Analisis Bibliometrik Mengenai Serangan Phishing dan Whatsapp menggunakan Vosviewer

Rafi Kurnia Sujiwana[1], Achmad Fahmi Ainur Ridho[2], Dwi Cindy Aryanti[3], Nur Aini Rakhmawati[4*]

[1,2,3,4] *Sistem Informasi Institut Teknologi Sepuluh Nopember*
Jl. Raya ITS, Sukolilo, Surabaya, Jawa Timur Indonesia

[1]kurniarafi44@gmail.com, [2]fahmiridho05@gmail.com,[3]aryantidwicindy@is.its.ac.id, [4*] nur.aini@is.its.ac.id

Intisari— **Era Teknologi yang serba canggih telah meningkat, namun terdapat juga ancaman terhadap dunia maya yaitu dengan phising. Phising menjadi salah satu ancaman yang berbahaya dan yang paling umum digunakan. Phishing mengeksploitasi setiap individu yang dituju dengan trik menipu untuk mencuri data pribadi. Pada 2023, publikasi terkait phishing dan whatsapp mencapai puncaknya dengan 64 publikasi (34.04%). Analisis perkembangan publikasi menunjukkan 3 klaster: Kluster 1 warna merah memiliki kata kunci *phishing, cybercrime, cybersecurity, sensitive information*, menggambarkan keterkaitan dengan kejahatan siber dan keamanan siber. Kluster 2 warna hijau memiliki kata kunci *social media, whatsapp, security, privacy, data security*, menekankan kerentanan privasi dan data pribadi dengan sosialisasi mengenai edukasi keamanan siber. Kluster 3 warna biru memiliki kata kunci *social engineering, phishing attacks, cybersecurity, awareness*, menunjukkan potensi ancaman terhadap keamanan dengan menerapkan metode khusus berupa penerapan cybersecurity. Metodologi dengan melakukan pemetaan kata kunci sangat membantu dalam hal mendeteksi pola hubungan dan pemantauan yang efektif terhadap risiko phishing.**
Kata kunci— Analisis Bibliometrik, Whatsapp, Phishing, Teknologi, Keamanan Siber, Privasi.

***Abstract*—The era of advanced technology has risen, but there are also threats to cyberspace, such as phishing. Phishing has become one of the most dangerous and commonly used threats. Phishing exploits targeted individuals by using deceptive tricks to steal personal data. In 2023, publications related to phishing and WhatsApp peaked at 64 publications (34.04%). Analysis of publication trends revealed 3 clusters: Cluster 1 in red includes keywords such as phishing, cybercrime, cybersecurity, sensitive information, depicting its relation to cybercrime and cybersecurity. Cluster 2 in green includes keywords such as social media, WhatsApp, security, privacy, data security, emphasizing the vulnerabilities of privacy and personal data with a focus on cybersecurity education. Cluster 3 in blue includes keywords such as social engineering, phishing attacks, cybersecurity, awareness, indicating the potential threat to security by applying specific methods in the form of cybersecurity implementation. The methodology of mapping keywords is very helpful in detecting relational patterns and effectively monitoring phishing risks.**
Keywords— Bibliometric Analysis, WhatsApp, Phishing, Technology, Cybersecurity, Privacy.

I. PENDAHULUAN

Era Teknologi yang saat ini serba canggih memberikan banyak manfaat yaitu kemudahan dalam melakukan segala hal [1]. Dengan kemudahan tersebut menjadikan teknologi tidak dapat dilepaskan lagi dari kehidupan sehari-hari [2]. Salah satu teknologi yang paling berpengaruh dalam keseharian adalah Teknologi Informasi atau disebut TI. Teknologi Informasi sangat mempengaruhi semua aspek pada setiap bangsa, seperti: keuangan, transportasi, hiburan, pendidikan, pekerjaan.

Namun, seiring dengan kemudahan yang diberikan, terdapat juga ancaman yang sangat kompleks terhadap keamanan teknologi informasi tersebut. Salah satu dari banyaknya ancaman yang sering terjadi adalah serangan phishing. Serangan phishing adalah suatu bentuk pencurian identitas dimana situs web jahat meniru situs asli, seperti lembaga keuangan, perusahaan, atau bahkan teman dan keluarga untuk mendapatkan informasi sensitif secara ilegal [3]. Contohnya, para pelaku mengirimkan email dengan tautan pengalihan ke situs web berbahaya di mana korban diminta untuk memberikan data sensitif yang dimiliki, seperti: nomor rekening bank atau login dan kata sandi. Pelaku juga dapat melampirkan file ke email palsu untuk diunggah oleh korban sehingga otomatis dapat mengeksekusi malware yang disematkan di dalam file tersebut [4].

Serangan phishing saat ini semakin sulit dideteksi secara manual. Pelaku terus mengembangkan teknik dan taktik dalam menyesuaikan pesan agar terlihat lebih meyakinkan. Menurut Pusat Pengaduan Kejahatan Internet FBI, terdapat lebih dari 2018 pengaduan yang mengakibatkan kerugian lebih dari 1,2 miliar karena penyusupan email bisnis [5]. Berdasarkan Laporan Tahunan Kejahatan Internet FBI terbaru, kejadian serangan phishing telah melonjak ke level tertinggi sejak tahun 2019, sehingga mengakibatkan jumlah korban yang jauh lebih besar dibandingkan dengan pelanggaran data pribadi, yang menduduki peringkat kedua dalam hal jumlah korban pada tahun 2022 [5]. Selain itu, kerugian finansial yang terkait dengan kejahatan internet, termasuk phishing, mencapai angka yang mengejutkan sebesar 10,3 miliar pada tahun 2022, hampir dua kali lipat dampak finansial yang terjadi pada tahun 2021 [5]. Menurut Indonesia Anti-Phishing Data Exchange (IDADX), pada kuartal IV 2023 sebanyak 8.161 laporan yang diantaranya sebanyak 8.024 laporan merupakan data phishing [6]. Oleh karena itu, masyarakat untuk tetap waspada dan bijak dalam menggunakan aplikasi whatsapp yaitu mewaspadai pesan tidak dikenal yang mengirimkan suatu link maupun dokumen palsu yang bisa menyebabkan terjadinya pengambilan data secara ilegal.

Penggunaan analisis bibliometrik telah menjadi sangat populer dalam penelitian selama beberapa tahun terakhir [7].

Analisis bibliometrik adalah salah satu metode yang digunakan dalam menganalisis suatu data bibliografi yang diperoleh dari berbagai sumber literatur, seperti: artikel, jurnal, dan lain-lain yang dapat memberikan pemahaman tentang keunggulan pada suatu disiplin ilmu yang terkait dengan lembaga pendidikan dan menerapkan berbagai teori. Sebagai contoh, analisis penulisan, analisis kutipan, *webometrics* (bibliometri berbasis web), kolaborasi penulisan (penulis bersama), *obsolescence* (kondisi usang) pada dokumen, faktor dampak, dan sebagainya [8].

Penelitian analisis bibliometrik mengenai serangan phising di aplikasi whatsapp bertujuan untuk memperoleh hubungan antara phishing dan whatsapp dengan mendeteksi berbagai titik koneksi yang dihasilkan dalam jaringan pemetaan kata kunci.

II. BACKGROUND/LATAR BELAKANG/REVIEW LITERATUR

Serangan phishing merupakan bentuk penipuan online yang bertujuan untuk mencuri informasi sensitif pengguna, seperti data pribadi, informasi keuangan, dan kata sandi. Pelaku phishing biasanya meniru situs web atau email resmi dari perusahaan, organisasi, atau bahkan individu untuk meyakinkan korban agar memberikan informasi pribadi mereka. Serangan ini dapat dilakukan melalui berbagai media, seperti email, SMS, situs web palsu, dan media sosial [9].

Pelaku phising menggunakan berbagai teknik untuk menipu korban, seperti rekayasa sosial, penargetan khusus, dan penipuan identitas. Teknik-teknik ini semakin canggih dan terstruktur sehingga metode tradisional dalam deteksi phishing, seperti aturan berbasis tanda tangan dan daftar hitam URL [9].

Serangan phishing memiliki dampak negatif yang signifikan bagi individu dan organisasi, antara lain:

1. Serangan phishing dapat mencuri data sensitif seperti informasi pribadi, informasi keuangan, dan rahasia dagang. Hal ini dapat berakibat pada kerugian finansial yang signifikan dan bahkan dapat membahayakan keamanan nasional [9].
2. Serangan phishing yang berhasil dapat merusak reputasi perusahaan atau organisasi yang menjadi target. Hal ini dapat berakibat pada hilangnya kepercayaan pelanggan dan mitra bisnis [9].
3. Serangan phishing dapat mengganggu operasi bisnis dan organisasi. Hal ini dapat mengakibatkan kerugian finansial dan terhambatnya produktivitas [10].
4. Serangan phishing dapat menimbulkan ketakutan dan kecemasan bagi korban. Hal ini dapat berakibat pada stres, depresi, dan bahkan trauma psikologis [10].

Beberapa teori yang mendukung analisis dan interpretasi data adalah:

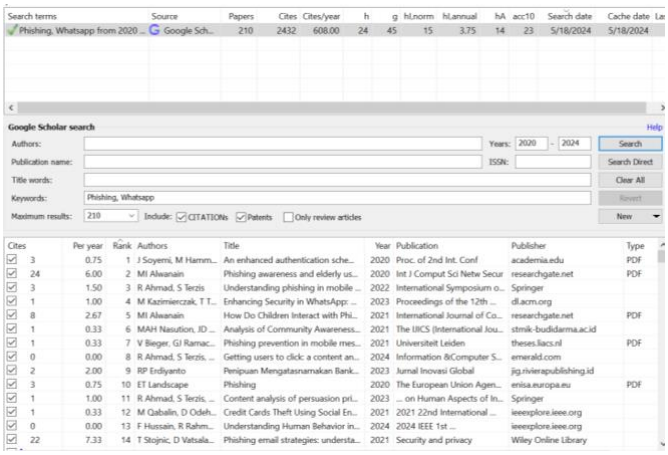
1. Teori Difusi Inovasi: Teori difusi inovasi dikembangkan oleh Everett Rogers, menjelaskan bagaimana ide, inovasi, atau teknologi baru menyebar dalam kebudayaan [11]. Dalam analisis bibliometrik, teori ini dapat membantu memahami bagaimana konsep atau metodologi baru dalam penelitian serangan phishing dan keamanan WhatsApp.
2. *Structure of Scientific Revolutions*: Teori ini dikemukakan oleh Thomas Kuhn menjelaskan bagaimana paradigma ilmiah berubah melalui revolusi ilmiah yang menjadi jargonnya [12]. Dalam konteks analisis bibliometrik, teori ini membantu memahami perubahan paradigma dan munculnya konsep-konsep baru dalam penelitian serangan phishing dan keamanan di WhatsApp.

III. METODOLOGI PENELITIAN

Pada penelitian ini menggunakan metode analisis bibliometrik untuk menggali suatu informasi tentang penyebaran jumlah publikasi dan kutipan dari berbagai sumber literatur yang berasal dari publikasi terindeks *Google Scholar* kemudian dianalisis melalui serangkaian langkah yang terdapat pada analisis bibliometrik. Langkah-langkah tersebut antara lain: tahap pencarian, tahap filtrasi, dan analisis bibliometrik dengan menggunakan *VOSviewer* sebagai *software* pendukung.

Tahap Pencarian

Pada tahap pencarian dilakukan dengan penelusuran penelitian terdahulu dan studi literatur [13]. Studi literatur adalah cara yang dipakai untuk menghimpun data-data atau sumber-sumber yang berhubungan dengan topik yang diangkat dalam suatu penelitian ini [14]. Google scholar digunakan sebagai sumber pencarian artikel ilmiah yang relevan [14].



Gambar 1. Tahap Pencarian

Sumber: Penulis

Software yang digunakan pada tahap ini yaitu aplikasi Harzing's Publish or Perish. Kata kunci "phishing, whatsapp" digunakan untuk mencari berbagai artikel ilmiah yang telah dipublikasikan pada tahun 2020 sampai 2024 dan sesuai dengan topik penelitian ini. Hasil pencarian dibatasi sebanyak 210 artikel. Artikel yang telah terkumpul kemudian disimpan dalam format *.ris*, selanjutnya difilter menggunakan aplikasi mendeley.

Tahap Filtrasi

Tahap filtrasi merupakan proses krusial dalam memilih artikel ilmiah yang relevan untuk analisis lebih lanjut [15]. Pada

tahap ini menggunakan aplikasi Mendeley dalam melakukan seleksi artikel ilmiah. Dalam tahap ini telah ditemukan sejumlah artikel yang memenuhi kriteria pencarian berdasarkan kata kunci "phishing, whatsapp" yaitu sejumlah 188 artikel kemudian melakukan evaluasi berdasarkan judul dan abstrak dari setiap artikel ilmiah untuk menentukan tingkat relevansi dengan topik penelitian ini. Semua artikel yang kurang relevan dilakukan eliminasi. Selain itu, penelusuran keyword yang mungkin tidak terbaca oleh aplikasi Mendeley juga dilakukan untuk memastikan informasi yang komprehensif dari setiap artikel terakses. Pada tahap akhir didapatkan 100 data bibliografi yang paling relevan dan dapat digunakan untuk tahap analisis bibliometrik. Proses filtrasi merupakan langkah penting dalam memastikan data yang digunakan pada tahap analisis adalah data yang sangat relevan dan dapat mewakili fokus penelitian.

Tahap Analisis Bibliometrik

Pada tahap analisis bibliometrik menggunakan aplikasi *VOSviewer* yang digunakan untuk memvisualisasikan peta bibliometrik. *VOSviewer* memiliki kemampuan text-mining yang memungkinkan visualisasi jaringan atau hubungan antara kutipan artikel dalam bentuk grafik [16]. Analisis bibliometrik bergantung pada komputerisasi dalam pengolahan data dan memerlukan pengaturan data tertentu secara berurutan untuk memastikan hasil yang dapat diandalkan secara statistik [17]. Teknik analisis bibliometrik yang digunakan dalam penelitian yaitu metode *co-occurrence*. Metode tersebut mengukur hubungan antara dua atau lebih artikel ilmiah berdasarkan jumlah kata kunci yang sama dan muncul dalam semua artikel tersebut [18].

Data bibliografi yang terkumpul pada tahap filtrasi kemudian diimport ke *VOSviewer* untuk dihitung jumlah kutipan yang diterima oleh semua artikel ilmiah. Hasil perhitungan jumlah kutipan digunakan untuk menghitung nilai *co-occurrence* antara dua atau lebih artikel ilmiah. Nilai *co-occurrence* yang tinggi menunjukan bahwa dua atau lebih artikel ilmiah tersebut memiliki hubungan erat [19]. Hubungan berupa antar topik penelitian, metode penelitian, atau penulis artikel ilmiah. Dalam penelitian menggunakan parameter *minimum number of occurrence* sebesar 3 yang berarti bahwa tiga atau lebih artikel ilmiah memiliki hubungan erat jika setidaknya tiga kata kunci yang sama. Hasil analisis bibliometrik ini kemudian divisualisasikan dalam bentuk peta bibliometrik. Peta bibliometrik ini digunakan untuk mengetahui tren penelitian, topik-topik penelitian yang saling terkait [20].

IV. HASIL DAN PEMBAHASAN/DISKUSI

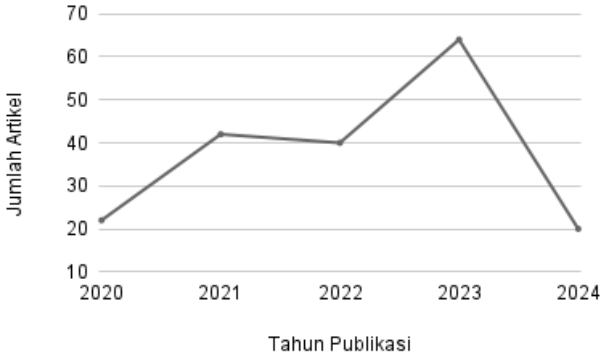
Pertumbuhan publikasi untuk topik phishing yang data diambil dari *Google Scholar* dalam rentang tahun 2020 hingga 2024 menggunakan pencarian kata kunci phishing dan whatsapp menunjukkan angka sejumlah 202 artikel. Berikut data jumlah publikasi dengan topik pencarian phishing dan media sosial dalam rentang tahun 2020-2024 berdasarkan data yang diambil dari *Google Scholar*.

TABEL I
JUMLAH PUBLIKASI ARTIKEL TAHUN 2020-2024

Tahun Publikasi	Jumlah Artikel	Persentase
2020	22	11.70 %
2021	42	22.34%
2022	40	21.27 %
2023	64	34.04 %
2024	20	10.63%

Sumber : Hasil Perhitungan Penulis

Berdasarkan tabel 1 diperoleh jumlah data dengan kata kunci pencarian phishing dan whatsapp menunjukkan adanya peningkatan dari tahun ke tahun dan mengalami penurunan yang cukup drastis pada tahun 2024. Persentase tersebut berasal dari jumlah perbandingan artikel pada tahun publikasi dengan jumlah artikel yang ada di *Google Scholar* dan menggunakan kata kunci phishing dan whatsapp.



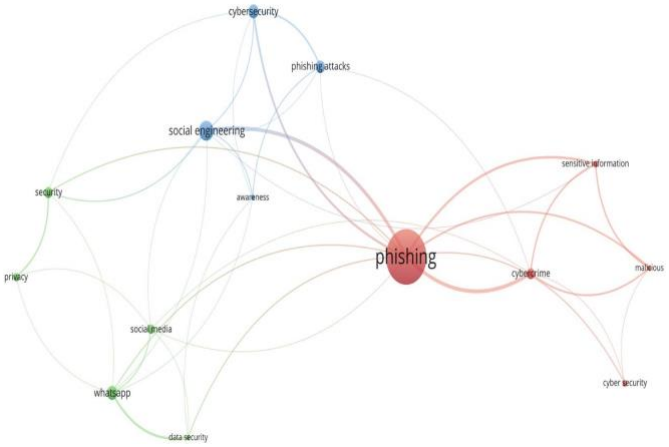
Gambar 1. Grafik Tren Perkembangan Publikasi Artikel dalam Rentang Tahun 2020-2024

Grafik di atas menunjukkan tren jumlah artikel yang dipublikasikan dari tahun 2020 hingga 2024. Tren publikasi terus naik dari tahun 2020 hingga mencapai puncaknya pada tahun 2023. Perkembangan tertinggi terjadi pada tahun 2023 dengan jumlah publikasi mencapai 64 artikel (34.04%), yang merupakan puncak tertinggi dalam periode lima tahun terakhir. Pada tahun 2024, jumlah publikasi mengalami penurunan drastis menjadi 20 artikel. Penurunan ini dikarenakan data yang digunakan hanya mencakup paruh pertama tahun 2024.

Analisis Co-Occurrence

Berdasarkan analisis yang telah dilakukan mengenai kata kunci phishing terindeks Google Scholar tahun 2020-2024 membentuk peta sebaran dengan jumlah klaster yang dihasilkan sebanyak tiga klaster. Analisis dilakukan dengan menggunakan co-occurrence dalam perangkat lunak

VOSviewer yang menghasilkan 379 keywords dengan batasan jumlah minimum kemunculan kata kunci adalah 4. Dengan batasan tersebut, diperoleh 17 kata kunci yang memenuhi. Berdasarkan analisis co-occurrence dari VOSviewer diperoleh hasil deteksi bahwa terdapat 14 kata kunci yang saling terkoneksi. Pemetaan dari 14 kata kunci ditampilkan dalam gambar 3 yang menunjukkan jaringan hubungan antar kata kunci dari paper yang telah dikumpulkan. Kata kunci dengan frekuensi terbesar merupakan phishing dan Whatsapp yang saling terhubung dengan satu sama lain melalui kata kunci lainnya



Gambar 2. Peta Perkembangan Bidang Topik Phishing terindeks Google Scholar tahun 2020-2024

Dalam VOSViewer Terdapat tiga klaster yang dihasilkan untuk 14 kata kunci. Klaster diberikan tanda berdasarkan fokus. Setiap klaster jaringan kata kunci dibedakan dengan warna. Ukuran node juga menunjukkan frekuensi kata kunci yang jika semakin besar ukuran maka semakin besar pula frekuensi kata kunci. Ketebalan lintasan jaringan ditentukan oleh kedekatan hubungan antara dua istilah [21]. Berdasarkan gambar 3 klaster terbagi menjadi tiga warna yaitu klaster 1 berwarna merah, klaster 2 berwarna hijau, dan klaster 3 berwarna biru. Klaster yang berfokus pada keamanan secara umum seperti whatsapp, *security*, dan *social media* menjadi penghubung antar kedua klaster lainnya.

Kluster 1 yang berwarna merah terdiri dari kata kunci *phishing*, *malicious*, *cybercrime*, *cybersecurity*, *sensitive information*. Kata kunci menunjukkan bahwa kata kunci phishing sebagai salah satu kejahatan siber. Kluster 2 berwarna hijau terdiri dari kata kunci *social media*, whatsapp, *security*, *privacy*, *data security*. Kata kunci pada klaster 2 berpusat pada whatsapp yang berkaitan erat dengan privacy dan data security. Kata kunci muncul menunjukkan bahwa whatsapp menjadi tempat sasaran dalam kejahatan *phishing*. Kluster 3 berwarna biru terdiri dari kata kunci *social engineering*, *phishing attacks*, *cybersecurity*, *awareness*. Kata kunci memiliki indikasi potensi ancaman terhadap keamanan memerlukan upaya mengurangi risiko dengan menerapkan keamanan siber.

Kata kunci phishing dan media sosial menghasilkan garis hubungan yang menunjukkan adanya keterkaitan antar keduanya disertai keterkaitan dengan berbagai kata kunci lainnya. Hal ini mengingatkan terhadap tren kasus *phishing* yang mengalami kenaikan jumlah kasus setiap tahun dengan perkembangan jenis dan teknik.

V. KESIMPULAN

Analisis bibliometrik adalah salah satu metode penelitian bagi para peneliti yang ingin menjelajahi sejarah di dalam bidang penelitian yang luas dan penuh informasi. Pendekatan yang digunakan memudahkan untuk mengakses dan melakukan evaluasi data ilmiah dalam jumlah besar. Berdasarkan hasil dan pembahasan analisis Google Scholar tahun 2020-2024 terhadap kata kunci "phishing" terbentuk tiga klaster dengan 14 kata kunci terkoneksi. Klaster pertama warna merah menunjukkan fokus pada kejahatan siber seperti phishing, cybercrime, dan sensitive information. Klaster kedua warna hijau berpusat pada whatsapp menekankan privacy dan data security yang umum menjadi tempat sasaran dalam kejahatan phishing. Klaster ketiga warna biru menyoroti ancaman keamanan dengan penerapan *cybersecurity*.

Berdasarkan analisis bibliometrik, *keyword* "phishing" pada penelitian yang terpublikasi memiliki hubungan yang sangat erat dengan keamanan dan Whatsapp. Terdapat penelitian yang menyoroti banyaknya kasus serangan phishing yang terjadi di whatsapp. Oleh karena itu, sosialisasi mengenai edukasi sangat penting dalam mengatasi ancaman kejahatan siber salah satunya phishing. Selain itu, juga menggambarkan kompleksitas dan dinamika keywords "phishing" dan relevansinya dalam konteks keamanan siber dan interaksi sosial [22].

UCAPAN TERIMA KASIH

Kami mengucapkan terimakasih yang sebesar-besarnya atas bimbingan, arahan, dan masukan dari Ibu Prof. Nur Aini Rahmawati selama proses penelitian dalam membimbing kami menyelesaikan penelitian dengan baik.

REFERENSI

[1]. Islamy, Imam T., et al. "Pentingnya Memahami Penerapan Privasi di Era Teknologi Informasi." *Jurnal Teknologi Informasi dan Pendidikan*, vol. 11, no. 2, 2018, pp. 21-28, doi:10.24036/tip.v11i2.137.

[2]. Chintia, Ervina & Nadiah, Rofiqoh & Nabila, Humayyun & Haedar, Zulfikar & Febriansyah, Adam & Rakhmawati, Nur. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal of Information Engineering and Educational Technology*., vol. 2. 65. 10.26740/jieet.v2n2.p65-69.

[3]. Greitzer, F.L.; Strozer, J.R.; Cohen, S.; Moore, A.P.; Mundie, D.; Cowley, J. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. *In Proceedings of the 2014 IEEE Security and Privacy Workshops*, San Jose, CA, USA, 17–18 May 2014; pp. 236–250.

[4]. F. Salahdine, Z. El Mrabet and N. Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," 2021 *IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*

(UEMCON), New York, NY, USA, 2021, pp. 0250-0255, 10.1109/UEMCON53757.2021.9666627.

[5]. Fan Z, Li W, Laskey KB, Chang K-C. "Investigation of Phishing Susceptibility with Explainable Artificial Intelligence". *Future Internet*. 2024; vol. 16, pp. 31. https://doi.org/10.3390/fi16010031

[6]. (2024) website idadx. [Online]. Available: https://idadx.id/

[7]. N. Donthu, S. Kumar, D. Pattnaik, dan W. M. Lim. "A bibliometric retrospection of marketing from the lens of psychology: Insights from Psychology & Marketing". *Psychol Mark*, vol. 38, Mei 2021, doi: 10.1002/mar.21472.

[8]. T. Tupan dan R. Rachmawati. "ANALISIS BIBLIOMETRIK ILMU DAN TEKNOLOGI PANGAN: PUBLIKASI ILMIAH DI NEGARA-NEGARA ASEAN". *Khizanah al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, vol. 6, no. 1, hlm. 26–40, 2018, doi: 10.24252/kah.v6a1a4.

[9]. Al-Dabi, S. S., & Al-Zarbani, S. S. (2021). Machine learning-based phishing detection systems: A survey. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51(12), 5674-5685.

[10]. Dehghani, S., & Banihashemi, A. (2020). A comprehensive survey on phishing detection: A machine learning perspective. *Journal of Computers in Engineering and Technology*, 13(1), 43-67.

[11]. Rogers, Everett, M. (2003). *Diffusions of Innovations; Fifth Edition*. Simon & Schuster Publisher.

[12]. Kesuma, Ulfa & Hidayat, Ahmad. (2020). Pemikiran Thomas S. Kuhn Teori Revolusi Paradigma. *Islamadina : Jurnal Pemikiran Islam*. 166. 10.30595/islamadina.v0i0.6043.

[13]. Sholiqah, S. N. A., Widyastuti, R. A., & Ratnawati, T. (2023). Peran *Artificial Intelligence* Untuk Mendeteksi Fraud Dalam Audit: Sebuah Studi Literatur. *Jurnal Riset Ekonomi dan Akuntansi*, 1(4), 226-238

[14]. Habsy, B. A. (2017). Seni memahami penelitian kualitatif dalam bimbingan dan konseling: studi literatur. *Jurnal Konseling Andi Matappa*, *1*(2), 90-100.

[15]. R. Riswano dan A. Rahmat. "Analisis Bibliometrik terhadap Tren Kompetensi untuk Green jobs pada Bidang Keahlian Pariwisata". *Jurnal Manajemen Perhotelan dan Pariwisata*, vol. 6, no. 2, 2023.

[16]. U. A. Bukar, M. S. Sayeed, S. F. Abdul Razak, S. Yogarayan, O. A. Amodu, dan R. A. Raja Mahmood. "A method for analyzing text using VOSviewer". *MethodsX*, Des 2023, doi: 10.1016/j.mex.2023.102339.

[17]. K. Khaeriyah, G. Wibisono, dan G. Pradini. "ANALISIS BIBLIOMETRIK PADA ACARA KONSER". *Turn Journal*, vol. 2, no. 2, hlm. 51–70, 2022.

[18]. U. Sahudi, Y. M. Saputra, A. Ma'mun, N. Nuryadi, dan D. Sofyan. "Co-Au-thorship and Co-Occurrence Bibliometric Analysis of the Scientific Literature on Social Capital and Sports". *Journal of Physical Education, Sport, Health, and Recreations*, vol. 11, no. 3, hlm. 133–140, 2022, [Daring]. Tersedia pada: http://journal.unnes.ac.id/sju/index.php/peshr

[19]. T. W. Widyaningsih, M. A. Dewi, dan A. Andrianingsih. "Analisis Bibliometrik untuk Memetakan Tren Penelitian Covid-19 dalam Topik Ilmu Komputer". *Techno.COM*, vol. 20, no. 3, hlm. 440–454, 2021, [Daring]. Tersedia pada: www.vosviewer.com.

[20]. R. Andrian. "*ANALISIS BIBLIOMETRIK : TREN TOPIK PENELITIAN PRODI PENDIDIKAN FISIKA DI BANDAR LAMPUNG*". Maret 2022.

[21]. F. N. Zakiyyah, Y. Winoto, dan R. Rohanda. "Pemetaan bibliometrik terhadap perkembangan penelitian arsitektur informasi pada Google Scholar menggunakan VOSviewer". *Informatio: Journal of Library and Information Science*, vol. 2, no. 1, hlm. 43, Jun 2022, doi: 10.24198/inf.v2i1.37766.

[22]. Sujiwana, R. K., Ridho, A. F. A., Aryanti, D. C., & Rakhmawati, N. A. (2024). Paper Dataset Regarding WhatsApp Phishing (1.0). Zenodo. [Daring]. Available: https://doi.org/10.5281/zenodo.11315156.