Dike : Jurnal Ilmu Multidisiplin
Volume 1, Nomor 2, Agustus 2023, Page 62-66
ISSN 2986-884X (media online)

Solusi Cerdas: Meningkatkan Keamanan dan Kinerja Jaringan pada Warnet dengan Mengatasi Kelemahan Sistem

Anggriawan Sifa Wahyusesa*[1], Pradana Wahyu Hidayanto[2], Enen Arienda Ramdayani[3]

[1,2,3)]Universitas Singaperbangsa Karawang, Ilmu Komputer, Karawang, Jawa Barat
Email: [1]2110631170050@student.unsika.ac.id, , [2]2110631170122@student.unsika.ac.id , [3]2110631170013@student.unsika.ac.id

Abstrak- Warnet (Warung Internet) merupakan tempat yang populer bagi masyarakat untuk mengakses internet dan menjalankan berbagai aktivitas online. Namun, keamanan dan kinerja jaringan di warnet seringkali menjadi perhatian karena dapat mempengaruhi pengalaman pengguna dan kerahasiaan data. Penelitian ini bertujuan untuk meningkatkan keamanan dan kinerja jaringan pada warnet dengan mengatasi kelemahan sistem yang ada. Metode penelitian yang digunakan adalah kombinasi antara analisis sistem yang ada, evaluasi risiko keamanan, dan implementasi solusi cerdas berbasis teknologi terkini. Pendekatan ini memungkinkan identifikasi kelemahan sistem yang rentan terhadap serangan dan pelanggaran keamanan. Hasil analisis menunjukkan bahwa kelemahan sistem yang ada termasuk celah keamanan pada perangkat jaringan, pengaturan kata sandi yang lemah, kurangnya sistem deteksi intrusi, serta kendala pada manajemen lalu lintas jaringan. Untuk mengatasi kelemahan-kelemahan ini, kami menerapkan berbagai solusi cerdas, termasuk: Penerapan firewall dan sistem keamanan jaringan yang canggih untuk melindungi data dan perangkat dari akses tidak sah dan serangan malware. Penggunaan protokol keamanan yang kuat untuk enkripsi data dan identifikasi pengguna yang sah. Implementasi sistem deteksi intrusi yang dapat mendeteksi aktivitas mencurigakan dan mengambil tindakan pencegahan secara otomatis. Peningkatan manajemen lalu lintas jaringan dengan memprioritaskan akses internet bagi pengguna yang membutuhkan koneksi stabil dan meningkatkan kecepatan akses bagi kegiatan kritikal.Melalui penerapan solusi cerdas ini, kami berhasil meningkatkan keamanan dan kinerja jaringan pada warnet. Pengguna kini dapat merasakan pengalaman internet yang lebih aman dan lancar, sementara pemilik warnet mendapatkan kepercayaan dari pelanggan karena upaya yang dilakukan dalam melindungi data dan privasi mereka. Penelitian ini menjadi contoh bagi warnet lain yang ingin meningkatkan keamanan dan kinerja jaringan mereka dengan menggunakan pendekatan cerdas berbasis teknologi terkini. Di era di mana ancaman keamanan digital semakin kompleks, solusi cerdas dapat menjadi langkah efektif untuk mengatasi kelemahan sistem dan menjaga kepercayaan pengguna dalam menggunakan layanan internet di warnet.

Kata Kunci : Solusi Cerdas, Keamanan Jaringan, Kinerja Jaringan, Warnet, Kelemahan Sistem, Analisis Sistem

Abstract - Internet cafes (Internet cafes) are popular places for people to access the internet and carry out various online activities. However, network security and performance in Internet cafes are often a concern because they can affect user experience and data confidentiality. This research aims to improve network security and performance in internet cafes by overcoming existing system weaknesses. The research method used is a combination of analysis of existing systems, evaluation of security risks, and implementation of smart solutions based on the latest technology. This approach allows the identification of system weaknesses that are vulnerable to attacks and security breaches. The results of the analysis showed that the weaknesses of the existing system include security holes in network devices, weak password settings, lack of intrusion detection systems, and constraints on network traffic management. To address these weaknesses, we implemented a variety of intelligent solutions, including: Implementation of firewalls and sophisticated network security systems to protect data and devices from unauthorized access and malware attacks. Use of strong security protocols for data encryption and legitimate user identification. Implementation of an intrusion detection system that can detect suspicious activity and take preventive measures automatically. Improved network traffic management by prioritizing internet access for users who need a stable connection and increasing access speeds for critical activities. Through the implementation of this intelligent solution, we have succeeded in improving the security and network performance of internet cafes. Users can now experience a safer and smoother internet experience, while internet café owners gain the trust of customers because of the efforts made in protecting their data and privacy. This research is an example for other internet cafes who want to improve the security and performance of their networks by using smart approaches based on the latest technology. In an era where digital security threats are increasingly complex, smart solutions can be an effective step to overcome system weaknesses and maintain user trust in using internet services in internet cafes.

Keywords : Smart Solutions, Network Security, Network Performance, Internet Cafe, System Weaknesses, System Analysis

1. PENDAHULUAN

Perkembangan teknologi dalam jaringan komputer secara bertahap meningkat pesat seiring dengan meningkatnya kebutuhan akan akses jaringan yang efisien, stabil dan dapat diandalkan. Perusahaan membutuhkan keamanan jaringan untuk melindungi data perusahaan, serta untuk mengontrol dan mengintegrasikan semua pengguna koneksi jaringan. Perusahaan ini memiliki banyak karyawan dan divisi yang berbeda, sehingga sering terjadi pergantian pekerjaan atau karyawan baru. Sehingga perlu adanya sistem keamanan jaringan yang terjamin untuk menentukan penggunaan hak

Submitted: **20/07/2023**; Accepted: **20/08/2023**; Published: **31/08/2023**

akses pada jaringan tersebut[1],[2]. Untuk mengatasi masalah tersebut, perusahaan sangat membutuhkan keamanan jaringan pada setiap port lan (local area network), yaitu dengan menggunakan metode default atau static port security, port security dynamic learning dan sticky port securty pada port-port di ruang kerja. Ini berguna untuk memblokir akses jaringan bagi karyawan yang tidak melaporkan perubahan tempat kerja dan dapat mencegah pencurian data oleh orang asing atau non-karyawan perusahaan.

Dengan pesatnya perkembangan teknologi saat ini, teknologi memegang peranan penting dalam kehidupan kita saat ini. Seiring dengan perkembangan teknologi informasi saat ini yang selalu berubah, menjadikan keamanan suatu informasi menjadi sangat penting. Banyak serangan yang sering dilakukan pada port yang terbuka, sehingga nantinya akan membuat orang yang tidak memiliki hak akses atau yang tidak berkepentingan dapat dengan mudah mengontrol port yang telah dimasukinya. Maka untuk melakukan pengamanan pada jaringan komputer dalam mengatasi serangan pada port salah satunya dengan menggunakan metode Port Knocking[3].

Port Knocking adalah sistem keamanan yang dibuat khusus untuk sebuah jaringan. Pada dasarnya cara kerja port knocking adalah dengan menutup semua port yang ada, dan hanya pengguna tertentu yang dapat mengakses port yang telah ditentukan, dengan cara tap terlebih dahulu. Berbeda dengan cara kerja Firewall, cara kerja Firewall adalah menutup semua port terlepas dari apapun meskipun pengguna memiliki hak untuk mengakses port tersebut. Sehingga pengguna yang memiliki hak akses juga tidak dapat mengaksesnya. Kelebihan Port Knocking dengan Firewall adalah walaupun semua port yang ada telah ditutup, namun user yang memiliki hak akses dan mengetahui Knocking untuk membuka suatu port, user tersebut tetap dapat menggunakan port yang telah dibukanya[4],[5].

Keamanan dalam suatu sistem tentunya sangat dibutuhkan untuk menjaga keutuhan data-data penting yang tersimpan di dalam sistem tersebut. Oleh karena itu, untuk menjaga keutuhan data ini dimulai setelah sistem terhubung dengan jaringan internet. Integritas data digunakan oleh dua perspektif, yaitu penyelenggara dan pengguna. Salah satu sistem yang digunakan dalam perspektif ini adalah Human Resources Information System (HRIS) atau sistem input data karyawan.

Kejahatan dunia maya dapat menyerang jaringan komputer, menyusup ke jaringan, mengambil data rahasia dan melumpuhkan sistem jaringan komputer. Dalam mengatasi kejahatan yang akan terjadi, diperlukan sistem yang dilengkapi dengan firewall dan Intrusion Detection System (IDS). Firewall dan IDS sebagai fitur keamanan jaringan yang dapat melindungi server, jaringan, dan memblokir serangan. Fitur firewall dan IDS dapat diimplementasikan di OSSEC Tools. OSSEC adalah Human Resources Information System (HIDS) open-source yang mampu melakukan analisis log, pemeriksaan integritas, pemantauan registri Windows, deteksi rootkit, peringatan berbasis waktu, dan respons aktif. OSSEC mampu memantau satu server atau ribuan server dalam mode server/agen[6],[7].

2. METODOLOGI PENELITIAN

Metode penelitian pada dasarnya adalah suatu metode untuk memperoleh data secara ilmiah yang mempunyai tujuan dan kegunaan tertentu. Berdasarkan ini, kami memiliki empat kata kunci perhatian adalah pendekatan ilmiah, data, tujuan dan kemudahan penggunaan. Pada jurnal ini, metode yang digunakan adalah metode kualitatif dengan studi pustaka sebagai salah satu dasar acuan dalam penyusunan jurnal ini. Selain itu, penulis juga menggunakan metode deskriptif karena dalam penelitian ini menggambarkan secara umum dan juga secara lengkap mengenai masalah yang tengah dibahas dalam jurnal ini.

3. HASIL DAN PEMBAHASAN

Tanpa kita sadari perkembangan teknologi dalam jaringan semakin pesat setiap harinya. Hal ini dapat memungkinkan terjadinya perubahan yang pesat juga bagi manusia beserta pola perilakunya. Tetapi kebutuhan manusia akan mobilitas dan fleksibilitas yang lebih besar, seiring kemajuan teknologi, membutuhkan sesuatu yang lebih praktis. Teknologi melekat pada jaringan yang ada dan telah menyebabkan perkembangan komunikasi yang telah mengubah penggunaan teknologi.

Dalam teknologi informasi dan komunikasi, dunia jaringan komputer berkembang begitu pesat sehingga setiap komputer harus dapat saling berkomunikasi dengan menggunakan media tertentu. Dengan jaringan LAN (Local Area Network) masih menggunakan kabel sebagai media , memungkinkan beberapa komputer untuk berkomunikasi satu sama lain. Dengan tumbuh teknologi di Indonesia, perkembangan teknologi dalam jaringan berkembang pesat dan semakin populer. Masih banyak yang harus dipahami dan banyak yang telah berubah, seperti bagaimana jaringan itu digunakan dari jaringan kabel ke nirkabel.

Perkembangan teknologi jaringan komputer saat ini menunjukkan bahwa Sistem keamanan sangat penting untuk sistem keamanan jaringan komputer yang terhubung ke jaringan maritim atau internet. Jaringan komputer saat ini adalah layanan yang sangat dibutuhkan. Jaringan komputer memiliki banyak keunggulan dibandingkan komputer yang

Submitted: **20/07/2023**; Accepted: **20/08/2023**; Published: **31/08/2023**

berdiri sendiri. Internet adalah jaringan komputer paling terbuka di dunia. Konsekuensi yang harus ditanggung adalah bagaimana mengamankan jaringan terhubung ke Internet. Namun, masalah jaringan sering terjadi. Antara lain, data yang dikirim lambat, rusak, dan tidak pernah sampai ke tujuan. Batas waktu dan masalah keamanan sering terjadi selama komunikasi. Bahkan saat ini, tidak ada jaringan yang benar-benar aman. Dengan berkembangnya teknologi komputer, keamanan jaringan menjadi isu yang sangat penting. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke Internet[8].

Secara umum, jaringan adalah lokasi di mana beberapa komputer yang terhubung ke jaringan bersama, dengan salah satu satu komputer bertindak sebagai komputer server yang dikonfigurasi atau dikonfigurasi, dan yang lain bertindak sebagai komputer klien. Cyber warnet merupakan warnet yang masih dalam pengembangan, dengan operasi baru, karena warnetnya kurang sempurna, baik dari sisi gedung serta sisi sistem. Pengguna warnet membutuhkan aliran dan permasalahan yang ada di Cyberwarnet adalah tingkat keamanan yang kurang optimal dari server warnet. Server saat ini tidak menerapkan sistem keamanan . Dijalankan oleh ping flood, smurf attack dan lain – lain yang menyebabkan sistem jaringan warnet menjadi down.

Jika pada suatu hari terjadi sebuah aktivitas yang mencurigakan seperti aktifitas keluar dan masuk pada sistem, maka hal itu semua akan terekam pada IDS. IDS adalah software atau hardware yang dapat melakukan otomatisasi dalam proses monitoring kejadian yang terjadi di sistem jaringan maupun komputer serta menganalisisnya untuk menemukan permasalahan dalam sistem tersebut. Terdapat 6 alasan dalam menggunakan IDS ini dalam hal menganalisis permasalahan yang terjadi di jaringan, antara lain:

1. Untuk mencegah resiko timbulnya sebuah masalah
2. Untuk mendeteksi serangan dan pelanggaran keamanan lainnya yang tidak bisa dicegah oleh perangkat keamanan lain.
3. Untuk mendeteksi usaha yang berkaitan dengan serangan seperti contohnya probing dan aktivitas dorknob rattling.
4. Untuk mendokumentasi ancaman yang masuk ke dalam sebuah organisasi.
5. Untuk bertindak sebagai pengendali kualitas dari dalam maupun dari luar organisasi.
6. Untuk memberikan informasi yang berguba terkait dengan penyusupan yang tengah terjadi dalam jaringan organisasi tersebut.

Hal tersebut akan membantu dengan konfigurasi organisasi atau kebijakan. Mendengus adalah NIDS yang bekerja dengan menggunakan tanda tangan deteksi, juga berfungsi sebagai sniffer dan paket penebang kayu. Banyak fitur snort yang mirip dengan Kombinasi dump/review TCP, tetapi snort memiliki banyak keuntungan lainnya. Sebagai alat ethereal yang terkenal, snort tersedia secara gratis dalam bentuk kode sumber di bawah ini Lisensi Publik Umum GNU, sebagian besar varian dan distro linux/unix, serta sistem windows.

Snort adalah perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis lalu lintas waktu nyata, itu dapat mendeteksi berbagai jenis serangan. Mendengus bukan hanya protokol analisis atau sistem deteksi intrusi (Intrusion Detection System) IDS, tapi sedikit campuran antara keduanya, dan bisa sangat berguna dalam menanggapi insiden serangan terhadap host jaringan. Fitur Snort dapat menjadi bantuan bagi administrator sistem dan jaringan, di mana ia dapat peringatkan kami tentang penyusup potensial berbahaya.

Menurut [9] keamanan jaringan yang ada saat ini telah menjadi isu yang sangat penting dengan seiringan hadirnya perkembangan teknologi komputer. Menurut [10] aspek-aspek dalam keamanan jaringan terdapat empat bagian yaitu sebagai berikut:

1. Kerahasiaan pesan (Confidenciality), merupakan mekanisme yang digunakan untuk menjaga keamanan informasi sehingga tidak dapat dibaca atau dilihat oleh orang yang tidak berwenang untuk melakukannya.
2. Keaslian pesan (Integrity), merupakan sebuah cara agar menjaga data maupun informasi yang tidak dapat diubah, dikurangi maupun ditambah oleh orang lain.
3. pengirim (Autentification), bahwa data dan informasi yang sudah digunakan serta dikirim bari dari pengguna merupakan data yang sebenarnya dan benar pesan tersebut merupakan milik dari pengguna tersebut.
4. Anti penyangkalan (NonRepudiation) adalah cara untuk menjaga agar setelah selesai melakukan transaksi dan aktivitas online lainnya, agar tidak bisa menyangkal bahwa belum melakukan hal tersebut.

Terdapat beberapa masalah pada jaringan nirkabel yang dapat mempengaruhi aspek keamanan dari sistem wireless, antara lain:

1. Perangkat akses informasi yang menggunakan sistem nirkabel biasanya berukuran kecil sehingga mudah untuk dicuri. Seperti notebook, PDA, handphone, dan sejenisnya sangat mudah untuk dicuri. Jika dicuri, informasi yang terkandung di dalamnya (atau kunci akses informasi) dapat jatuh ke tangan orang yang tidak berwenang.
2. Untuk memiliki hubungan. Sistem yang tidak menggunakan enkripsi dan keamanan otentikasi, atau menggunakan enkripsi yang mudah diretas akan mudah ditangkap.

Submitted: **20/07/2023**; Accepted: **20/08/2023**; Published: **31/08/2023**

3. Perangkat nirkabel kecil membatasi kemampuan perangkat dalam hal CPU, RAM, kecepatan komunikasi, catu daya. Akibatnya, sistem keamanan, seperti enkripsi yang digunakan, harus memperhatikan batasan ini. Saat ini tidak mungkin menggunakan sistem enkripsi canggih yang membutuhkan siklus CPU yang cukup tinggi untuk memperlambat transfer data.
4. Pengguna tidak dapat membuat sistem keamanan sendiri (membuat enkripsi sendiri) dan hanya bergantung pada vendor (pembuat perangkat). Namun mulai muncul perangkat mobile yang dapat diprogram oleh pengguna. Begitu juga saat ini notebook sudah menggunakan keamanan autentikasi akses dengan sistem biometrik.
5. Terbatasnya jangkauan radio dan interferensi menyebabkan ketersediaan layanan menjadi terbatas. Serangan DoS dapat dilakukan dengan menyuntikkan lalu lintas palsu.
6. Saat ini fokus sistem nirkabel adalah mengirim data secepat mungkin. Adanya enkripsi akan memperlambat proses pengiriman data sehingga penggunaan enkripsi masih belum diprioritaskan. Setelah kecepatan transmisi data memadai dan harga menjadi murah, maka kita akan melihat perkembangan dari sisi keamanan dengan menggunakan enkripsi.

Selain masalah keamanan yang dapat mempengaruhi aspek keamanan dari sistem wireless, terdapat juga kelemahan yang mana dapa mengambaht kinerja sebuah jaringan karena kelemahan ini terdapat pada lapisan jaringan nirkabel. Kelemahan tersebut diantaranya yakni:

1. Physical Layer. Seperti yang kita semua tahu, lapisan fisik komunikasi data mengatakan banyak tentang pembawa data itu sendiri. Dalam sistem komunikasi data nirkabel, media perantara tidak lain adalah di luar ruangan. Di luar ruangan, data lewat secara bebas dalam bentuk sinyal radio pada frekuensi tertentu. Tentu saja, mudah untuk membayangkan betapa rapuhnya lalu lintas data di dunia nyata. Siapa pun dapat menangkapnya, mengetiknya, dan bahkan membacanya secara langsung tanpa disadari. Tentu saja, jika itu hanya untuk kesenangan pribadi, menguping, atau membaca oleh orang lain, itu sedikit lebih rumit, tetapi tidak terlalu berbahaya. Tetapi bagaimana jika kerentanannya ada di jaringan nirkabel perusahaan? Jaringan nirkabel ini berisi berbagai transaksi bisnis, proyek perusahaan, informasi rahasia, rahasia keuangan, dan banyak informasi sensitif lainnya. Tentu saja, penyadapan tidak dapat diterima jika perusahaan tidak ingin menjadi sasaran manusia.
2. Network Layer, Ada banyak pembicaraan tentang perangkat dengan kemampuan untuk membuat jaringan komunikasi, biasanya disertai dengan sistem pengalamatan. Dalam jaringan komunikasi nirkabel, perangkat yang biasa digunakan sering disebut titik akses, atau disingkat AP. Sistem pengalamatan IP terdeteksi dengan andal pada perangkat ini. AP ini terkadang disebut perangkat bebas dan terbuka karena dirancang untuk berkomunikasi melalui media yang bebas dan terbuka. Perangkat jaringan yang tidak divalidasi dan dikontrol dengan baik dapat menjadi titik masuk bagi penyusup. Dari hanya melihat konten, hingga perubahan bertahap, hingga pembajakan langsung, AP memiliki peluang yang sangat bagus untuk belajar. Oleh karena itu, keamanan AP-AP juga harus diperhatikan pada jaringan nirkabel yang ada. Selain itu, komunikasi antar AP juga harus dipantau dan keamanan harus diperhatikan.
3. User Layer. Jaringan nirkabel menggunakan media publik untuk lalu lintas data, tetapi jika jaringan yang ada bukanlah jaringan publik yang dapat diakses publik, maka tentu saja Anda ingin membatasi akses dan mencegah akses oleh pengguna yang tidak sah untuk mengakses jaringan nirkabel Anda, itu tidak sulit. Tentu saja, ketika seorang pengguna dapat menggunakan jaringan yang ada, ini menempatkan pengguna lain yang berwenang pada kerugian besar. Perangkat jaringan yang biasanya terhubung ke jaringan nirkabel juga perlu dilacak dan dipantau dengan benar, karena sangat berguna untuk memantau, menagih, dan memahami tren di jaringan yang ada.
4. Application Layer. Jaringan yang hanya menggunakan media kabel, terutama jaringan nirkabel yang rentan di semua tingkatan, dapat menciptakan celah yang cukup besar dalam aplikasi. Aplikasi bisnis yang dikonsumsi melalui media nirkabel secara alami sangat rentan terhadap keamanan, baik melalui intrusi sederhana atau Denial of Service (DoS). Jaringan nirkabel yang baik juga harus dapat melindungi aplikasi yang berjalan di dalamnya agar tidak mudah terganggu.

Dengan adanya kelemahan yang terdapat pada jaringan nirkabel sepertii yang suda dijelaskan diatas, maka dibawah ini terdapat beberapa cara yang dapat digunakan untuk mengamankan jaringan nirkabel yang kita miliki, yaitu:

1. Menggunakan kunci WEP, yakni standar keamanan dan enkripsi pertama yang digunakan pada jaringan nirkabel.
2. Menggunakan kunci WPA-PSK atau WPA2-PSK.
3. Menyembunyikan SSID.
4. Memakai enkrispsi.
5. Memanfaatkan fasilitas MAC.
6. Gunakan enkripsi yang kuat.
7. Captive portal.

Submitted: **20/07/2023**; Accepted: **20/08/2023**; Published: **31/08/2023**

8. Ubah pengaturan SSID.
9. Mengisolasi wireless network dan LAN.
10. Mematikan WAP saat tidak digunakan.
11. Mengganti password.
12. Memakai MAC filtering.
13. Matiakn SSID Broad casting.
14. Memancarkan gelombang pada frekuensi yang berbeda.
15. Mengontrol signal wireless.

Beberapa kelemahan pada masing-masing layer adalah menggunakan enkripsi yang terpercaya, merubah password default admin, menonaktifkan broadcast SSID, merubah default SSID, menggunakan MAC filtering, wireless Hal ini dapat diatasi dengan memisahkan jaringan dari LAN dan menggunakan gelombang frekuensi yang berbeda.

4. KESIMPULAN

Teknologi nirkabel merupakan teknologi yang dapat digunakan untuk aplikasi teknologi informasi berbasis jaringan bergerak. Oleh karena itu, portabilitas dan fleksibilitas menjadi keunggulan utama penggunaan teknologi nirkabel. Penggunaan jalur komunikasi nirkabel menggunakan teknologi frekuensi radio dan spesifikasi frekuensi bervariasi tergantung pada perangkat dan operator yang menyediakannya. Menggunakan lebih banyak frekuensi terbuka daripada kabel, kerentanan keamanan di jalur komunikasi lebih berbahaya daripada menggunakannya. Model pemrosesan keamanan saat menggunakan jalur komunikasi dengan teknologi nirkabel termasuk menyembunyikan SSID, Termasuk menggunakan kunci WPA-PSK atau WPA2-PSK, menerapkan filter MAC ke perangkat, dan memasang infrastruktur captive portal. Model manajemen keamanan ini adalah yang paling umum saat ini dan dapat diterapkan untuk mengatasi tantangan yang ditimbulkan oleh ancaman keamanan menggunakan teknologi nirkabel.

REFERENSI

[1] E. Panggabean and J. R. Sagala, "Analisa Perbandingan Metode Jaringan Syaraf Tiruan Dengan Metode Sistem Pendukung Keputusan Untuk Penerimaan Tenaga Kerja," *JUMIN*, vol. 2, no. 2, pp. 41–44, Jun. 2021, doi: 10.55338/jumin.v2i2.697.
[2] S. P. Lestari, H. N. Fadlan, R. Angelia Purba, and I. Gunawan, "REALISASI KRIPTOGRAFI PADA FITUR ENKRIPSI END-TO-END PESAN WHATSAPP," *JUMIN*, vol. 4, no. 1, pp. 1–8, Nov. 2022, doi: 10.55338/jumin.v4i1.423.
[3] Z. A. Tarigan and J. R. Sagala, "Peramalan (Forecasting) Jumlah Kunjungan Pasien Di Klinik Kasih Ibu Menggunakan Metode Weight Moving Average," vol. 3, 2021.
[4] A. R. Faqih and A. A. Widya, "Implementasi Aplikasi E-Ticket pada Bumdes Desa Sumbermulyo Kec. Jogoroto Kab. Jombang sebagai Solusi Digitalisasi Pengelolaan Tiket.," vol. 2, 2023.
[5] N. D. Farhanah, "Optimalisasi Penentuan Kinerja Perawat Terbaik di Klinik Amanah dengan Sistem Pendukung Keputusan dan Metode Simple Additive Weighting," vol. 2, 2023.
[6] A. S. Sitio and F. A. Sianturi, "Analisa dan Perancangan Metode TOPSIS Seleksi Calon Pegawai," *Journal Of Informatic Pelita Nusantara*, vol. 4, no. 1, 2019.
[7] E. Bu'ulolo and F. A. Sianturi, "Diagnose Expert System Dental Disease In Humans Method Using Dempster Shafer," *Journal of Computer Networks, Architecture and High Performance Computing*, vol. 2, no. 2, pp. 227–230, 2020.
[8] Y. F. Hutahaean and M. Harahap, "Sistem Pendukung Keputusan Rekrutmen Tenaga Kerja Honorer Implementasi Metode Maut Pada Dinas Perkebunan Provinsi Sumatera Utara," *JUMIN*, vol. 3, no. 2, pp. 79–91, Jun. 2022, doi: 10.55338/jumin.v3i2.276.
[9] M. Sianturi and N. Andika, "Peningkatan Efisiensi Penelusuran Aset melalui Sistem Manajemen Aset dan Analytical Hierarchy Process," *Jurnal Sistem Informasi*, vol. 2, 2022.
[10] F. A. Sianturi, P. M. Hasugian, and B. Sinaga, "Pelatihan Microsoft Office Untuk Guru-Guru Se-Kecamatan Namorambe," *Jurnal Pengabdian Kepada Masyarakat Nusantara*, vol. 1, no. 1 Maret, pp. 1–7, 2019.

Submitted: **20/07/2023**; Accepted: **20/08/2023**; Published: **31/08/2023**