SYSTEMATIC LITERATURE REVIEW: SEKTOR SERANGAN SIBER DAN METODE PENDETEKSI SERANGAN SIBER PADA WEBSITE PELAYANAN PUBLIK DI KALIMANTAN TIMUR

Dimas Alameka

NPP. 30.0984

Asdaf Kota Samarinda, Provinsi Kalimantan Timur

Program Studi Teknologi Rekayasa Informasi Pemerintahan

Email: alamekadimas@gmail.com

Pembimbing Skripsi: Prof. Dr. Drs. Ismail Nurdin, M.Si

ABSTRACT

Problem/ Background*: The progress of the internet network is also experiencing very rapid development. with the development of the internet it also makes the use of websites even greater. Websites accessed by the public can be in the form of information websites, public services to transaction websites such as online stores and online banks. In line with that, the development of crime on the internet is also rampant* ***Purpose****: to find out and recommend methods of preventing and overcoming cyberattacks on websites.* ***Methods****: This research uses mixed methods. Where the mixed method is not balanced, primary methods and secondary methods. Primary methods are used to obtain the main data, while secondary methods are used to obtain data to support the data obtained from primary methods.* ***Results****: The results of this study can be seen that there are several cyberattacks on websites such as malware attacks which are frequent attacks. Furthermore, there are methods of preventing and overcoming cyberattacks such as machine learning which is the most effective method with a presentation of 98.5%.* ***Conclusion****: The most effective prevention method is machine learning which can detect cyberattacks with an accuracy rate of 98.25%. This is higher than other cyberattack prevention methods such as web security 5.30%, automatic protection datamining 75% and SCADA 94%.*

Keywords**:** *Countermeasures, Cyberattacks, Prevention, Systematic Literature Review, Website*

ABSTRAK

Pemasalahan : Kemajuan jaringan internet juga mengalami perkembangan yang sangat pesat. dengan perkembangan internet itu juga membuat penggunaan website semakin besar. *Website* yang diakses oleh masyarakat dapat berupa *website* informasi, pelayanan publik hingga website transaksi seperti toko *online* dan *bank online*. Sejalan dengan itu perkembangan dari kejahatan di internet juga merajalela. **Tujuan :** untuk mengetahui dan merekomendasikan metode pencegahan dan penanggulangan serangan siber pada *website*. **Metode :** Penelitian ini menggunakan metode mix methods. Dimana metode campuran tidak berimbang, metode primer dan metode sekunder. Metode primer digunakan untuk memperoleh data yang utama, sedangkan metode sekunder digunakan untuk memperoleh data guna mendukung data yang diperoleh dari metode primer. **Hasil :** Hasil pada penelitian ini dapat diketahui bahwa ada beberapa serangan siber pada website seperti serangan malware yang menjadi serangan yang sering terjadi. Selanjutnya ada metode pencegahan dan penanggulangan serangan siber seperti mechine learning dimana sebagai metode yang paling efektif dengan presentasi 98,5%. **Kesimpulan :** Metode pencegahan yang paling efektif yaitu Machine learning yang dapat mendeteksi serangan siber dengan tingkat akurasi 98.25%. Hal ini lebih tinggi dari metode pencegahan serangan siber lainnya seperti web security 5.30%, automatic protection datamining 75% dan SCADA 94%.

Kata kunci : Penanggulangan, Pencegahan, Serangan Siber, *Systematic Literature Review*, *Website*

I. Pendahuluan

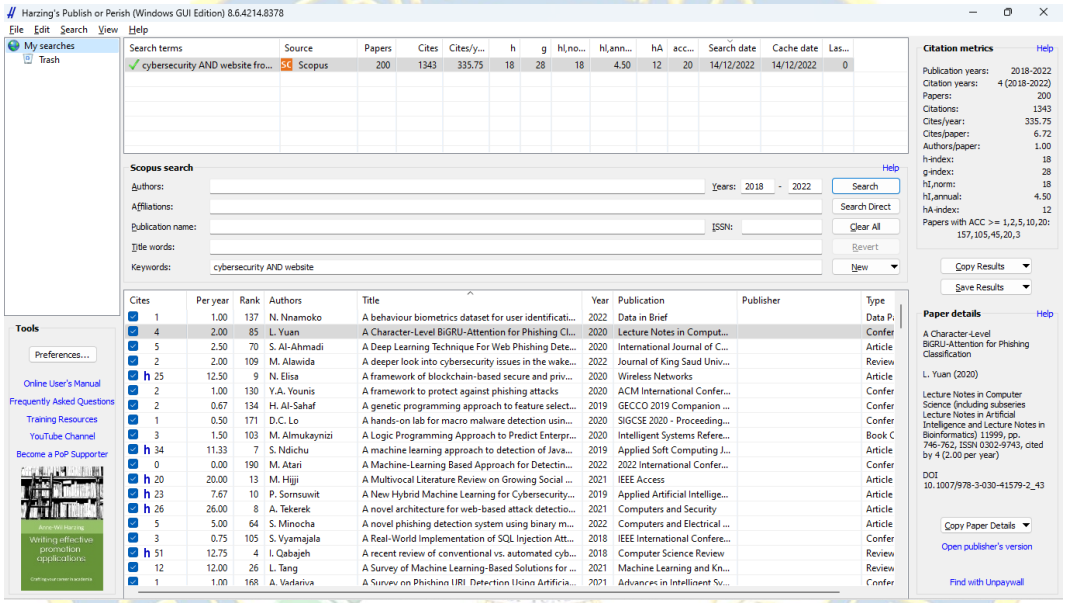
1.1 Latar belakang

Perkembangan teknologi sekarang mengalami kemajuan yang sangat pesat, bisa ditinjukkan dengan pertumbuhan teknologi seperti teknologi informasi yang sangat melesat maju dan terus mengalami perkembang dan perubahan dengan banyaknya teknologi - teknologi baru yang ditemukan sampai membuat pemikiran manusia yang sebelumnya tidak dapat dibayangkan bisa diwujudkan.

Selain dari perkembangan teknologi yang terjadi saat ini, kemajuan jaringan internet juga mengalami perkembangan yang sangat pesat. dengan perkembangan internet itu juga membuat penggunaan website semakin besar. Website yang diakses oleh masyarakat dapat berupa website informasi, pelayanan publik hingga website transaksi seperti toko online dan bank online. Oleh sebab itu, pengguna harus mengetahui awal terjadinya serangan siber hingga cara penanggulangan yang harus dilakukan.

Pada tahun 2022 terjadi kebocoran data penduduk, surat penting negara hingga berkas kasus-kasus yang kontrovesial yang terjadi di Indonesia. Sehingga pemerintah memberian perhatian khusus untuk menanggulangin kebocoran data dan keamanan sistem informasi khususnya berkaitan data yang bersifat rahasia baik pribadi hingga rahasia negara.

Banyaknya penelitian yang telah dilakukan oleh mahasiswa, dosen maupun peneliti yang menghasilkan penelitian berupa jurnal, skripsi, *thesis* maupun berbentuk makalah terkait dengan serangan siber pada *website* dengan rentang waktu 2018 - 2022. Hal ini dapat dilihat dari pencarian penelitian di dalam *Scopus* dan menggunakan *Publish or Perish* (PoP) mendapatkan sebanyak 200 penelitian yang telah dilakukan dan terdeteksi di *Scopus.*



Sumber : Diolah oleh penulis, 2023

Gambar 1.1 Hasil Pencarian Penelitian Menggunakan *Publish or Perish*

Dalam hal ini banyak literatur yang telah dipublikasikan tentang serangan siber maupun serangan siber pada *website*. Namun belum ada yang melakukan pengumpulan data penelitian, pemetaan tren penelitian dan evaluasi secara kritis, maka diperlukan penelitian menggunakan metode *systematic literature review*.

Systematic literature review serangan siber pada *website* ini penting dilakukan, karena dalam mengetahui pemetaan tren penelitian dari tahun 2018 hinga 2022, sektor serangan siber, metode yang dilakukan dalam mendeteksi serangan siber pada *website* dan cara mendeteksi serta mengantisipasi serangan siber pada *website* diperlukan pemahaman yang lebih luas dan data yang akurat dari beberapa penelitian dengan cara mengidentifikasi, menafsirkan, dan mengkaji hasil penelitian tersebut.

1.2 Kesenjangan Masalah yang Diambil

Perkembangan teknologi terkususnya perkembangan internet tidak sejalan dengan penanganan kejahatan yang terjadi. Hal ini dibuktikan dengan pada tahun 2022 terjadi kebocoran data penduduk, surat penting negara hingga berkas kasus-kasus yang kontrovesial yang terjadi di Indonesia. Sehingga diperlukan penelitian yang membahas metode pencegahan dan penanggulangan serangan siber terkhususnya pada sektor website pelanan publik milik pemerintah provinsi Kalimantan Timur.

1.3 Penelitian Terdahulu

Penelitian ini terinspirasi oleh beberapa penelitian terdahulu. Penelitian Tan dan Soewijo berjudul Manajemen Risiko Serangan Siber Menggunakan Framework Nist Cybersecurity di Universitas ZXC (Tan & Soewito, 2022) menemukan Kondisi keamanan siber di lingkungan Universitas ZXC masih belum mencapai standar yang direkomendasikan. Hal ini ditunjukan melalui hasil penilaian aplikasi Nessus yang menunjukan kondisi cela pada sistem

layanan web dan situs web yang cukup banyak. Penelitian Herdiana dkk yang berjudul Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19 (Herdiana et al., 2021) disampaikan beberapa teknik untuk mendeteksi serangan siber dan cara menghindari serangan siber saat Covid-19 bahkan setelahnya sehingga kejahatan siber dapat berkurang. Penelitian Putra berjudul Design Integrated Honeypot Untuk Deteksi dan Identifikasi Serangan Siber (Putra et al., 2019) dari penelitiannya menghasilkan implementasi aplikasi glastopf, dionaea dan honeypot. Hasil dari implementasi tersebut memberikan cara identifkas dan mendeteksi serangan siber khususnya serangan malware dan memudahkan administrator dalam memantau keadaan sistem. Penelitian Anggono berjudul Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis (Anggono et al., 2021) Memberikan gambaran cybercrime dan cybersecurity pada fintect. Penelitian Parulian berjudul Ancaman dan Solusi Serangan Siber di Indonesia (Parulian et al., 2021) menemukan Peningkatan ancaman siber sebesar 6,15% yang terjadi di Indonesia dari tahun 2020 s/d 2021, ancaman yang sering terjadi di antaranya serangan Denial of Service (Dos) Attack yang berupa serangan synflood dan ICMP flood, phising, serta pencurian data pribadi.

1.4 Pernyataan Kebaruan Ilmiah

Penulis melakukan penelitian yang berbeda dan belum dilakukan oleh penelitian terdahulu, dimana konteks penelitian yang dilakukan yakni menemukan metode pencegahan dan penanggulangan serangan siber pada website dan memberikan masukkan atau rujukan untuk dapat diimplementasikan kedalam sektor pemerintah (pelayanan publik berbasis internet).

1.5 Tujuan

Tujuan ini difokuskan terhadap sasaran yang ingin dicapai oleh penulis. Tujuan dari penulisan ini untuk mengetahui dan memberikan rekomendasi metode-metode dalam melakukan pencegahan dan penanggulangan serangan siber pada website pelayanan publik.

II Metode

Penelitian ini menggunakan pendekatan *mixed methods*. Menurut Sugiyono (Sugiyono, 2017:404), metode penelitian *mixed methods* merupakan "Metode penelitian kombinasi adalah suatu metode penelitian yang mengkombinasikan atau menggabungkan antara metode kuantitatif dan metode kualitatif untuk digunakan secara bersama-sama dalam suatu kegiatan penelitian, sehingga diperoleh data yang lebih komprehensif, valid, reliabel, dan objektif".

Metode penelitian yang digunakan dalam penelitian ini adalah metode campuran tidak berimbang (concurrent embedded design). Sugiyono (Sugiyono, 2011 : 412) mengemukakan bahwa “metode campuran tidak berimbang (concurrent embedded design) adalah metode penelitian yang mengkombinasikan penggunaan metode penelitian kuantitatif dan kualitatif secara simultan atau bersama-sama, tetapi bobot metodenya berbeda”. Pada metode ini terdapat metode primer dan metode sekunder. Metode primer digunakan untuk memperoleh data yang utama, sedangkan metode sekunder digunakan untuk memperoleh data guna mendukung data yang diperoleh dari metode primer.

Penelitian ini menggunakan model primer yaitu kuantitatif *Systematic literature review*. *Systematic literature review* adalah memaparkan data secara sistematis untuk mengumpulkan data penelitian, mengevaluasi secara kritis, mengintegrasikan dan menyajikan temuan dari beberapa studi penelitian, serta menyediakan tahapan untuk menilai tingkat kualitas data sebagai bukti yang ada pada rumusan masalah (Delgado-Rodríguez & Sillero-Arenas, 2018), serta metode kualitatif sebagai model sekunder.

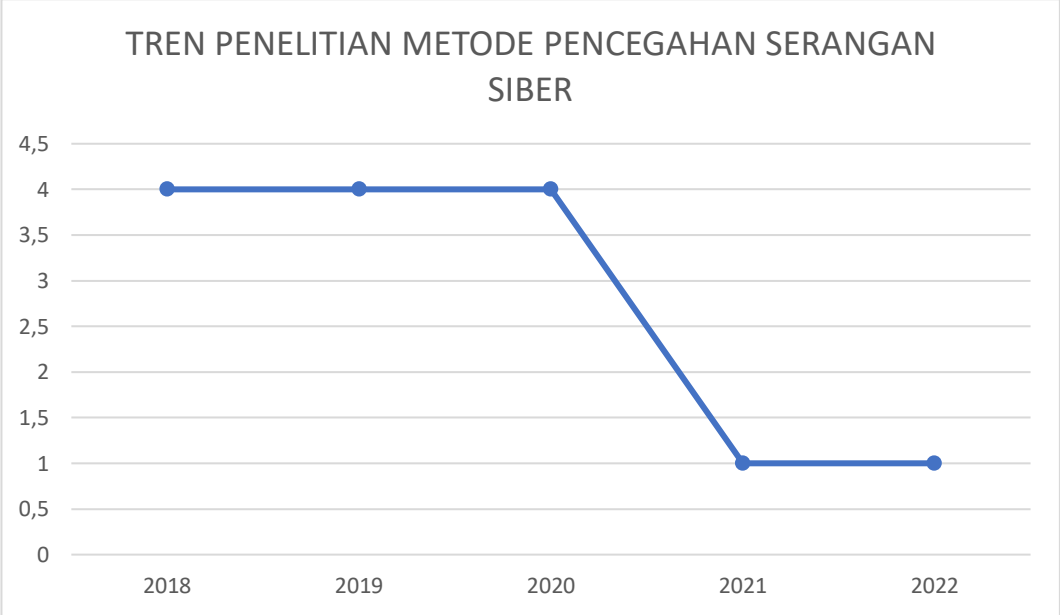
III Hasil dan Pembahasan

Data yang didapatkan yang berupa literature terindeks scopus sebanyak 67 literature sesuai dengan kata kunci dan dengan rentang waktu 2018 – 2022 dan literature tersebut dicari menggunakan aplikasi Publish or Perish (PoP). Provinsi Kalimantan Timur memberikan tugas kepada Dinas Komunikasi dan Informatika Kalimantan Timur untuk mengatur, mencegah dan

menangani seranga siber di lingkungan Pemerintahan Kalimantan Timur. Didalam Dinas Komunikasi dan Informatika Kalimantan Timur memiliki Seksi Keamanan Informasi dan Persandian yang memiliki tugas melakukan pengumpulan dan penyiapan bahan perumusan kebijakan, koordinasi, pembinaan, pengaturan teknis dan pengendalian yang meliputi keamanan informasi dan persandian.

3.1 Tren Penelitian Serangan Siber Pada Website

Sebanyak empat belas literatur yang sesuai dengan permasalahan dalam penelitian ini. Dilihat dari tahun publikasi dari literatur tersebut mendapatkan selanjutnya dianalisis menggunakan aplikasi *Vosviewer* untuk melihat visualisasi data.



Sumber : Diolah oleh penulis, 2023

Gambar 3.1 Tren Penelitian Metode Pencegahan Serangan Siber

Pada tahun 2018 hingga 2020 publikasi penelitian yang mengangkat topik pencegahan serangan siber sebanyak 4 publikasi, sedangkan pada tahun 2021 hingga 2022 mengalami penurunan yang hanya ada satu publikasi tiap tahunnya.

Sumber : Diolah oleh penulis, 2023

Gambar 3.2 Hasil Visualisasi Data Menggunakan *Vosviewer*

Hasil visualisasi data menggunakan aplikasi *Vosviewer* dapat kita lihat bahwa terdapat 4 cluster yang terindentifikasi yang terdiri dari *information security, malware, cybercrime* dan *mechine learning.* Hal ini didapatkan dari hasil kejadian bersama (*co- occurrence*) untuk menjawab tema umum penelitian mengenai *cybercrime* (serangan siber).

3.2 Sektor yang Menjadi Target Serangan Siber

Sektor yang menjadi target serangan siber diantaranya yaitu Kesehatan, Keuangan, Jasa, Pendidikan, Ilmu Pengetahuan Hayati,Teknologi, Ritel, Komunikasi, Industri, Konsumen Energi, Hiburan, Perhotelan, Transportasi, Media,Penelitian, Sektor Publik. Selanjutnya sektor yang memiliki intensitas tinggi dilakukannya penyerangan yaitu disektor kesehatan, diposisi kedua yaitu sektor keuangan dan yang ketiga yaitu disektor pendidikan (Paul & Zhang, 2021). Hal ini berbanding terbalik dari kejadian yang ada di Indonesia pada tahun 2021. Di Indonesia yang menjadi peringkat pertama yang menjadi sektor yang sering dilakukan serangan siber yaitu pada sektor pendidikan sebanayak 2.217 kasus. Pada posisi kedua ditempati oleh sektor swasta sebanyak 1.483 kasus serta pada posisi ketiga terdapat di sektor pemerintahan daerah sebanyakan 1.097 kasus (BSSN, 2021).

Provinsi Kalimantan Timur juga terkena serangan siber pada tahun 2022, terkhususnya pada sektor pemerintahan, swasta dan individu. Berikut data sektor yang terkena serangan siber di Kalimantan Timur :

Tabel 3.1 Sektor Serangan Siber

No	Sektor	Jumlah (serangan)
1	Pemerintahan	48.755
2	Swasta	21.742
3	Individu	2.137

Sumber : Diolah oleh penulis, 2023

3.3 Jenis Serangan Siber yang Sering Terjadi

Jenis serangan siber yang sering terjadi dalam rentang waktu maret 2020 sampai desember 2021 dalam urutan pertama ditempati oleh hacking dengan jumlah 330 kali penyerangan. Ditempat kedua diisi oleh spam email dengan jumlah 250 kali penyerangan dan ditempat ketiga ditempati oleh malicious domain (Alawida et al., 2022). Akan tetapi hal ini terjadi saat terjadinya wabah Covid-19.

Pada negara indonesia, serangan siber yang sering terjadi yaitu malware. Serangan malware yang terjadi pada tahun 2020 berjenis trojan yang seringkali berbentuk program ataupun file yang dapat mengakibatkan kebocoran data pengguna, malware ini melakukan penyerangan sebanyak 72.247.625 kali penyerangan (BSSN, 2020), serta pada tahun 2021 terjadi serangan malware mylobot botnet melakukan penyerangan sebanyak 730.946.448 kali (BSSN, 2021). Malware ini dirancang untuk pengiriman spam, pencurian data, *ransomeware*. *fraud, Denial-of-Service (DoS)*, dan lain-lain.

Provinsi Kalimantan Timur masih terjadi serangan siber dari para peretas. Hal yang dilakukan pada tahun 2022 oleh peretas yaitu *captcha-web, common web attack, port honey pot*. Berikut data jenis serangan siber di Kalimantan Timur :

Tabel 3.2 Jenis Serangan Siber di Kalimantan Timur

No	Jenis serangan	Jumlah (serangan)
1	*Captcha-Web*	40.432
2	*Common Web Attack*	1324
3	*Port Honey Pot*	1223

Sumber: Laporan Tahunan Monitoring Keamanan Siber Kalimantan Timur 2022

3.4 Metode Mendeteksi Serangan Siber Pada Website

Banyak metode yang dapat digunakan untuk mendeteksi serta mencegah serangan siber. Diantaranya yaitu dengan memasang aplikasi *anti-phising* seperti *McAfee, Google, Microsoft, were proposed. For instance, The Anti-Phishing Explorer 9, McAfee Site Advisor,* dan *Google Safe Base* (Qabajeh et al., 2018), *software* anti-spam, antimalware dan *antivirus* (Alawida et al., 2022), *xss and fuzzy, Web security, Machine learning, Automatic protection, data mining, SCADA* (Divya & Malathi, 2018). Selain itu melakukan pengamanan pencegahan seperti, penetration test, security patch management, dynamic scanning, static scanning, educate developers on safe coding, dan lain- lain (Paul & Zhang, 2021).

Monitoring keamanan siber pada Diskominfo Kaltim dilakukan berdasarkan hasil pantauan alat deteksi Host IDS (Intrusion Detection System) yang terpasang di 15 virtual server milik Pemerintah Provinsi Kalimantan Timur. Diskominfo sudah melakukan aksi pencegahan seperti peningkatan firewall, memblokir situs yang dianggap berbahaya serta rutin melakukan scanning pada *database* diskominfo Kalimantan Timur.

3.5 Metode Pencegahan yang Efektif Dalam Mendeteksi dan Mengantisipasi Serangan Siber

Metode pencegahan yang paling efektif yaitu *Machine learning* yang dapat mendeteksi serangan siber dengan tingkat akurasi 98.25%. Hal ini lebih tinggi dari metode pencegahan serangan siber lainnya seperti XXS dan fuzzy 97.10%, web security 5.30%, automatic protection datamining 75% dan SCADA 94% (Divya & Malathi, 2018).

3.6 Diskusi Temuan Utama Penelitian

Berdasarkan pengamatan yang dilakukan penulis ditemukan beberapa temuan yaitu di Pemerintahan Kalimantan Timur belum menerapan metode yang efektif dalam mencegah dan menanggulangi serangan siber. Hal ini dapat dilihat dari kurang terpenuhinya 5 indikator penulis akan membahas secara mendalam terkait Sektor Serangan Siber Dan Metode Pendeteksi Serangan Siber Pada Website Pelayanan Publik di Kalimantan Timur. Adapun teori yang akan diuraikan Teori penerapan *E- Government* oleh Indrajit (Indrajit, 2016) dengan dimensi *support, capacity, value*

IV Kesimpulan

Penarikan kesimpulan dilakukan pada akhir melakukan penelitian yang bertujuan untuk mengetahui secara keseluruhan dari sebuah penelitian yang telah dilakukan. Adapun kesimpulan yang diambil oleh peneliti sebagai berikut :

Tren penelitian tentang metode pencegahan serangan siber dari tahun 2018 – 2022 mengalami penurunan pada dua tahun terakhir. Pada tahun 2018 hingga 2020 publikasi penelitian yang mengangkat topik pencegahan serangan siber sebanyak 4 publikasi, sedangkan pada tahun 2021 hingga 2022 mengalami penurunan yang hanya ada satu publikasi tiap tahunnya.

Sektor yang sering diserang oleh serangan siber dari tahun 2018 hingga 2022 di negara Indonesia yaitu peringkat pertama yang menjadi sektor yang sering dilakukan serangan siber yaitu pada sektor pendidikan sebanayak 2.217 kasus. Pada posisi kedua ditempati oleh sektor swasta sebanyak 1.483 kasus serta pada posisi ketiga terdapat di sektor pemerintahan daerah sebanyakan 1.097 kasus. Sedangkan di Provinsi Kalimantan Timur juga terkena serangan siber pada tahun 2020-2022, terkhususnya pada sektor pemerintahan, swasta dan individu.

Jenis serangan siber yang sering terjadi pada website Pada negara indonesia, serangan siber yang sering terjadi yaitu malware. Serangan malware yang terjadi pada tahun 2020 berjenis trojan yang seringkali berbentuk program ataupun file yang dapat mengakibatkan kebocoran data pengguna, malware ini melakukan penyerangan sebanyak 72.247.625 kali penyerangan, serta pada tahun 2021 terjadi serangan malware mylobot botnet melakukan penyerangan sebanyak 730.946.448 kali. Malware ini dirancang untuk pengiriman spam, pencurian data, ransomeware. fraud, Denial-of-Service (DoS), dan lain-lain. Pada pemerintah Provinsi

Kalimantan Timur, jenis serangan siber yang sering terjadi yaitu sql injection, malware serta konten negatif dihalaman website.

Metode yang digunakan untuk mendeteksi serangan siber pada website di Perintahan Provinsi Kalimantan Timur yang diwakili oleh Dinas Komunikasi dan Informatika Kalimantan Timur sebagai garda terdepan dalam melakukan pencegahan dan penyelesaian masalah serangan siber. Melakukan serangkaian pencegahan seperti rutin melakukan scanning pada database diskominfo, serta rangkaian pencegahan lainnya seperti peningkatan firewall.

Metode pencegahan yang paling efektif yaitu Machine learning yang dapat mendeteksi serangan siber dengan tingkat akurasi 98.25%. Hal ini lebih tinggi dari metode pencegahan serangan siber lainnya seperti web security 5.30%, automatic protection datamining 75% dan SCADA 94%

Keterbatasan Penelitain. penelitian memiliki keterbatasan utama yakni waktu dan biaya penelitian. Penelitian juga hanya dilakukan pada satu Lokus sebagai studi kasus yakni di Provinsi Kalimantan Timur.

Arah Masa Depan. Penulis menyadari masih awalnya temuan penelitian oleh karena itu penulis menayarankan untuk menggunakan metode pencegahan dan penanggulangan serangan siber pada website yang efektif dalam sektor pemerintah dikarenakan sektor pemerintah menjadi sektor terpenting dalam memberikan pelayanan publik kepada masyarakan dan terciptanya pelayanan publik berbasis internet yang aman dan nyaman.

V Ucapan Terima Kasih

Bapak Dr. Hadi Prabowo, M.M selakui Rektor Institut Pemerintahan Dalam Negeri,Bapak Dr. Halilul Khairi, M.Si selaku Dekan Fakultas Manajemen Pemerintahan Institut Pemerintahan Dalam Negeri, Bapak Dr. Megandaru Widhi K., S.IP, M.Si selaku Kepala Program Studi Teknologi Rekayasa Informasi Pemerintahan Institut Pemerintahan Dalam Negeri, Bapak Agung Nurrahman., S.STP, M.PA selaku Sekretaris Program Studi Teknologi Rekayasa Informasi Pemerintahan Institut Pemerintahan Dalam Negeri, Bapak Prof. Dr. Drs. Ismail Nurdin, M.Si selaku Dosen Pembimbing yang selama ini memberikan bimbingan serta mengarahkan penyusunan proposal skripsi ini, Seluruh Dosen Pengajar, Pelatih, Pamong Pengasuh, dan juga Civitas Akademika IPDN yang telah memberikan jasa serta dedikasinya dalam pembelajaran selama melaksanakan pendidikan,Segenap keluarga besar Kontingen Kalimantan Timur, kakak angkatan XXIX, dan adik-adik angkatan XXXI dan XXXII yang selalu membantu dan memberikan semangat, khususnya Saudara Kontingen angkatan XXX yang telah menjadi keluarga kedua, Segenap Saudara Kelas G-3, wisma Sumatera Utara Atas yang selalu mendengar keluh kesah peneliti,Semua pihak yang tidak bisa disebutkan satu persatu, atas seluruh bantuan, dukungan serta doa yang diberikan.

VI Daftar Pustaka

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Anggono, A., Tarjo, & Riskiyadi, M. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Manajemen Dan Organisasi*, *12*(3), 239–251. https://doi.org/https://doi.org/10.29244/jmo.v12i3.33528

BSSN. (2020). *LAPORAN TAHUNAN HASIL MONITORING KEAMANAN SIBER 2020*.

BSSN. (2021). *LAPORAN TAHUNAN HASIL MONITORING KEAMANAN SIBER 2021*.

Delgado-Rodríguez, M., & Sillero-Arenas, M. (2018). Systematic review and meta-analysis. *Medicina Intensiva (English Edition)*, *42*(7), 444–453. https://doi.org/10.1016/j.medine.2017.10.012

Divya, S., & Malathi, S. (2018). Preventing web Application to avoid Illegal Entry of Hackers-a Review. In *Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018* (pp. 183–187). https://doi.org/10.1109/CESYS.2018.8723945

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Information Communication & Technology*, *21*(1), 42–52.

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies*, *1*(2), 85–92.

Paul, J. A., & Zhang, M. (2021). Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker. *European Journal of Operational Research*, *291*(1), 349–364. https://doi.org/10.1016/j.ejor.2020.09.013

Putra, I. A., Dewi, M. A. R., & Sulistyo. (2019). DESIGN INTEGRATED HONEYPOT UNTUK DETEKSI DAN IDENTIFIKASI SERANGAN SIBER. *IT*, *10*(3). https://doi.org/10.37639/jti.v10i3.141

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. In *Computer Science Review* (Vol. 29, pp. 44–55). https://doi.org/10.1016/j.cosrev.2018.05.003

Sugiyono. (2011). *Metode Penelitian Kombinasi (Mixed Methods)*. Alfabeta.

Sugiyono. (2017). *Metode Penelitian Kuantitatif, Kualitatif, dan Kombinasi (Mixed Methods)* (2nd ed.). CV. Alfabeta.

Tan, T., & Soewito, B. (2022). *MANAJEMEN RISIKO SERANGAN SIBER MENGGUNAKAN FRAMEWORK NIST CYBERSECURITY DI UNIVERSITAS ZXC*. *6*(2), 411–422. https://doi.org/10.52362/jisamar.v6i2.781