JURNAL INFORMATIKA DAN TEKNOLOGI KOMPUTER
Halaman Jurnal: https://journal.amikveteran.ac.id/index.php/jitek
Halaman UTAMA Jurnal : https://journal.amikveteran.ac.id/index.php

SYSTEMATIC LITERATURE REVIEW (SLR): PENYALAHGUNAAN *WIFI* PUBLIK TERHADAP ORANG AWAM YANG ADA DI INDONESIA

Eddy Ryansyah [a], Agung Susilo Yuda Irawan [b]
[a] Informatika, eddyryansyah1612@gmail.com, Universitas Singaperbangsa Karawang
[b] Informatika, agung@unsika.ac.id, Universitas Singaperbangsa Karawang

ABSTRACT

The use of the internet on computer network devices in the current technological era certainly very easy for us in daily life to work and other activities in cyberspace. There are so many places to eat or other public places that use computer network devices, namely wifi so that visitors feel at home or feel happy because they have the facilities that are needed by them, namely the internet. However, it is undeniable that there are public wifi devices that have a negative impact because they are free. One solution to prevent internet network users from using negatively charged public wifi can be done by understanding what steps must be taken before and after accessing public wifi. Therefore, the purpose of this study is to provide understanding and learning to ordinary people in Indonesia to minimize or rather eradicate the use of the internet network on public wifi which has a negative impact in public spaces. In realizing the above, the author uses the method of taking 30 journal papers that have been published through Google Scholar with a range of years between 2018 and 2022 to be researched and analyzed using the SLR (Systematic Literature Review) method. SLR is a systematic method used to review a topic in the form of a journal paper to provide opinions on solving problems. Based on this research, it was found that public wifi in computer network learning can improve the problem-solving ability of ordinary users. Based on the literature review conducted, the level of understanding of ordinary people in Indonesia can be developed by learning computer networks on social media and in articles on the internet.

***Keywords**: SLR, hacker, wifi, network, indonesia.*

ABSTRAK

Penggunaan internet pada perangkat jaringan komputer di era teknologi saat ini tentunya sangat memudahkan kita dalam kehidupan sehari-hari untuk bekerja maupun kegiatan beraktivitas lainnya yang ada di dunia maya. Banyak sekali tempat makan saji ataupun tempat publik lainnya yang memakai perangkat jaringan komputer yaitu *wifi* agar para pengunjung betah atau merasa senang karena memiliki fasilitas yang sangat dibutuhkan olehnya yaitu internet. Namun, tidak bisa dipungkiri bahwa terdapat perangkat *wifi* publik yang memiliki dampak bermuatan negatif karena bersifat gratis. Salah satu solusi untuk mencegah pengguna jaringan internet memakai *wifi* publik yang bermuatan negatif tersebut dapat dilakukan dengan cara memahami apa saja langkah yang harus dilakukan sebelum dan sesudah mengakses *wifi* publik tersebut. Oleh karena itu, tujuan dalam penelitian ini adalah untuk memberikan pemahaman dan pembelajaran terhadap orang awam yang ada di Indonesia guna meminimalisir atau lebih tepatnya memberantas penggunaan jaringan internet pada *wifi* publik yang memiliki dampak bermuatan negatif di ruang publik. Dalam mewujudkan hal di atas, penulis menggunakan metode pengambilan 30 *paper* jurnal yang telah diterbitkan melalui *google scholar* dengan rentang tahun antara 2018 sampai tahun 2022 untuk diteliti dan dianalisis dengan menggunakan metode SLR (*Systematic Literature Review*). SLR merupakan metode sistematis yang dipakai untuk mengulas suatu topik berupa *paper* jurnal guna memberikan pendapat dalam penyelesaian masalah. Berdasarkan penelitian ini didapatkan bahwa *wifi* publik dalam pembelajaran jaringan komputer dapat meningkatkan kemampuan pemecahan masalah pengguna awam. Berdasarkan kajian literatur yang dilakukan, tingkat pemahaman orang awam di Indonesia dapat dikembangkan dalam pembelajaran jaringan komputer di media sosial maupun di artikel pada internet.

Kata Kunci: SLR, *hacker*, *wifi*, jaringan, indonesia.

Received September 5, 2022; Revised September 29, 2022; Accepted Oktober 29, 2022

1. PENDAHULUAN

Pada zaman sekarang perkembangan dan kemajuan teknologi sudah berkembang sangat pesat. Keamanan dalam sebuah jaringan sangat krusial dan wajib selalu diperhatikan, jaringan yang sudah terhubung dalam internet tentu sangat perlu diperhatikan lantaran rentan terjadinya pencurian data oleh *hacker*, baik itu dalam jaringan LAN (*Local Area Network)* atau dalam jaringan *wireless* maupun pada perangkatnya yaitu *wifi*. Jaringan LAN berbentuk nirkabel atau jaringan *wifi* adalah jaringan area lokal yang menggunakan sinyal elektromagnetik dengan frekuensi 2,4 GHz sebagai media transmisi untuk menggantikan kabel tembaga di LAN. Teknologi *wifi* memungkinkan data seperti data video dan berupa teks dikirim melalui jaringan internet. Pada waktu data dikirim melewati beberapa terminal untuk hingga ketujuan, dapat dikatakan hal ini akan menaruh kesempatan dalam pengguna lain yang tidak bertanggung jawab untuk mengganti atau menyadap data kita, bahkan hingga mencuri data sebelumnya untuk kepentingan pribadi *hacker*. Dalam perancangan pemasangan perangkat, sistem keamanan jaringan yang terhubung ke internet wajib dipersiapkan dengan cara yang sangat matang dan dimengerti oleh admin supaya bisa menjaga data-data krusial yang berada dalam jaringan tersebut secara efektif dan dapat meminimalisir terjadinya agresi dari para *hacker* ataupun *cracker* [1].

Penggunaan teknologi berbasis *wifi* di ruang publik sudah menjadi hal yang lumrah belakangan ini. Saat ini, internet digunakan untuk semua aktivitas seperti pembelian, penjualan, dan pemasaran produk. Kecepatan internet yang baik perlu didukung oleh peralatan yang hebat sehingga tidak mengganggu pekerjaan Anda. Tentunya salah satu tempat umum untuk mengakses internet adalah dengan menggunakan layanan *wifi* [2]. Beberapa lokasi yang terdapat relatif rawan sanggup terkena *sniffing*, misalnya pada lokasi untuk belajar seperti gedung sekolah, lokasi untuk berlibur seperti di mal dimana *cracker* ataupun *hacker* bisa mencuri data email dan password berdasarkan para pengguna lain yang berada pada satu lingkup jaringan yang sama dengan *hacker*.

Pada penelitian ini, akan dilakukan pengkajian literatur terhadap jurnal terkait mengenai penyalahgunaan *wifi* publik terhadap orang awam yang ada di Indonesia. Hasil penelitian tersebut kemudian akan dianalisis untuk mengetahui hasil penelitian dari jurnal terkait dari pencegahan penyalahgunaan pada suatu jaringan *wifi* publik. Dan juga yang tidak kalah penting yaitu untuk meningkatkan kesadaran dan pemahaman dari para pengguna jaringan *wifi* akan pentingnya kesadaran dalam menggunakan dan memanfaatkan jaringan internet di ruang publik.

2. TINJAUAN PUSTAKA

2.1. *Systematic Literature Review* (SLR)

Systematic Literature Review (SLR) merupakan salah satu jenis metode penelitian pustaka. Berdasarkan dari tujuannya, SLR menekankan pada tahap pencarian. Tahap pencarian bersifat eksplisit dan langkah-langkah yang dilakukan dijelaskan secara rinci sehingga dapat direplikasi oleh penulis yang lain. SLR adalah upaya untuk membuat tinjauan pustaka yang seringkali subjektif menjadi lebih objektif untuk mengurangi bias penulis [3].

2.2. Jaringan Komputer

Jaringan komputer merupakan kumpulan komputer yang saling berhubungan guna dapat berbagi informasi dan memungkinkan perangkat untuk berkomunikasi. Manfaat dalam menggunakan jaringan komputer untuk aktivitas apapun yaitu seperti pesan langsung, video, berkomunikasi melalui email, fitur berbagi perangkat seperti *printer*, mesin fotokopi, berbagi *file*, pemindai, dan berbagi perangkat lunak pada sistem jarak jauh [4].

2.3. Internet

Interconnected Network atau yang biasa disebut dengan internet merupakan sebuah sistem teknologi informasi yang dapat menghubungkan suatu perangkat di seluruh dunia dengan membentuk suatu ruang lingkup jaringan yang sangat luas. Jaringan internet mempunyai berbagai ragam informasi dalam bentuk gambar, audio, teks, video, dan lainnya yang dapat diakses melalui *World Wide Web* (WWW). Pengguna bisa mengakses internet dengan cara mengirimkan data memakai standar protokol internet atau yang biasa disebut sebagai IP. Internet bisa dikenal sebagai media yang digunakan untuk mengefektifkan proses komunikasi dalam skala global dengan aplikasi seperti email, VoIP, *website*, dan lain sebagainya [5].

2.4. *Wi-Fi*

Wifi merupakan nama lain yang diberikan pada *Wireless Local Area Network* (WLAN) yaitu jaringan komputer yang memakai gelombang sinyal radio sebagai media transmisi pertukaran data. *Wireless Fidelity* atau yang biasa kita sebut *wifi* merupakan salah satu standar *wireless networking* nirkabel dimana hanya dengan komponen yang memadai bisa terkoneksi pada jaringan [6]. *Wifi* memakai standar komunikasi IEEE 802.11b yang hanya dapat mencapai jangkauan ruang lingkup tidak lebih dari sekitar ratusan meter. 802.11 yaitu standar IEEE untuk W-LAN di dalam ruangan.

2.5. *Hacker*

Hacker atau yang bisa disebut dengan peretas adalah seorang ahli di bidang komputer, pemrograman, dan jaringan yang dapat menembus suatu keamanan sistem maupun jaringan. Saat melakukan tindakan, peretas menyerang kerentanan yang ada di suatu sistem. Setiap tindakannya selalu merugikan pihak tertentu apabila saat beraksi dan kegiatannya sudah pasti terlibat dalam kegiatan yang melanggar hukum (kriminal) [7].

2.6. *Sniffing*

Sniffing merupakan metode serangan yang memantau atau memegang kendali semua paket yang dikirim melalui media komunikasi berbentuk kabel ataupun *wireless*. *Sniffing* adalah teknik untuk memantau setiap paket yang mengarah ke jaringan lalu perangkat lunak atau perangkat keras yang memantau semua lalu lintas yang mengarah ke jaringan [8].

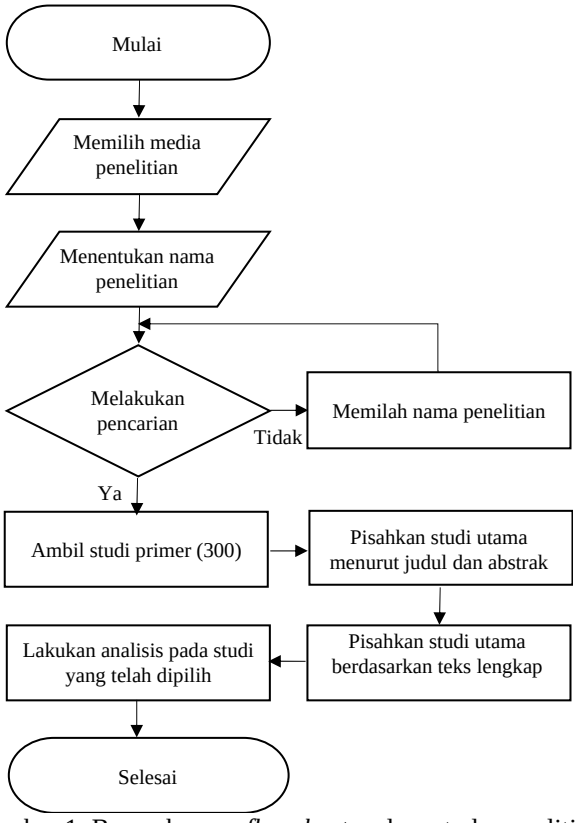
3. METODOLOGI PENELITIAN

Untuk pembuatan *paper* jurnal ini, penulis memilih memakai cara SLR. SLR sendiri memiliki pengertian sebagai berikut sebuah teknik untuk mengklasifikasikan, memilah, dan mengartikan semua penelitian yang berkaitan dengan parameter pengukuran yang mempunyai hubungan juga [9]. Sedangkan menurut sumber selanjutnya SLR memiliki definisi yaitu suatu teknik pengelompokan data yang saling mempunyai keterikatan menjadi gabungan dalam suatu bentuk jurnal [10]. SLR mempunyai tujuan yaitu cara mengulas penelitian yang sudah ada sebelumnya yang sejenis dan menjadikannya berupa satu kesatuan [11].

Selanjutnya setelah mengetahui berbagai pendapat orang-orang mengenai SLR, hal yang penulis lakukan yaitu mengumpulkan sebanyak 30 judul *paper* jurnal yang mempunyai kemiripan dengan tema yang penulis ambil yaitu penyalahgunaan *wifi* publik terhadap orang awam yang ada di Indonesia. Caranya dengan mengabadikan semuanya yang didapatkan dari *google cendekia* atau *google scholar*, yang kemudian penulis baca dan analisis yang selanjutnya dijadikan menjadi satu *paper* jurnal yang utuh dan memuat isi yang sama. Untuk lebih jelasnya perihal mengenai kriteria atau kendala untuk menentukan apakah data tersedia untuk penelitian, berikut kriteria yang cocok dalam penelitian ini:

1) Data yang akan digunakan adalah data yang tersedia untuk periode 2018-2022.
2) Data yang tersedia dari *https://scholar.google.co.id/* dengan menggunakan tambahan *software* aplikasi PoP (Publish or Perish).
3) Data yang digunakan hanya data yang berhubungan dengan penyalahgunaan *wifi* publik terhadap orang awam yang ada di Indonesia.

Berikut rincian bagan berupa *flowchart* yang digunakan pada tahapan penelitian *paper* jurnal ini:



Gambar 1. Bagan berupa *flowchart* pada metode penelitian

4. HASIL DAN PEMBAHASAN

4.1. Hasil

Pada *literature review* yang dilaksanakan pada bulan November 2022, pencarian pertama dilakukan berdasarkan tahun terbit, dengan menggunakan kata kunci pada tema jurnal ini yaitu "Penyalahgunaan *Wifi* Publik Terhadap Orang Awam yang Ada di Indonesia" pada periode waktu 2018-2022. Hasil pencarian *Publish or Perish* (PoP) menyertakan 300 artikel dari *Google Scholar*, setelah itu artikel tersebut diseleksi. Literatur yang digunakan hanya artikel jurnal, proses pemilihan studi penelitian juga dilakukan dengan melihat judul, abstrak, dan teks tambahan, sehingga menghasilkan hasil kajian utama yang akan digunakan untuk analisis lebih lanjut.

Setelah memperoleh 300 artikel, pekerjaan penting yang dipilih sendiri untuk meningkatkan hasil pencarian. Berikut rinciannya:

Tabel 1. Penyaringan data pada artikel

No.	Penyaringan Pencarian	Jumlah Artikel
1	Tidak benar	204
2	Judul dan abstrak salah	47
3	Judul dan abstrak sudah sesuai tetapi diisinya tidak benar	19
4	Artikel unggulan	30
	Total	**300**

Dari tabel di atas terlihat ada 204 artikel yang tidak valid, artinya *paper* jurnal yang dibuat oleh penulis, bukan artikel jurnal yang diajukan karena tidak valid. Jurnal dan abstrak yang tidak sama dengan tema penelitian atau topik penelitian, maksimal 47 artikel. Terdapat 19 artikel yang judul dan abstraknya sesuai dengan topik penelitian, namun teks lengkapnya tidak pernah dibahas, sehingga dipilih 30 artikel untuk dianalisis lebih lanjut. Selanjutnya informasi yang didapat akan dibagikan ke dalam berbagai jenis jurnal.

Tabel 2. Hasil penelitian terhadap penyalahgunaan *wifi* publik terhadap orang awam di indonesia[12]-[41]

No.	Peneliti	Hasil Penelitian
1	(Amarudin & Ulum, 2018)	Dalam penelitian ini menggunakan simulator GNS3 untuk mendesain dan mensimulasikan topologi keamanan jaringan. Berdasarkan penelitian yang telah dilakukan bahwasanya simulator GNS3 dapat dengan mudah ditentukan dalam mendesain topologi jaringan maupun dalam mensimulasikan pengujian keamanan jaringan khususnya pada metode keamanan *Port Knocking*. Berdasarkan penelitian yang telah dilakukan juga didapatkan hasil bahwasanya metode *Port Knocking* dapat diterapkan untuk mengakses Router dari akses orang lain yang tidak berhak mengaksesnya [12].
2	(Sajati et al., 2022)	Menurut temuan penelitian, keamanan jaringan dapat diimplementasikan dalam serangan DDOS menggunakan perangkat lunak LOIC dan Model Proses Forensik. Analisis data juga dapat dimanfaatkan sebagai bahan pelaporan bagi pihak berwenang dan sebagai salah satu bukti adanya penyerangan (bila diperlukan). Analisis dapat dilakukan dengan menggunakan hasil serangan, khususnya berapa kali itu terjadi, jenis serangan, dan jumlah total paket [13].
3	(Fauzi & Suartana, 2018)	Berdasarkan hasil pengujian pada saat user menggunakan protokol HTTP untuk melakukan aktivitas internet maka didapat tidak adanya gangguan dalam jaringan *access point*. Dalam mendeteksi serangan paket *sniffing* diindikasi *arp spoof* menggunakan *snort*, agar dapat memonitoring serangan paket *sniffing* secara otomatis *snort* akan memberikan *alert* berupa (*Attempted ARP cache overwrite attack*). RM dapat diistilahkan sebagai teknologi pemrograman yang menjadi jembatan untuk menghubungkan sistem *database* SQL dengan konsep pemrograman berorientasi objek, sehingga meningkatkan keamanan terhadap peretasan yang dapat dilakukan oleh orang-orang yang tidak bertanggung jawab [14].
4	(Riska et al., 2018)	Berdasarkan hasil implementasi sistem keamanan jaringan komputer dengan metode *port knocking* untuk mengurangi serangan pada server, *port knocking* dapat menentukan *port* yang dapat diakses dan tidak dapat diakses oleh *client*. Apabila *port* tidak mendapat akses *client*, maka tidak dapat melakukan *sharing file* atau berkomunikasi dengan server [15].
5	(Lukman & Bachtiar, 2018)	Berdasarkan hasil analisa pada IT Telkom Purwokerto dapat disimpulkan perlunya menyediakan alat *backup* listrik yang memadai ketika terjadi pemadaman listrik seperti menggunakan *Uninterruptible Power Supply* (UPS). Kecepatan *bandwidth* yang kurang maksimal dikarenakan banyak pengguna yang memakai secara bersamaan. Perlunya sistem proteksi dalam penggunaan internet dengan menambahkan *Demiliterized Zone* (DMZ) [16].
6	(Raharjo & Ekawati, 2022)	Secara kualitas kinerja server (*performance*), Teknologi *Synology* NAS memiliki *performance* yang jauh lebih cepat dibandingkan Teknologi Server Fisik karena dapat menjalankan akses *file* yang kompleks dan besar. Berdasarkan hasil kesimpulan di atas, maka Teknologi *Synology* NAS dapat dijadikan sebagai sistem alternatif dan direkomendasikan untuk menggantikan Teknologi Server Fisik *File* Server Tradisional, karena dapat meningkatkan *performance* aplikasi, dengan tanpa mengesampingkan aspek kehandalan [17].
7	(Diara, 2020)	Berdasarkan analisis kuantitatif penulis terhadap dokumen strategi keamanan siber Korea Selatan, konteks strategi keamanan siber Korea Selatan meliputi aspek keamanan siber nasional, kesadaran keamanan siber, ancaman dunia maya, aturan internasional, undang-undang, dan regulasi nasional, krisis siber nasional, kejahatan siber, infrastruktur siber dan terbuka. Pendekatan Korea Selatan terhadap keamanan siber menciptakan kesenjangan mendasar dalam privasi individu saat mengakses dunia maya

		[18].
8	(Fadilah et al., 2021)	Dari penjelasan pada pembahasan penelitian ini dapat disimpulkan bahwa pengertian anggaran itu sendiri, terutama perbandingan-perbandingan yang menganggap kesetaraan (sistem anggaran yang sangat beragam, ternyata masih memiliki persamaan) [19].
9	(Rachman & Susan, 2021)	Komponen tersebut meliputi (1) Kesadaran radikal; (2) Konstruksi bahasa sebagai alat pengaruh dan informasi; dan (3) Aksi sosial dengan batas teritorial yang lebih sedikit. Konstruksi bahasa, misalnya di jaringan mahasiswa Papua dan beberapa ormas di Surabaya yang terkait dengan rasisme dan nasionalisme, menjadi alat untuk menggalang dukungan, dukungan, membangun solidaritas, bertukar formasi dan membenarkan kekerasan [20].
10	(Usman, 2021)	Pesatnya perkembangan teknologi informasi dan komunikasi mendorong terjadinya globalisasi. Mengingat sifat global dari kemajuan teknologi ini muncullah kemajuan dan kecanggihan berbagai kejahatan [21].
11	(Putranti et al., 2020)	Seringkali, suatu ancaman tidak dikenali sampai muncul di jaringan dan oleh karena itu dapat diabaikan dalam situasi ancaman yang dianggap sebagai bagian dari penilaian risiko. Mengelola jaringan tangguh menggunakan kerangka kerja ini mengakui dan menekankan interaksi antara setiap area organisasi pada setiap tahap siklus manajemen peristiwa. Sebuah elemen yang metodologi pendekatan lain untuk ketahanan diabaikan. Kedua, ketahanan jaringan tergantung pada efektivitas semua aspek organisasi sepanjang siklus manajemen acara di empat bidang (SDM, infrastruktur, wawasan, dan regulasi) telah ditentukan [22].
12	(Luthfah, 2021)	Hal ini terlihat pada *cyber* yang digunakan sebagai senjata untuk menyerang negara lain melalui sistem teknologi yang dampaknya dapat merugikan perekonomian, budaya, keuangan, masyarakat, bahkan pertumbuhan demografi dari negara tersebut. Oleh karena itu, perlu dilakukan persiapan terhadap perkembangan ancaman jenis ini agar segera diintegrasikan ke dalam konsep kebijakan dan regulasi keamanan nasional. Tantangan ini perlu diatasi oleh Indonesia dengan membentuk konsep bersama yang mengintegrasikan berbagai jenis ancaman [23].
13	(Herdiana et al., 2021)	Analisis peristiwa seperti pengumuman dan laporan media menunjukkan korelasi yang lemah antara pengumuman dan kampanye serangan siber terkait yang menggunakan peristiwa ini sebagai pengait untuk meningkatkan peluang keberhasilan asosiasi. Pandemi Covid-19 dan meningkatnya tingkat serangan siber yang ditimbulkannya memiliki implikasi yang lebih luas di luar tujuan-tujan ini. Juga, pengangguran meningkat yang berarti semakin banyak orang yang duduk di rumah secara *online*, dan mungkin beberapa di antaranya mengeksploitasi penjahat dunia maya untuk menghidupi diri mereka sendiri. Studi ini menunjukkan apa yang dapat digambarkan sebagai pandangan depan dan belakang yang pengecut antara peristiwa dan serangan siber [24].
14	(Putri et al., 2022)	Ancaman siber dewasa ini merupakan salah satu ancaman serius yang dapat berkisar dari tingkat individu hingga tingkat nasional. Ada beberapa jenis metode serangan dunia maya, seperti spionase dunia maya, sabotase, sabotase, dan serangan jaringan listrik. Ada dua jenis modus operandi yang digunakan oleh peretas untuk melakukan kejahatan dunia maya, yaitu peretasan fisik dan peretasan logis. Secara logika, *hacking* adalah modus yang paling sering digunakan oleh para *hacker*. Mode ini mencakup pengintaian, analisis, akses, pemeliharaan akses, dan cakupan pelacakan. Pemerintah Indonesia secara khusus mengkhawatirkan jumlah yang berpotensi buruk dari *spyware predator* ini. Mengingat insiden dengan dua politisi Mesir, ada kemungkinan pejabat Indonesia juga menjadi sasaran pemasangan *spyware predator* ini. Potensi buruk yang dapat terjadi jika

		terdapat *predatory spyware* pada ponsel pejabat Indonesia adalah penjualan data yang telah diambil oleh *hacker* kepada pihak ketiga, yang tentunya membahayakan keamanan nasional [25].
15	(Vimy et al., 2022)	Kompleksitas ancaman yang terus berkombinasi dan bersinergi terutama terkait ancaman serangan siber, tentunya mengharuskan Indonesia menguatkan pertahanan dalam bentuk pembuatan kebijakan dan undang-undang, sinergitas *stakeholder* terkait, serta menambah orang orang ahli yang kompeten di bidang siber, dan juga upaya pengenalan melalui seminar kepada masyarakat umum dan pengenalan pada anak-anak sekolah untuk menambah kesadaran akan pentingnya hal ini yang kemudian berimplikasi pada meningkatnya ketertarikan publik akan ancaman siber dan kemungkinan *Cyber War*. Upaya Gap-gap yang muncul tentu harus ditutupi dengan membuat kelembagaan analisis dan juga memberikan saran masukan terkait objek vital negara. Dan dengan upaya yang maksimal diharapkan dalam jangka panjang, Indonesia menjadi negara yang aman dari ancaman siber, memiliki sistem pertahanan siber yang kuat dan memiliki banyak ahli yang kompeten di sektor pertahanan siber [26].
16	(Munawar & Putri, 2020)	Keamanan jaringan komputer adalah masalah yang harus diperhatikan oleh setiap pengguna komputer. Perlu diperhatikan dalam melakukan pembersihan tautan ilegal, situs-situs *phising*, *spam*, dan semacamnya dalam komputer. Jangan pernah memberikan kesempatan kepada pelaku kejahatan karena hal itu merupakan kelalaian yang dapat berdampak serius terhadap keamanan komputer. Masih ada jalan panjang yang harus ditempuh untuk perkembangan teknologi keamanan jaringan komputer di masa depan. Berbagai terobosan teknis harus direalisasikan sesegera mungkin, dan langkah-langkah perlindungan keamanan perlu ditingkatkan [27].
17	(Laksono & Nasution, 2020)	Hasil implementasi dari praktik simulasi pada penelitian tersebut dapat disimpulkan bahwa *Access Control List* (ACL) pada jaringan *Virtual Local Area Network* (VLAN) di Perusahaan X berhasil diterapkan. Dibuktikan dengan melakukan *testing* terhadap *client*, hak akses 'deny' pada saat mengakses *service* FTP dari server Perusahaan X dengan tujuan keamanan data [28].
18	(Ilham & Candra, 2018)	Berdasarkan hasil penelitian, perangkat *Raspberry* Pi dapat melakukan proses pemblokiran iklan pada web dan sistem pada menu *blacklist* yaitu untuk memblokir semua iklan melalui *link website* yang disalin ke dalam *blacklist*, dan *whislist* melindungi iklan pada *website* untuk tidak diblokir [29].
19	(Saskara et al., 2019)	Dari pengujian didapatkan jaringan nirkabel yang menggunakan *Captive Portal* dan RADIUS Server dapat menangkal *Man In The Middle Attack* dan *Eavesdropping*, namun tidak dapat menghalau *Denial of Service*, *Authentication Attack* Tunggal dan Mac *Address Spoofing*. Sedangkan dengan ditambahkannya lapisan autentikasi dengan enkripsi seperti WPA atau WPA2 segala jenis serangan *Penetration Test* dapat digagalkan [30].
20	(Dar & Harahap, 2018)	Dari hasil pengujian didapat bahwa *Snort*-IDS ssangat reaktif dalam menyikapi paket-paket yang terdeteksi sebagai gangguan. *Snort*-IDS juga mampu mendeteksi penyerangan-penyerang yang dikategorikan sebagai *Denial of Service* (DoS) seperti *PingFlood*, *Syn Attack*, TCP dan UDP *Attack*. Namun, secara *default*, *Snort* memiliki keterbatasan dari segi *rules* yang ada, maka tidak cukup hanya dengan menerapkan *Intrusion Detection System* (IDS). Perlu juga dilengkapi dan diterapkan dengan *Intrusion Prevention System* (IPS) [31].
21	(Bakti et al., 2018)	Hasil menyatakan bahwa penerapan pengendalian dan keamanan pengguna internet dapat diterapkan pada MA Ishlalu Ikhwan Wathan Mispalah Praya, ketika *user* mengetikkan URL *address* maka situs-situs terlarang akan

		difilter oleh *proxy* server. Dengan adanya pembagian *bandwitdth* dapat dilakukan berdasarkan IP dari masing-masing *Access Point* dan *interface* yang terhubung ke mikrotik, sehingga mendapatkan *bandwidth* untuk target *upload* 256k dan target *download* 256k dengan kestabilan dan kecepatan transfer data yang cenderung sama [32].
22	(Dewi et al., 2020)	*Website* pemerintah di negara bagian Sumatera Utara antara lain SQL *Injection*, *Blind* SQL *Injection* dan lain-lain mengandung banyak kerentanan keamanan. Dari hasil penelitian yang telah dilakukan maka dapat disimpulkan bahwa metode *protocol* PPTP yang diterapkan pada Kantor Desa Kertaraharja penerapan metode *tunneling* tersebut jaringan komputer antara kantor dapat salaing terhubung dan berkomunikasi, akibatnya pekerjaan dan pertukaran informasi berjalan semakin fleksibel dan semakin cepat [33].
23	(Sanjaya & Setiyadi, 2019)	Dari hasil rancangan jaringan komputer menggunakan metode *Network Development Life Cycle* (NDLC) dapat disimpulkan Rumah Shalom Mahanaim telah menjadi lebih baik. Banyak konfigurasi dan penerapan dari beberapa tahapan yang dilalui agar jaringan yang digunakan lebih optimal dapat menggunakan pengaturan *management bandwidth*, penerapan *firewall filter* dan *limit up time* untuk membatasi waktu pengguna internet untuk anak-anak, konfigurasi L7 *Protocol*, penerapan VLAN, penggunaan autentikasi *login* jaringan dan *monitoring* [34].
24	(Putra et al., 2018)	Hal tersebut dapat menjadi solusi untuk menghemat penggunaan sumber daya berupa kertas, tenaga dan waktu dalam proses penghitungan suara pada pemilu digital atau sering disebut dengan *electronic voting*. Hasil penelitian didapat dengan adanya keamanan jaringan komputer menggunakan VPN dengan metode PPTP dapat mempermudah pekerjaan teknisi IT untuk mengontrol dan mengatasi permasalahan-permasalahan jaringan yang ada di perusahaan dari jarak jauh, tanpa mengharuskan untuk datang langsung ke tempat [35].
25	(Sumardi & Zaen, 2018)	Berdasarkan pemabahasan dan hasil uji coba yang telah diuraikan, rancangan jaringan komputer *Local Area Network* (LAN) dan *Wireless Fidelity* (WiFi) area berbasis mikrotik *router* dapat diimplementasikan pada SMAN 4 Praya. Pada sisi *administrator*, sistem *login* pada mikrotik *hotspot* dapat mempermudah dalam hal pemeliharaan dan *monitoring* [36].
26	(Ardianto et al., 2018)	Setelah melakukan penelitian dan perancangan jaringan *hotspot* berbasis mikrotik menggunakan metode autentikasi pengguna (*user*) maka didapat kesimpulan (1) Konfigurasi jaringan *hotspot* berbasis mikrotik RB750 ini menggunakan topologi *star*; (2) Sistem keamanan yang digunakan pada jaringan *wireless* telah diatur dari server mikrotik melalui konfigurasi IP *hotspot* menggunakan *software* Winbox V.3.0; dan (3) Jaringan ini menggunakan konfigurasi *rate limits* pada *user profile hotspot* sebagai manajemen *bandwidth* pada setiap *user* dengan tujuan agar pengguna jaringan dapat berjalan dengan lancar dan stabil sesuai dengan kebutuhan pengguna [37].
27	(Tantoni et al., 2020)	Berdasarkan penelitian tersebut dapat disimpulkan dengan diterapkannya Inter-VLAN *routing* dapat berjalan pada RB260GS sebagai *switch manageable* dan RB1100AHX4 sebagai *router*. Sekaligus dapat menjadi solusi untuk meningkatkan performa jaringan dan Inter-VLAN dapat memecah *broadcast* [38].
28	(Mulyanto & Prakoso, 2020)	Dari hasil proses perencanaan dan implementasi perancangan jaringan komputer bahwa akses jaringan di Inspektorat Kabupaten Sumbawa telah merata di setiap ruangan karena telah dipasang *access point* dengan perangkat pendukung jaringan selain dari modern *wireless* yang berfungsi untuk memaksimalkan layanan. Dan telah tersedia perangkat omada *controller* yang berfungsi untuk memonitoring perangkat keras jaringan dan

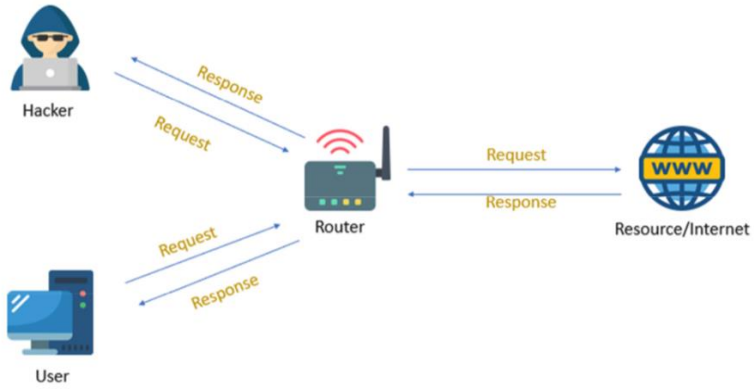
		mengatur lalu lintas serta akses data pada jaringan tersebut [39].
29	(Sabdho & Maria, 2018)	Hasil analisis keamanan jaringan *wireless* dengan metode *penetration testing* pada sebuah institusi memberikan gambaran kelemahan jaringan pada PT Mora Telematika Indonesia yang harus diperhatikan kembali karena memiliki banyak celah untuk dieksploitasi, dan banyak kesempatan bagi siapapun untuk menyerang keamanan jaringan wireless tersebut [40].
30	(Gustiawan et al., 2021)	Hasil yang diperoleh antara lain adalah pelaksanaan desain topologi jaringan *hotspot* menggunakan Mikrotik RouterOS yang dapat memaksimalkan *bandwidth* dan meningkatkan kinerja jaringan *hotspot*. Temuan penelitian ini adalah *administrator* jaringan *hotspot* dengan Mikrotik RouterOS dapat membatasi *bandwidth* pengguna berdasarkan paket *voucher* yang telah dibuat dan tidak membuat *bandwidth* menarik antar pengguna karena distribusi *bandwidth* yang sama [41].

Dari 30 jurnal tersebut, metode yang paling umum digunakan adalah metode kuantitatif, yang sesuai dengan apa yang saat ini dibutuhkan dalam jurnal SLR ini. Karena penelitian kuantitatif memberikan rekomendasi yang lengkap dan terperinci, langkah-langkah yang spesifik, literatur yang lengkap, dan hipotesis yang dirumuskan dengan jelas.

Metode kuantitatif memiliki keunggulan dalam hal efisiensi. Analisis kuantitatif bekerja dengan menggunakan contoh-contoh untuk memecahkan masalah yang dihadapi. Selain *sampling*, untuk beberapa hal, metode kuantitatif memberikan gambaran yang lebih akurat tentang fakta-fakta yang ada. Setiap tahun terdapat jurnal pada setiap *website* yang membahas tentang analisis keamanan sistem pada *wifi*, bahkan pada tahun 2022 ini terdapat beberapa jurnal dengan pendekatan kuantitatif yang sebagian besar membahas mengenai perlakuan mengenai keamanan data pada sistem *wifi*.

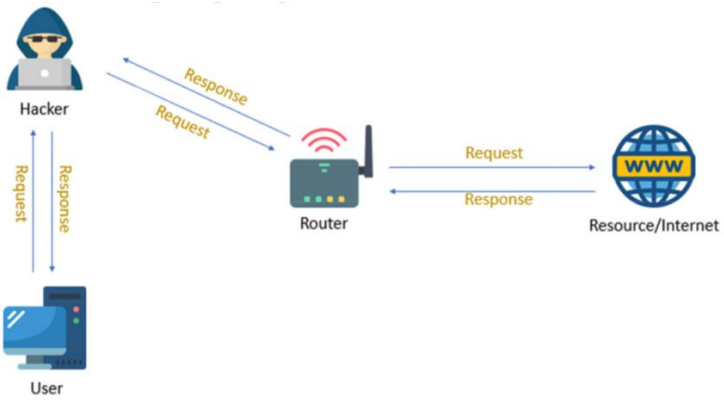
4.2. Pembahasan

Berdasarkan hasil kajian literatur di atas dapat kita lihat bahwa penyalahgunaan *wifi* publik sering terjadi pada lokasi yang sering kita singgahi untuk berlibur yaitu di daerah sekitar kafe pada mal. Hal tersebut dikarenakan tempat yang strategis untuk bersantai para pengunjung dan sebagai orang awam yang ada di Indonesia kita harus sadar dengan adanya para *hacker* atau peretas kita harus berhati-hati dalam memakai jaringan internet yang ada di ruang publik. Berikut suatu gambaran topologi atau kronologi terjadinya sebuah peretasan data oleh *hacker* dengan cara menggunakan teknik *sniffing*:



Gambar 2. Topologi sebelum diretas menggunakan teknik *sniffing*[1]

Pada Gambar 2 yakni merupakan gambaran topologi atau kronologi yang umumnya dipakai seluruh pengguna yang dimana para *user* akan langsung terhubung dengan perangkat *router*, tetapi apabila ketika jaringan tersebut disadap oleh *hacker* maka gambaran topologi atau kronologi nya akan berubah menjadi pada Gambar 3 berikut ini:



Gambar 3. Topologi setelah diretas menggunakan teknik *sniffing*[1]

Seperti Gambar 3 inilah yang terjadi apabila koneksi jaringan internet sudah diretas oleh seorang *hacker*. Dengan teknik *sniffing*, *hacker* berhasil masuk dan menempatkan dirinya di antara *user* dan perangkat *router* yang berarti setiap pengguna melakukan *request* maka datanya akan nampak oleh peretas apa yang diminta dan begitu pun pada perangkat *router* yang bekerja menerima *request* dari pengguna dan melakukan *response* pada permintaan pengguna yang dimana *response* tersebut pun akan terlihat oleh *hacker* yang posisinya sudah berada di antara *user* dan perangkat *router*, dengan begitu *hacker* bisa melihat keseluruhan aktivitas *user* saat menggunakan internet dan juga dapat mencuri data *user* dengan cara merekam data yang terlintas olehnya.

Maka diperlukan adanya pencegahan sebelum terjadinya hal di atas benar-benar terjadi dengan cara: Selalu berhati-hati dalam berselancar di dunia internet pada *wifi* publik terutama yang bersifat gratis, jangan memasukkan email dan *password* sembarangan apabila *wifi* publik tersebut meminta agar dapat berhasil mengakses koneksi jaringan internet dari *wifi* publik tersebut, dan hindari penggunaan akses *wifi* publik bersifat gratis yang tidak kita kenal siapa yang punya. Meningkatkan pengetahuan terkait penyalahgunaan *wifi* publik pada orang awam melalui internet juga dapat mencegah hal terjadinya peretasan pada *hacker* karena sudah mengetahui motif atau apapun yang akan dilakukan olehnya. Lalu, bagaimana cara mengatasi apabila kita sebagai pengguna sedang terkena peretasan pada teknik *sniffing* tersebut seperti yang telah digambarkan pada gambar 3 di atas. Yang dapat dilakukan untuk mengatasi hal tersebut yaitu salah satunya dengan cara mematikan koneksi internet pada *wifi* publik yang terhubung lalu setelah itu lupakan jaringan tersebut agar perangkat tidak dapat terhubung ke jaringan itu lagi secara otomatis.

5. KESIMPULAN DAN SARAN

Berdasarkan analisa yang penulis lakukan terhadap 30 judul *paper* jurnal menggunakan teknik pengumpulan dan penelitian SLR, diperoleh fakta bahwa tinjauan pustaka sistematis adalah proses yang dapat mengidentifikasi, mengevaluasi, dan menafsirkan semua bukti dalam penelitian untuk menjawab pertanyaan penelitian tertentu. Sebanyak 300 artikel kemudian dipilih dan hasil studi utama dipilih hingga 30 *paper* jurnal dengan kriteria inklusi dan eksklusi yang sesuai. Hasil akhir yang dicapai adalah beberapa hal yang mendorong peneliti untuk mengangkat topik atau topik tersebut, terbukti dengan adanya inkonsistensi hasil penelitian sebelumnya dan perbedaan temuan penelitian.

Penulis menyadari bahwa masih terdapat kekurangan dari penjelasan materi di atas. Oleh karena itu, beberapa saran yang diberikan untuk pengembangan materi pembelajaran ini yaitu: Materi pembelajaran ini masih bersifat teori dasar, jadi masih dapat dikembangkan lagi baik dari materi, contoh gambar/tabel maupun studi kasus yang diberikan. Materi pembelajaran ini dapat lebih menarik jika dikembangkan dengan cara menampilkan suatu implementasi pada contoh studi kasus langkah yang diambil.

Ucapan Terima Kasih

Penulis mengucapkan terimakasih kepada Bapak Agung Susilo Yuda Irawan, M.Kom. selaku Dosen Program Studi Informatika, Universitas Singaperbangsa Karawang yang sekaligus dosen pembimbing dalam penyusunan SLR ini karena telah memberi masukan dan saran yang membangun, serta mengarahkan sehingga penyusunan *paper* jurnal ini dapat terselesaikan. Serta pihak lain yaitu tim penulis hendak

menyampaikan banyak terimakasih atas keikutsertaan dan kerjasamanya dalam menuntaskan *paper* jurnal ini secara maksimal.

DAFTAR PUSTAKA

[1] Y. Hae, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 2095–2105, 2021, doi: 10.35957/jatisi.v8i4.1196.

[2] R. Sahara, S. Abdullah, and R. Saputra, "Analisis Ancaman Sniffing pada Jaringan WiFi di PT. Stepa Wirausaha Adiguna," *Pros. Semin. Nas. Ris. Dan Inf. Sci.*, vol. 4, pp. 224–230, 2022.

[3] D. Priharsari, "Systematic Literature Review di Bidang Sistem Informasi dan Ilmu Komputer," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 2, pp. 263–268, 2022, doi: 10.25126/jtiik.202293884.

[4] I. Y. Windra, "Simulasi Perancangan Infrastruktur Jaringan Komputer Pada Institut Teknologi Keling Kumang Menggunakan Pendekatan Network Development Life Cycle (NDLC)," *TAWAK:Jurnal Hunatech*, vol. 1, no. 2, pp. 37–52, 2022, [Online]. Available: https://ejournaltawak.itkk.ac.id/index.php/hunatech/article/view/24

[5] R. I. Ramadhan and M. Ladjamuddin, "Perancangan Sistem Web Filtering Dengan Metode Dns Forwarding Pada Jaringan Komputer Berbasis Mikrotik Routeros," *J. JITEK*, vol. 2, no. 2, pp. 146–157, 2022.

[6] A. R. Mustofa, "Pengaruh Fasilitas Free Wi-fi Terhadap Keputusan Pembelian di Angkringan Daeng," *J. Sahmiyya*, vol. 1, pp. 107–112, 2022, [Online]. Available: https://e-journal.iainpekalongan.ac.id/index.php/sahmiyya/article/download/5416/2395

[7] F. R. Irfandi, U. Yunan, K. Septo, and A. Almaarif, "Software Security Hardening Pada Virtual Private Server Berdasarkan NIST SP 800-123 di Universitas XYZ," vol. 4, no. 1, pp. 94–102, 2022, doi: 10.47065/josh.v4i1.2299.

[8] F. Fatimah, T. Mary, and A. Y. Pernanda, "Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat," *JURTEII J. Teknol. Inf.*, vol. 1, no. 2, pp. 7–11, 2022, doi: 10.22202/jurteii.2022.5707.

[9] E. Triandini, S. Jayanatha, A. Indrawan, G. Werla Putra, and B. Iswara, "Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan Sistem Informasi di Indonesia," *Indones. J. Inf. Syst.*, vol. 1, no. 2, p. 63, 2019, doi: 10.24002/ijis.v1i2.1916.

[10] D. Fitriani and A. Putra, "Systematic Literature Review (SLR): Eksplorasi Etnomatematika pada Makanan Tradisional," *J. Math. Educ. Learn.*, vol. 2, no. 1, p. 18, 2022, doi: 10.19184/jomeal.v2i1.29093.

[11] A. Apriliani, M. Budhiluhoer, A. Jamaludin, and K. Prihandani, "Systematic Literature Review Kepuasan Pelanggan terhadap Jasa Transportasi Online," *Systematics*, vol. 2, no. 1, p. 12, 2020, doi: 10.35706/sys.v2i1.3530.

[12] A. Amarudin and F. Ulum, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.

[13] H. Sajati, S. Sudaryanto, R. Iman, and S. Nugroho, "Pengaruh Routing Protocol Switch Multilayer untuk Transfer Data Pada Jaringan Komputer," *J. Nas. Teknol. Komput.*, vol. 2, no. 2, pp. 81–91, 2022.

[14] A. Rizal Fauzi and I. Made Suartana, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids," *J. Manaj. Inform.*, vol. 8, no. 2, p. 7, 2018.

[15] P. Riska, P. Sugiartawan, and I. Wiratama, "Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking," *J. Sist. Inf. dan Komput. Terap. Indones.*, vol. 1, no. 2, pp. 53–64, 2018, doi: 10.33173/jsikti.12.

[16] A. M. Lukman and Y. Bachtiar, "Analisis Sistem Pengelolaan, Pemeliharaan dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto," *Evolusi J. Sains dan Manaj.*, vol. 6, no. 2, pp. 49–56, 2018, doi: 10.31294/evolusi.v6i2.4427.

[17] S. Raharjo and F. Ekawati, "Optimasi Perlindungan Data Dari Serangan Siber Dengan Synology Untuk Kelangsungan Bisnis Perusahaan," *J. Ilmu Komput.*, vol. V, no. 01, pp. 39–45, 2022.

[18] D. D. Diara, "Strategi Keamanan Siber Korea Selatan," *J. Indones. Sos. Sains*, vol. 1, no. 4, pp. 257–270, Nov. 2020, doi: 10.36418/jiss.v1i4.44.

[19] A. Fadilah, R. Aranggraeni, and S. R. Putri, "Eksistensi Keamanan Siber terhadap Tindakan

Cyberstalking dalam Sistem Pertanggungjawaban Pidana Cybercrime," *Syntax Lit. J. Ilm. Indones.*, vol. 6, no. 4, pp. 1555–1572, Apr. 2021, doi: 10.36418/syntax-literate.v6i4.2524.

[20] M. F. Rachman and N. Susan, "Modal Sosial Masyarakat Digital dalam Diskursus Keamanan Siber," *J. Indones. Maju*, vol. 1, no. 1, pp. 1–11, 2021, [Online]. Available: https://www.jurnalim.id/index.php/jp/article/view/6

[21] B. F. Usman, "Faktor-Faktor Yang Melatar Belakangi Kerjasama Indonesia Dengan Inggris Dibidang Keamanan Siber Tahun 2018," *Moestopo J. Int. Relations*, vol. 1, no. 2, pp. 107–114, 2021, [Online]. Available: https://journal.moestopo.ac.id/index.php/mjir/article/view/1484

[22] I. R. Putranti, A. Amaliyah, and R. Windiani, "Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah," *J. Ketahanan Nas.*, vol. 26, no. 3, p. 359, 2020, doi: 10.22146/jkn.57322.

[23] D. Luthfah, "Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law)," *terAs Law Rev. J. Huk. Humanit. dan HAM*, vol. 3, no. 1, pp. 11–22, 2021, doi: 10.25105/teras-lrev.v3i1.10742.

[24] Y. Herdiana, Z. Munawar, and N. Indah Putri, "Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19," *J. ICT Inf. Commun. Technol.*, vol. 20, no. 1, pp. 42–52, 2021, doi: 10.36054/jict-ikmi.v20i1.305.

[25] A. W. O. K. Putri, A. R. M. Aditya, D. L. Musthofa, and P. Widodo, "Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator)," *Glob. Polit. Stud. J.*, vol. 6, no. 1, pp. 35–46, 2022, doi: 10.34010/gpsjournal.v6i1.6698.

[26] T. Vimy, S. Wiranto, R. Rudiyanto, P. Widodo, and ..., "Ancaman Serangan Siber Pada Keamanan Nasional Indonesia," *J. ...*, vol. 6, no. 1, pp. 2319–2327, 2022, [Online]. Available: http://journal.upy.ac.id/index.php/pkn/article/view/2989

[27] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 14–20, 2020.

[28] A. T. Laksono and M. A. H. Nasution, "Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 83, 2020, doi: 10.30865/json.v1i2.1920.

[29] D. N. Ilham and R. A. Candra, "Analisis Celah Keamanan Jaringan Komputer dengan Menggunakan Raspberry PI 2," *J. Manaj. Inform. Komputerisasi Akunt.*, vol. 2, no. 2, pp. 140–147, 2018.

[30] G. A. J. Saskara, I. P. O. Indrawan, and P. M. Putra, "Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan Wpa/Wpa2 Di Politeknik Ganesha Guru," *J. Pendidik. Teknol. dan Kejuru.*, vol. 16, no. 2, pp. 236–247, 2019, doi: 10.23887/jptk-undiksha.v16i2.18559.

[31] M. H. Dar and S. Z. Harahap, "Implementasi Snort Intrusion Detection System (IDS) Pada Sistem Jaringan Komputer," *J. Inform.*, vol. 6, no. 3, pp. 14–23, 2018, doi: 10.36987/informatika.v6i3.1619.

[32] W. Bakti, K. Imtihan, and A. S. Pardiansyah, "Proxy Server dan Management Bandwidth Jaringan Komputer Menggunakan Mikrotik RB952Ui5ac2nD (Studi Kasus MA Ishlahul Ikhwan Nahdlatul Wathan Mispalah Praya)," *J. Inform. dan Rekayasa Elektron.*, vol. 1, no. 1, pp. 44–49, 2018, doi: 10.36595/jire.v1i1.31.

[33] S. Dewi, "Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis," *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.

[34] T. Sanjaya and D. Setiyadi, "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," *Mhs. Bina Insa.*, vol. 4, no. 1, pp. 1–10, 2019, [Online]. Available: http://ejournal-binainsani.ac.id/

[35] J. L. Putra, L. Indriyani, and Y. Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna," *IJCIT (Indonesian J. Comput. Inf. Technol.*, vol. 3, no. 2, pp. 260–267, 2018.

[36] S. Sumardi and M. T. A. Zaen, "Perancangan Jaringan Komputer Berbasis Mikrotik Router OS Pada SMAN 4 Praya," *J. Inform. dan Rekayasa Elektron.*, vol. 1, no. 1, p. 50, 2018, doi: 10.36595/jire.v1i1.32.

[37] F. Ardianto, B. Alfaresi, and R. A. Yuansyah, "Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode Otentikasi Pengguna," *J. Surya Energy*, vol. 2, no. 2, p. 167, 2018.

[38] A. Tantoni, K. Imtihan, and W. Bagye, "Implementasi Jaringan Inter-VLAN Routing Berbasis

Mikrotik RB260GS dan Mikrotik RB1100AHX4," *JIRE*, vol. 3, no. 1, pp. 77–84, 2020.

[39] Y. Mulyanto and S. B. Prakoso, "Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (NDLC)," *J. Inform. Teknol. dan Sains*, vol. 2, no. 4, pp. 223–233, 2020, doi: 10.51401/jinteks.v2i4.825.

[40] H. D. Sabdho and U. Maria, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang," *Semhavok*, vol. 1, no. 1, pp. 15–24, 2018.

[41] M. Gustiawan, R. J. Yudianto, J. Pratama, and A. Fauzi, "Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 4, pp. 244–247, 2021, doi: 10.32672/jnkti.v4i4.3098.