup kebijakan keamanan dan perilaku pengguna dalam memanfaatkan jaringan. Pendekatan ini memungkinkan pemetaan risiko *sniffing* yang lebih komprehensif dan seimbang, dibandingkan penelitian sejenis yang umumnya hanya berfokus pada satu aspek tertentu.

Berdasarkan latar belakang permasalahan yang telah diuraikan, Penelitian ini bertujuan untuk menganalisis risiko serangan *sniffing* pada jaringan Wi-Fi, mengukur tingkat keamanan jaringan Wi-Fi terhadap aktivitas *sniffing* dengan menggunakan pendekatan ISO 27001, serta memberikan rekomendasi langkah-langkah mitigasi yang efektif dalam mengurangi risiko *sniffing* pada jaringan Wi-Fi. Hasil penelitian diharapkan dapat meningkatkan kesadaran mengenai pentingnya keamanan jaringan Wi-Fi, sekaligus memberikan rekomendasi praktis bagi organisasi dalam merancang dan menerapkan langkah mitigasi risiko yang lebih efektif.

2. Metode Penelitian



Gambar 1. *Flow Diagram* Analisis Risiko Wi-Fi

Penelitian ini menggunakan metode kuantitatif [15] pada infrastruktur Wi-Fi yang digunakan di organisasi atau tempat umum. Dataset untuk analisis risiko Wi-Fi terhadap ancaman *sniffing* diambil dari beberapa domain ISO 27001 dan Indeks Keamanan Informasi (KAMI) [13], [14] yang dapat dilihat pada tabel sebagai berikut.

Tabel 1. Domain ISO 27001 dan KAMI untuk Dataset Analisis Risiko Wi-Fi

Aspek	Domain ISO/IEC 27001	Domain Indeks KAMI
Perlindungan komunikasi Wi-Fi	A.13 – *Communications Security*	Teknologi dan Keamanan
Kontrol akses jaringan Wi-Fi	A.9 – *Access Control*	Kerangka Kerja Pengamanan
Enkripsi data	A.10 – *Cryptography*	Teknologi dan Keamanan
Logging dan monitoring jaringan	A.12 – *Operations Security*	Kerangka Kerja Pengamanan
Penilaian risiko *sniffing*	(terintegrasi di semua domain)	Manajemen Risiko Keamanan Informasi

Penelitian ini menyatakan tingkat keamanan risiko menggunakan Skala *Likelihood* untuk mengukur tingkat kemungkinan (probabilitas) suatu risiko/kejadian terjadi. Dalam konteks penelitian risiko sniffing pada Wi-Fi publik, skala *likelihood* dipakai untuk menilai peluang risiko sniffing terjadi serta membantu menentukan level risiko saat dikombinasikan dengan skala dampak (*impact*). Skala Likelihood untuk penelitian ini dapat dilihat sebagai berikut.

Tabel 2. Skala *Likelihood*

Rentang *Mean*	Kategori	Definisi *Likelihood*
4,21 – 5,00	Sangat Rendah (*Rare*)	Hampir tidak mungkin terjadi karena kontrol keamanan konsisten dan jaringan stabil
3,41 – 4,20	Rendah (*Unlikely*)	Jarang terjadi; ada celah kecil tetapi kontrol utama masih efektif
2,61 – 3,40	Sedang (*Possible*)	Mungkin terjadi pada kondisi tertentu
1,81 – 2,60	Tinggi (*Likely*)	Sering terjadi karena kontrol teknis/manajerial tidak konsisten dan jaringan sering tidak stabil
1,00 – 1,80	Sangat Tinggi (*Almost Certain*)	Hampir pasti terjadi; Wi-Fi sangat rentan dan kontrol keamanan tidak memadai

Populasi pada penelitian ini adalah pihak pengguna IT yaitu seluruh mahasiswa Universitas XYZ pada tahun 2024 berjumlah 260 orang. Teknik pengambilan sampel dalam penelitian ini adalah *purposive sampling* [15] dengan kriteria responden merupakan pengguna Wi-Fi publik yang memiliki pemahaman dasar tentang keamanan jaringan. Pemilihan *purposive sampling* dilakukan untuk memastikan responden mampu memahami butir pernyataan terkait risiko *sniffing* dan praktik keamanan jaringan, sehingga data yang diperoleh lebih relevan dengan tujuan penelitian. Penetapan jumlah sampel pada penelitian ini menggunakan formula rumus Slovin. Jumlah sampel ditetapkan dengan mengacu pada rumus Slovin sebagai acuan kebutuhan minimal responden, bukan sebagai dasar penarikan sampel secara acak. Jumlah sampel yang dihasilkan digunakan sebagai target minimal agar data yang terkumpul mencukupi untuk dianalisis. Perhitungan Rumus Slovin sebagai berikut [15].

$$n = \frac{260}{1+260\,(0{,}05)^2} \quad (1)$$

Berdasarkan hasil perhitungan rumus Slovin, jumlah sampel adalah 157,6. Peneliti membulatkan ke atas jumlah sampel yang diteliti, sehingga jumlah sampel dalam untuk pihak pengguna IT adalah 158 responden.

Teknik pengumpulan data menggunakan kuesioner yang disebar kepada responden yang memenuhi kriteria yang telah ditetapkan. Kuesioner dalam penelitian ini menggunakan kuesioner tipe skala Likert. Teknik analisis data menggunakan piranti lunak SPSS untuk pengujian validitas dan reliabilitas serta pengujian teknik analisis deskriptif.

3. Hasil dan Pembahasan

3.1 Uji Validitas, Reliabilitas, dan Normalitas

Tabel 3. Uji Validitas Penelitian

Nomor Pernyataan	Nilai Pearson	Status	Nomor Pernyataan	Nilai Pearson	Status
1	0,796	Valid	17	0,777	Valid
2	0,813	Valid	18	0,795	Valid
3	0,795	Valid	19	0,802	Valid
4	0,792	Valid	20	0,855	Valid
5	0,849	Valid	21	0,809	Valid

Nomor Pernyataan	Nilai Pearson	Status	Nomor Pernyataan	Nilai Pearson	Status
6	0,809	Valid	22	0,836	Valid
7	0,795	Valid	23	0,868	Valid
8	0,854	Valid	24	0,825	Valid
9	0,833	Valid	25	0,865	Valid
10	0,812	Valid	26	0,851	Valid
11	0,838	Valid	27	0,800	Valid
12	0,823	Valid	28	0,839	Valid
13	0,428	Valid	29	0,861	Valid
14	0,432	Valid	30	0,851	Valid
15	0,819	Valid	31	0,823	Valid
16	0,410	Valid	32	0,850	Valid

Hasil uji validitas menunjukkan bahwa seluruh butir pernyataan kuesioner yang digunakan dalam penelitian ini dinyatakan valid, dengan nilai korelasi Pearson berada pada rentang 0,410 hingga 0,868 dan seluruhnya melampaui nilai r-tabel (0,300) yang dipersyaratkan sehingga instrumen penelitian dinilai layak dan dapat digunakan untuk analisis lebih lanjut dalam menilai risiko *sniffing* pada jaringan Wi-Fi kampus.

Tabel 4. Uji Reliabilitas Penelitian

Reliability Statistics	
Cronbach's Alpha	N of Items
.760	32

Hasil uji reliabilitas menunjukkan bahwa instrumen penelitian memiliki nilai Cronbach's Alpha sebesar 0,760 dengan jumlah item sebanyak 32 pernyataan. Nilai ini berada di atas batas minimum reliabilitas yang umum digunakan, yaitu 0,70, sehingga menunjukkan bahwa instrumen memiliki tingkat konsistensi internal yang baik.

Tabel 5. Uji Normalitas Penelitian

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Keamanan Wi-Fi	.070	158	.050	.988	158	.163

a. Lilliefors Significance Correction

Uji normalitas dilakukan untuk sebagai langkah verifikasi untuk memastikan distribusi data tidak menyimpang secara ekstrem sehingga interpretasi nilai rata-rata lebih stabil. Hasil uji normalitas menunjukkan bahwa data variabel Keamanan Wi-Fi memenuhi asumsi distribusi normal. Berdasarkan uji Kolmogorov–Smirnov, diperoleh nilai signifikansi sebesar 0,050, yang berada pada batas penerimaan normalitas. Sementara itu, uji Shapiro–Wilk menunjukkan nilai signifikansi sebesar 0,163, yang lebih besar dari 0,05. Temuan ini mengindikasikan bahwa data residual terdistribusi secara normal, sehingga asumsi normalitas terpenuhi dan data layak digunakan untuk analisis statistik lanjutan.

3.2 Analisis Statistik Deskriptif

Tabel 6. Analisis Statistik Deskriptif

Nomor Peryataan	Mean	Std. Deviation	Status Likelihood	Nomor Peryataan	Mean	Std. Deviation	Status Likelihood
Ruang Lingkup Sistem Wi-Fi				**Access Control (Hak Akses & Prosedur Login)**			
1	3.5309	1.19092	Rendah	17	3.7346	1.15179	Rendah
2	3.5988	1.08324	Rendah	18	3.6358	1.06179	Rendah
3	3.5123	1.11588	Rendah	19	3.4815	1.11579	Rendah
4	3.5432	1.09827	Rendah	20	3.5741	1.06208	Rendah
Distribusi Password Access Point				**Pengelolaan Risiko & Konten Berbahaya**			
5	3.7901	1.06574	Rendah	21	3.7222	1.18610	Rendah
6	3.5802	1.13514	Rendah	22	3.6420	1.08986	Rendah
7	3.5988	1.13914	Rendah	23	3.5247	1.15399	Rendah
8	3.6111	1.13252	Rendah	24	3.5062	1.09911	Rendah
Manajemen Risiko Jaringan				**Perlindungan Data Pribadi**			
9	3.5123	1.10469	Rendah	25	3.5926	1.18246	Rendah

Nomor Peryataan	Mean	Std. Deviation	Status Likelihood	Nomor Peryataan	Mean	Std. Deviation	Status Likelihood
10	3.3827	1.19593	Sedang	26	3.6667	1.10335	Rendah
11	3.6111	1.06468	Rendah	27	3.6358	1.17297	Rendah
12	3.5123	1.08769	Rendah	28	3.5309	1.08732	Rendah
Teknologi Wi-Fi (Kinerja, Overload, Stabilitas)				**Communications Security**			
13	3.0432	1.12757	Sedang	29	3.5000	1.12703	Rendah
14	3.0432	1.13306	Sedang	30	3.6852	1.06013	Rendah
15	3.4444	1.14208	Rendah	31	3.6358	1.07920	Rendah
16	3.0123	1.15284	Sedang	32	3.5679	1.07413	Rendah

3.2.1 Identifikasi Potensi Risiko *Sniffing* pada Jaringan Wi-Fi

Berdasarkan hasil identifikasi, potensi risiko *sniffing* pada jaringan Wi-Fi Universitas XYZ paling menonjol terdapat pada komponen teknologi Wi-Fi dan manajemen risiko jaringan yang ditunjukkan oleh nilai *mean* kategori sedang. Kondisi ini mengindikasikan bahwa meskipun secara umum infrastruktur Wi-Fi berada pada kategori rendah, masih terdapat titik-titik rentan yang dapat dimanfaatkan untuk melakukan *sniffing*.

3.2.2 Analisis Risiko Serangan *Sniffing* pada Jaringan Wi-Fi

Berdasarkan hasil identifikasi risiko, meskipun seluruh butir pernyataan kuesioner secara umum berada pada kategori rendah, terdapat empat butir pernyataan yang berada pada kategori sedang, yaitu satu pernyataan pada aspek manajemen risiko jaringan dan tiga pernyataan pada aspek teknologi Wi-Fi yang mencakup stabilitas, kinerja saat beban tinggi, dan kecepatan pada jam ramai.

Dari sisi kemungkinan *(likelihood*), keberadaan indikator pada kategori sedang mengindikasikan bahwa peluang terjadinya serangan sniffing tidak berada pada tingkat rendah. Ketika jaringan mengalami perlambatan, gangguan, atau kepadatan akses, mekanisme pengamanan seperti monitoring lalu lintas dan kontrol teknis berpotensi tidak berfungsi secara maksimal. Selain itu, respons manajemen risiko yang tidak selalu cepat dapat menyebabkan aktivitas mencurigakan, termasuk *sniffing*, tidak segera terdeteksi. Oleh karena itu, kemungkinan terjadinya serangan *sniffing* pada kondisi tersebut dapat dikategorikan pada tingkat sedang.

Analsisi risiko memperlihatkan bahwa tingkat risiko serangan *sniffing* pada jaringan Wi-Fi Universitas XYZ dapat dievaluasi berada pada kategori risiko sedang. Meskipun sebagian besar kontrol keamanan telah diterapkan dengan baik, keberadaan beberapa indikator pada kategori sedang menunjukkan adanya titik lemah yang tidak dapat diabaikan.

3.2.3 Rekomendasi Mitigasi Risiko *Sniffing* Berbasis ISO 27001

Penguatan keamanan komunikasi jaringan Wi-Fi perlu ditempatkan sebagai langkah prioritas dalam upaya menekan risiko *sniffing*. Organisasi dapat menerapkan mekanisme enkripsi yang lebih kuat, seperti WPA3 atau setidaknya WPA2-*Enterprise*, pada seluruh *access point* yang digunakan.

Peningkatan kontrol akses jaringan juga menjadi komponen penting dalam mitigasi risiko *sniffing*. Pengelola jaringan perlu memastikan bahwa setiap pengguna Wi-Fi memiliki kredensial akses yang bersifat individual dan tidak digunakan secara bersama. Autentikasi berbasis akun resmi institusi, disertai pembatasan hak akses sesuai peran pengguna, dapat memperkuat pengamanan jaringan.

Pengelolaan *password* dan kredensial *access point* perlu dilakukan secara lebih sistematis untuk mencegah kebocoran akses jaringan. Penyimpanan kredensial jaringan juga perlu dilengkapi dengan mekanisme perlindungan yang memadai. Langkah-langkah ini berperan penting dalam mengurangi risiko penyalahgunaan akses yang dapat dimanfaatkan untuk aktivitas *sniffing*.

Jaringan yang sering mengalami gangguan atau *overload* cenderung lebih rentan terhadap eksploitasi keamanan. Peningkatan kualitas infrastruktur akan membantu menjaga konsistensi pengamanan dan mencegah munculnya celah keamanan akibat penurunan performa jaringan.

4. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa risiko serangan *sniffing* pada jaringan Wi-Fi Universitas XYZ masih berada pada tingkat yang perlu mendapat perhatian. Meskipun sebagian besar risiko keamanan jaringan Wi-Fi berada pada kategori rendah, beberapa indikator, khususnya pada aspek manajemen risiko jaringan serta teknologi Wi-Fi yang meliputi kinerja, beban jaringan, dan stabilitas, masih berada pada kategori sedang.

Pengukuran tingkat keamanan jaringan Wi-Fi dengan menggunakan pendekatan ISO 27001 menunjukkan bahwa kontrol keamanan secara umum telah diterapkan, terutama pada aspek kontrol akses, perlindungan data pribadi, dan keamanan komunikasi. Namun, penerapan kontrol tersebut belum sepenuhnya konsisten di seluruh komponen jaringan. Hasil evaluasi menunjukkan bahwa kemungkinan terjadinya serangan *sniffing* berada pada tingkat sedang, sehingga tingkat risiko secara keseluruhan berada pada kategori sedang.

Penelitian ini menghasilkan rekomendasi langkah-langkah mitigasi yang difokuskan pada penguatan enkripsi komunikasi, peningkatan kontrol akses jaringan, pengelolaan kredensial yang lebih terstruktur, peningkatan stabilitas dan kinerja jaringan, serta peningkatan kesadaran keamanan pengguna.

Penelitian ini memiliki keterbatasan. Evaluasi risiko s*niffing* pada jaringan Wi-Fi Universitas XYZ dilakukan melalui pendekatan kuesioner, sehingga hasil yang diperoleh lebih merepresentasikan persepsi dan tingkat pemahaman responden dibandingkan bukti teknis langsung dari kondisi jaringan. Oleh karena itu, penelitian selanjutnya disarankan untuk mengombinasikan pendekatan ISO 27001 berbasis kuesioner dengan pengujian teknis langsung agar hasil evaluasi keamanan Wi-Fi lebih komprehensif dan akurat.

Daftar Pustaka

[1] R. N. Pietraru, Ş. Andrei, M. Nicolae, and D. M. Merezeanu, "A WiFi Sniffing Solution for Safe Return to Classes," in *2021 12th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, 2021, pp. 1–5. doi: 10.1109/ATEE52255.2021.9425125.

[2] F. Angellia *et al.*, *Internet of Things: Membangun Dunia yang Terkoneksi*. PT. Sonpedia Publishing Indonesia, 2024.

[3] B. Baharuddin and M. W. S. Adam, *Network Security*. CV Eureka Media Aksara, 2025.

[4] L. Song, A. Striegel, and A. Mohammed, "Sniffing only control packets: a lightweight client-side WiFi traffic characterization solution," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6536–6548, 2020.

[5] M. Uras, R. Cossu, E. Ferrara, O. Bagdasar, A. Liotta, and L. Atzori, "Wifi probes sniffing: an artificial intelligence based approach for mac addresses de-randomization," in *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2020, pp. 1–6.

[6] N. Pimple, T. Salunke, U. Pawar, and J. Sangoi, "Wireless security—an approach towards secured wi-fi connectivity," in *2020 6th international conference on advanced computing and communication systems (ICACCS)*, 2020, pp. 872–876.

[7] M. I. Syed, A. Fladenmuller, and M. D. de Amorim, "Unity is strength: Improving Wi-Fi passive measurements through sniffer redundancy," *Ad Hoc Networks*, vol. 151, p. 103287, 2023.

[8] C. Carvalho and E. Marques, "Adapting ISO 27001 to a public institution," in *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 2019, pp. 1–6.

[9] V. Monev, "Organisational information security maturity assessment based on ISO 27001 and ISO 27002," in *2020 International Conference on Information Technologies (InfoTech)*, 2020, pp. 1–5.

[10] I. M. Lopes, T. Guarda, and P. Oliveira, "Implementation of ISO 27001 standards as GDPR compliance facilitator," *J. Inf. Syst. Eng. Manag.*, vol. 4, no. 2, pp. 1–8, 2019.

[11] M. Gregorczyk, P. Żórawski, P. Nowakowski, K. Cabaj, and W. Mazurczyk, "Sniffing detection based on network traffic probing and machine learning," *IEEE Access*, vol. 8, pp. 149255–149269, 2020.

[12] G. Yera and X. Liu, "An anti-sniffing protocol for location-based services in wireless networks," in *2020 International Conference on Computing, Networking and Communications (ICNC)*, 2020, pp. 251–255.

[13] P. Bheevgade, C. Saha, R. Nath, S. Dabhade, H. Barot, and S. O. Junare, "The Rise of Public Wi-Fi and Threats," in *International Conference on Information Security, Privacy and Digital Forensics*, 2022, pp. 175–189.

[14] A. Bartoli, E. Medvet, A. De Lorenzo, and F. Tarlao, "(in) secure configuration practices of wpa2 enterprise supplicants," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–6.

[15] P. D. Sugiyono, "Metode Penelitian Kuantitatif, Kualitatif, R&d," *Bandung Alf.*, vol. 67, 2021.