KOMPID
KUMPULAN ILMU KOMPUTER DAN PERUBAHAN DIGITAL

JURNAL **KUMPULAN ILMU KOMPUTER DAN PERUBAHAN DIGITAL**
Vol. 1 No. 1 Bulan Juni Tahun 2025
P-ISSN - | E-ISSN -

ANALISIS DAMPAK RANSOMWARE PADA KEAMANAN DATA PERUSAHAAN DAN STRATEGI MITIGASINYA

Raka Gian Aditya Asbath[1], Ilpan[2], Rio Putra Anugrah[3], Awan Setiawan[4]
rakagian107@gmail.com[1], ilpancengbeng@gmail.com[2], rioputraanugrah90@gmail.com[3], awans2425@gmail.com[4]
Universitas Langlangbuana

ABSTRAK

Penelitian ini mengeksplorasi dampak serangan ransomware terhadap keamanan data perusahaan dan mengevaluasi strategi mitigasi yang ada. Ancaman ransomware telah menjadi perhatian utama di era digital, yang menyebabkan kerugian finansial dan pelanggaran data di berbagai sektor. Penelitian ini mengumpulkan data dari tinjauan literatur dan laporan industri menggunakan pendekatan kualitatif dengan metode deskriptif. Penelitian ini menemukan bahwa serangan ransomware dapat menyebabkan gangguan operasional, kehilangan data, dan kerugian finansial. Penyerang mengeksploitasi teknologi enkripsi, mata uang kripto, dan ketersediaan kode ransomware yang tersebar luas untuk memeras korbannya. Strategi mitigasi yang efektif termasuk menggunakan kecerdasan buatan untuk deteksi dan respons proaktif, pencadangan data secara teratur, dan edukasi keamanan digital. Studi ini menyimpulkan bahwa penerapan kecerdasan buatan dalam strategi mitigasi dapat secara signifikan mengurangi dampak dan risiko serangan ransomware. Penelitian ini berkontribusi dalam memahami dampak ransomware dan memberikan rekomendasi untuk meningkatkan keamanan data perusahaan.

Kata kunci : Ransomware; Keamanan Data; Kecerdasan Buatan; Strategi Mitigasi; Enkripsi.

ABSTRACT

This research explores the impact of ransomware attacks on corporate data security and evaluates existing mitigation strategies. The threat of ransomware has become a major concern in the digital age, causing financial losses and data breaches in various sectors. This research collected data from literature reviews and industry reports using a qualitative approach with descriptive methods. The research found that ransomware attacks can cause operational disruption, data loss and financial loss. Attackers exploit encryption technology, cryptocurrencies and the widespread availability of ransomware code to extort their victims. Effective mitigation strategies include using artificial intelligence for proactive detection and response, regular data backup, and digital security education. The study concluded that the application of artificial intelligence in mitigation strategies can significantly reduce the impact and risk of ransomware attacks. This research contributes to understanding the impact of ransomware and provides recommendations to improve enterprise data security.

Keywords : *Ransomware, Data Security, Artificial Intelligence, Mitigation Strategies, Encryption.*

1. PENDAHULUAN

Pendahuluan Dalam era digital saat ini, tantangan terhadap keamanan digital semakin meningkat. Salah satu ancaman terbesar dalam dunia keamanan siber saat ini adalah serangan ransomware. Ransomware merupakan jenis malware yang mengenkripsi atau mencuri data digital dan meminta tebusan finansial dari korban untuk melepaskan atau mengembalikannya. Jenis target yang menjadi korban serangan ini dari pemerintah federal hingga pemerintah kota, dan dari perusahaan swasta hingga warga negara menunjukkan bahwa ransomware harus mendapatkan perhatian ilmiah yang lebih besar dari para ilmuwan sosial.

Salah satu kasus yang menggemparkan di Indonesia adalah serangan yang terjadi pada Pusat Data Nasional(PDN). Merujuk Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem

Pemerintahan Berbasis Elektronik (SPBE), disebutkan bahwa PDN merupakan fasilitas yang digunakan atau berfungsi untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan, pengolahan, dan pemulihan data bagi Instansi Pusat dan Pemerintah Daerah. Data yang disimpan oleh PDN meliputi berbagai jenis data dari berbagai sektor yang digunakan untuk mendukung tata kelola pemerintahan, kebijakan publik, dan pelayanan masyarakat. Dengan demikian, dapat disimpulkan data yang termasuk di PDN adalah data penting milik seluruh instansi pemerintahan yang menggunakan PDN sebagai tempat penyimpanan, pengolahan, dan pemulihan data.

Studi sebelumnya telah mempelajari berbagai aspek ransomware dan bagaimana hal itu berdampak pada keamanan data perusahaan. Salah satu contohnya adalah penelitian Ransomare yang bertujuan untuk memahami ancaman keamanan digital ransomware [1]. Selain itu, penelitian lain menemukan metode keamanan sistem informasi untuk melawan serangan ransomware [2].

Selain itu, penelitian ini memberikan ulasan menyeluruh tentang ancaman ransomware dan metode deteksi terbaru. Penulis membahas bagaimana ransomware telah membuat ekosistem cybercriminal yang berbeda, didukung oleh elemen seperti teknologi enkripsi, mata uang kripto, dan kemudahan mendapatkan kode ransomware. Memberikan pemahaman mendalam tentang proses serangan ransomware, siklus hidup serangan ransomware dijelaskan dalam 7 tahap. Selain itu, jurnal ini membahas berbagai jenis ransomware, termasuk locky dan crypto, serta bagaimana mereka diatur [3].

Artikel ini menawarkan kontribusi baru dalam literatur dengan menggabungkan analisis dampak ransomware pada keamanan data perusahaan dan strategi mitigasi yang lebih holistik Dengan demikian, artikel ini tidak hanya memberikan pemahaman mendalam tentang bagaimana ransomware mempengaruhi perusahaan, tetapi juga menawarkan solusi inovatif untuk mengurangi risiko dan dampaknya.

Penelitian ini berangkat dari pertanyaan utama: "Bagaimana dampak serangan ransomware terhadap keamanan data perusahaan dan strategi mitigasi apa yang paling efektif dalam menghadapi ancaman ini?" Hipotesis yang diajukan adalah bahwa penggunaan teknologi kecerdasan buatan dalam strategi mitigasi dapat secara signifikan mengurangi dampak dan risiko serangan ransomware pada perusahaan.

Tujuan dari artikel ini adalah untuk menganalisis dampak serangan ransomware pada keamanan data perusahaan serta mengevaluasi efektivitas berbagai strategi mitigasi yang ada. Secara khusus, artikel ini bertujuan untuk mengidentifikasi dan mengusulkan strategi mitigasi yang inovatif dan efektif, termasuk penggunaan teknologi kecerdasan buatan, untuk membantu perusahaan melindungi diri dari ancaman ransomware.

2. METODE PENELITIAN

Pendekatan kualitatif dan metode deskriptif digunakan dalam penelitian ini untuk mendeskripsikan fenomena yang ada, baik alam maupun buatan manusia, atau untuk menganalisis atau mendeskripsikan hasil subjek, tetapi tidak dimaksudkan untuk memberikan implikasi yang lebih luas [4]. Bentuk, aktivitas, karakteristik, perubahan, hubungan, kesamaan, dan perbedaan fenomena dapat termasuk dalam kategori ini [5].

Data dalam penelitian ini dikumpulkan melalui studi literatur. Studi literatur dilakukan dengan menelaah berbagai publikasi ilmiah, laporan industri, dan dokumen terkait yang membahas tentang ransomware, dampaknya, dan strategi mitigasinya. Sumber-sumber ini dipilih berdasarkan relevansi dan kredibilitasnya dalam memberikan informasi yang komprehensif dan terkini mengenai topik penelitian.

3. HASIL DAN PEMBAHASAN

A. Ransomware

Ransomware adalah jenis perangkat lunak berbahaya yang digunakan oleh penjahat siber untuk membobol komputer dan kemudian mengenkripsi file sehingga orang yang berwenang tidak dapat mengaksesnya lagi. Setelah file dienkripsi, pelaku ancaman diberi ketentuan untuk membayar tebusan sebagai imbalan untuk kunci yang dapat mendekripsi file. Namun, dalam beberapa kasus, pelaku ancaman mungkin tetap tidak memberikan akses ke file [6].

Serangan ransomware menggunakan berbagai strategi yang dapat mengunci komputer atau mengenkripsi data, membuatnya sulit untuk dihapus oleh ahli komputer. Selain itu, mereka memiliki

kemampuan untuk mengambil data pribadi dari komputer dan sistem jaringan korban. Ransomware dapat menyerang PC individu, sistem komersial, dan sistem kontrol industri, termasuk data dan perangkat lunak di dalamnya [7].

B. Tipe-tipe Ransomware

Meskipun berpengaruh pada semua industri, ransomware sangat efektif pada perusahaan pemerintah, penerbangan, dan kedirgantaraan. Serangan ransomware menjadi semakin kompleks dan meluas, sehingga sulit untuk mengikuti instruksi yang terus berkembang yang menjelaskan perangkat lunak berbahaya ini. Tiga jenis utama ransomware adalah ransomware pengunci layar, ransomware pengenkripsi file data, dan ransomware pemerasan ganda [3].

1. Ransomware Pengunci Layar
   Jenis ransomware ini tidak mengenkripsi file atau folder korban; sebaliknya, mengunci antarmuka sehingga menghalangi korban untuk menggunakan sistem secara keseluruhan. Ransomware jenis ini kemudian meminta pembayaran untuk mendapatkan akses kembali. Meskipun jenis ransomware ini tidak berusaha untuk mengenkripsi file atau data, sistem komputer tetap terkunci setelah mesin dipaksa untuk dihidupkan kembali[6].
2. Ransomware Enkripsi
   Ransomware yang mengenkripsi file data akan menginfeksi perangkat korban dengan mengenkripsi file dan folder penting. Setelah item dikunci dan dienkripsi, notifikasi akan muncul yang menyatakan bahwa Anda harus membayar sejumlah uang untuk membuka data yang dikunci[2].
3. Ransomware *Double Extorition*
   Ransomware pemerasan ganda menghancurkan file korban dan mengekstrak data dalam jumlah besar sebelum dienkripsi pada tahap akhir serangan. Korban yang menolak tuntutan pembayaran akan melihat informasi pribadi mereka tersebar luas di Internet [8]. Operator tambahan melakukan tugas tambahan, seperti identifikasi korban dan pengiriman biner ransomware.

C. Pemicu Serangan Ransomware

Karena tindakan fasilitatif dari beberapa pemungkin, serangan ransomware telah berkembang baik dalam frekuensi maupun jenisnya. Ini adalah kemungkinan besar karena kemajuan teknologi dan perubahan gaya hidup [3].

1. Teknologi Enkripsi
   Privasi memanfaatkan enkripsi. Sejumlah besar data dikirim melalui internet saat ini, yang sangat bergantung pada internet. Namun, data ini dapat disadap dengan mudah. Oleh karena itu, teknologi enkripsi dibuat untuk memastikan bahwa data hanya dapat dibaca oleh orang yang ditunjuk. Teknologi ini telah menunjukkan bahwa itu memiliki banyak manfaat. Teknologi ini digunakan oleh ransomware untuk mengenkripsi file korban untuk tujuan pemerasan. Terdapat tiga jenis teknologi enkripsi yang umum digunakan oleh ransomware: enkripsi simetris, enkripsi asimetris, dan enkripsi hibrida [3].
2. Mata Uang Dunia Maya
   Pembayaran utama untuk tebusan adalah mata uang virtual. Ini terutama disebabkan oleh fakta bahwa uang ini memungkinkan penerima untuk mempertahankan identitas anonim di hadapan pihak berwenang. Mata uang siber seperti Bitcoin telah menjadi populer. Hal ini benar, terutama karena toko online yang menerima mata uang dunia maya semakin populer. Teknologi rantai blok adalah jenis enkripsi tambahan yang menggunakan fungsi hash satu arah. Ini adalah alat penting dalam metode pembayaran mata uang dunia maya untuk menjamin kredibilitas mata uang [9].
3. Aksesibilitas Ransomware
   RaaS membuatnya mudah mendapatkan kode ransomware. Selain itu, orang-orang yang tidak terbiasa dapat mengakses kit pengembangan gratis seperti Torlocker, TOX, dan Hidden Tear. Ini secara signifikan mengurangi pintu masuk ransomware[10].

D. Pencegahan Ransomware

Ransomware merupakan ancaman serius dalam dunia digital yang dapat menyebabkan kerugian finansial dan kerugian data yang signifikan. Oleh karena itu, penting bagi individu dan organisasi untuk mengambil langkah-langkah pencegahan guna melindungi diri mereka dari serangan ransomware. Beberapa langkah yang dapat diambil untuk mengantisipasi ransomware.

Penerapan langkah-langkah pencegahan dapat membantu individu dan organisasi untuk mengurangi risiko terhadap serangan ransomware. Namun, penting juga untuk tetap waspada dan mengikuti perkembangan terkini dalam keamanan digital guna memastikan perlindungan yang optimal. Untuk mengantisipasi serangan ransomware, berikut adalah beberapa langkah pencegahan yang dapat diambil :

1. Backup data secara teratur: Lakukan pencadangan data penting secara teratur ke lokasi yang terpisah dan aman, seperti penyimpanan eksternal atau cloud. Pastikan pencadangan dilakukan secara otomatis dan diverifikasi keabsahannya. Dengan melakukan ini, Anda memiliki salinan data yang dapat dipulihkan jika terjadi serangan ransomware.
2. Perbarui perangkat lunak dan sistem operasi: Pastikan sistem operasi, perangkat lunak aplikasi, dan perangkat keras yang digunakan selalu diperbarui dengan rilis terbaru. Perbarui secara teratur agar kerentanan yang diketahui dapat diperbaiki dan mencegah eksploitasi yang memungkinkan ransomware masuk.
3. Gunakan solusi keamanan yang kuat: Instal perangkat lunak keamanan yang terpercaya, seperti antivirus, antispyware, dan firewall. Pastikan perangkat lunak ini diperbarui secara teratur dengan definisi virus terbaru untuk mendeteksi dan menghalangi ancaman ransomware.
4. Waspadai email dan tautan yang mencurigakan: Jangan mengklik tautan atau membuka lampiran yang mencurigakan dalam email yang tidak dikenal atau tidak diharapkan. Verifikasi sumber email terlebih dahulu sebelum mengambil tindakan. Hindari mengklik tautan yang tidak dipercaya atau mencurigakan di situs web yang tidak terpercaya.
5. Gunakan sandi yang kuat dan unik: Gunakan kata sandi yang kompleks, terdiri dari kombinasi huruf, angka, dan karakter khusus. Hindari menggunakan kata sandi yang mudah ditebak atau umum. Gunakan manajer kata sandi untuk mengelola sandi yang kuat dan unik untuk setiap akun yang Anda miliki.
6. Batasi hak akses: Berikan hak akses yang sesuai kepada pengguna dan kelompok pengguna. Batasi akses administrator hanya kepada mereka yang membutuhkannya. Ini akan membantu mencegah penyebaran ransomware dari akun yang terbatas.
7. Perhatikan pembaruan firmware: Selain memperbarui perangkat lunak, penting juga untuk memperbarui firmware perangkat keras seperti router, switch, dan perangkat jaringan lainnya. Firmware yang diperbarui dapat membantu melindungi perangkat keras dari kerentanan yang dapat dimanfaatkan oleh ransomware.
8. Tingkatkan kesadaran pengguna: Berikan pelatihan dan edukasi kepada pengguna tentang praktik keamanan digital yang aman. Ajarkan mereka untuk tidak mengklik tautan atau membuka lampiran yang mencurigakan, serta pentingnya melaporkan aktivitas yang mencurigakan kepada tim keamanan.
9. Gunakan firewall dan filter lalu lintas: Aktifkan firewall pada perangkat jaringan Anda dan gunakan filter lalu lintas untuk membatasi akses ke situs web berbahaya atau mencurigakan yang dapat menjadi sumber infeksi ransomware.
10. Monitor dan deteksi ancaman: Implementasikan sistem pemantauan dan deteksi ancaman yang kuat untuk mengmengidentifikasi dan menangani serangan ransomware secepat mungkin. Gunakan perangkat lunak atau solusi deteksi ancaman yang canggih untuk mendeteksi perilaku atau pola yang mencurigakan dari ransomware.

Dengan mengambil langkah-langkah pencegahan ini, maka dapat ditingkatkan keamanan sistem dan mengurangi risiko terkena serangan ransomware. Tetap mengikuti praktik keamanan yang baik dan tetap waspada terhadap ancaman yang mungkin muncul akan membantu melindungi data dari serangan ransomware.

E. Teknik Mendeteksi Ransomware

Salah satu elemen penting dari keamanan siber adalah deteksi ransomware. Bagian ini akan membahas berbagai metode pendeteksian ransomware yang diusulkan dalam literatur serta kekuatan, kelemahan, dan keterbatasannya [7].

1. Deteksi berbasis tanda tangan
   Pendekatan tradisional untuk deteksi berbasis tanda tangan bergantung pada pola atau tanda ransomware yang diketahui dalam kode atau perilaku malware. Metode ini menggunakan basis data

tanda tangan atau tanda ransomware yang diketahui dan memindai sistem atau jaringan untuk mencocokkannya. Jika ada kecocokan, ransomware diklasifikasikan sebagai berbahaya dan langkah-langkah yang tepat diambil[11-12].

Deteksi berbasis tanda tangan memiliki manfaat karena mudah dan efektif dalam menemukan jenis ransomware yang sudah ada. Namun, metode ini tidak dapat menemukan jenis ransomware baru atau yang tidak dikenal yang tidak sesuai dengan pola atau tanda tangan yang ada. Selain itu, penyerang dapat dengan mudah menghindari pengenalan tanda tangan dengan mengubah kode atau perilaku ransomware untuk menghindari pengenalan [13].

2. Deteksi Berbasis Heuristik

Metode yang lebih canggih untuk menemukan pola perilaku ransomware atau anomali yang menunjukkan aktivitas berbahaya dikenal sebagai deteksi berbasis heuristik. Metode ini dimulai dengan membuat aturan atau heuristik yang menggambarkan perilaku ransomware dan kemudian memeriksa sistem atau jaringan untuk setiap penyimpangan atau anomali dari aturan ini. Ransomware diidentifikasi sebagai mencurigakan atau berbahaya jika ada perbedaan atau kelainan tersebut, dan tindakan yang tepat diambil [11-12].

Salah satu manfaat deteksi berbasis heuristik adalah kemampuannya untuk menemukan jenis ransomware baru atau tidak dikenal yang tidak cocok dengan pola atau tanda tangan yang ada. Selain itu, meskipun metode ini bergantung pada pola perilaku yang sebenarnya daripada tanda tangan kode statis, metode ini tidak terlalu rentan terhadap false positive. Namun, deteksi berbasis heuristik bergantung pada aturan atau heuristik yang telah ditetapkan sebelumnya, yang hanya dapat menemukan beberapa pola atau anomali yang mungkin terjadi dalam perilaku ransomware. Selain itu, peretas dapat dengan mudah menghindari identifikasi berbasis heuristik dengan mengubah cara ransomware bekerja untuk menghindari identifikasi [13].

3. Deteksi Berbasis Jaringan

Deteksi berbasis jaringan adalah metode yang bergantung pada pemantauan aktivitas mencurigakan atau berbahaya di jaringan. Metode ini bergantung pada analisis lalu lintas jaringan untuk menemukan pola atau anomali yang terkait dengan serangan ransomware, seperti volume lalu lintas keluar yang besar, koneksi jaringan yang tidak biasa, atau enkripsi lalu lintas jaringan [11-12].

Salah satu manfaat deteksi berbasis jaringan adalah kemampuannya untuk menemukan aktivitas ransomware meskipun malware belum menginfeksi sistem atau jika ransomware menggunakan metode enkripsi yang tidak biasa. Selain itu, metode ini tidak terlalu rentan terhadap false positive dibandingkan dengan metode deteksi lainnya karena bergantung pada pola lalu lintas jaringan yang sebenarnya daripada aturan atau tanda kode statis. Deteksi berbasis jaringan, bagaimanapun, terbatas karena bergantung pada alat analisis lalu lintas jaringan, yang mungkin tidak tersedia atau tidak dapat menangkap semua aktivitas ransomware. Selain itu, peretas dapat dengan mudah menghindari deteksi berbasis jaringan dengan menggunakan saluran komunikasi yang tersembunyi atau mengenkripsi lalu lintas jaringan [13].

4. Deteksi Hibrida

Metode deteksi hibrida menggabungkan berbagai pendekatan untuk mendeteksi ransomware untuk meningkatkan akurasi dan kecepatan secara keseluruhan. Metode ini menggabungkan kekuatan dari pendeteksian berbasis tanda tangan, berbasis heuristik, berbasis pembelajaran mesin, dan berbasis jaringan, antara lain, untuk membuat sistem deteksi yang lebih kuat dan efisien [11-12].

Deteksi hibrida memiliki beberapa keuntungan, seperti kemampuan untuk mengatasi keterbatasan pendekatan deteksi individual dan meningkatkan akurasi dan kecepatan secara keseluruhan. Selain itu, karena menggabungkan berbagai sumber informasi dan analisis, pendekatan ini tidak terlalu rentan terhadap hasil positif dan negatif palsu dibandingkan dengan pendekatan deteksi unik. Namun, kekurangan deteksi hibrida adalah kompleksitas dan kebutuhan sumber daya yang tinggi[13].

4. SIMPULAN DAN SARAN

A. Simpulan

Penelitian ini berhasil menjawab pertanyaan utama mengenai dampak serangan ransomware terhadap keamanan data perusahaan dan strategi mitigasi yang efektif. Hasil penelitian menunjukkan bahwa serangan ransomware dapat menyebabkan kerugian signifikan, baik dalam hal finansial maupun kehilangan data yang bernilai, serta mengganggu operasional perusahaan. Dampaknya meluas ke berbagai sektor, termasuk pemerintah, perusahaan swasta, dan masyarakat umum. Dalam hal strategi mitigasi, terbukti bahwa penggunaan teknologi kecerdasan buatan dalam mendeteksi dan merespons serangan ransomware secara proaktif sangat efektif. Selain itu, implementasi backup data secara teratur dan penggunaan solusi keamanan yang kuat merupakan langkah penting dalam mengurangi risiko. Edukasi pengguna dan peningkatan kesadaran tentang praktik keamanan digital juga sangat diperlukan. enelitian ini berhasil menjawab pertanyaan utama mengenai dampak serangan ransomware terhadap keamanan data perusahaan dan strategi mitigasi yang efektif. Dari hasil penelitian, terbukti bahwa serangan ransomware dapat menyebabkan kerugian signifikan baik dalam hal finansial maupun kehilangan data yang bernilai. Temuan menunjukkan bahwa penggunaan teknologi kecerdasan buatan dalam strategi mitigasi terbukti efektif dalam mengurangi dampak dan risiko serangan ransomware.

B. Saran

Rekomendasi dari penelitian ini meliputi peningkatan teknologi deteksi dengan mengembangkan dan menerapkan algoritma kecerdasan buatan yang lebih canggih untuk mendeteksi pola serangan ransomware secara real-time, serta integrasi pendekatan deteksi berbasis tanda tangan, heuristik, jaringan, dan hibrida untuk meningkatkan efektivitas deteksi. Selain itu, perlu dilakukan pelatihan rutin bagi karyawan tentang bahaya ransomware dan cara menghindarinya, serta meningkatkan kesadaran akan pentingnya langkah-langkah pencegahan seperti backup data dan pembaruan perangkat lunak. Kolaborasi antara perusahaan, pemerintah, dan komunitas keamanan siber untuk berbagi informasi dan strategi terbaru dalam melawan ransomware juga sangat dianjurkan. Penelitian lebih lanjut tentang penggunaan kecerdasan buatan dan teknologi terbaru dalam mitigasi ancaman ransomware sangat diperlukan. Penelitian ini memberikan kontribusi signifikan dalam pemahaman tentang dampak ransomware dan strategi mitigasi yang efektif, dengan harapan bahwa implementasi rekomendasi yang dihasilkan dapat membantu perusahaan meningkatkan keamanan data mereka dan mengurangi risiko serangan ransomware di masa depan.

DAFTAR PUSTAKA

Jurnal

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains dan Teknologi*, 2(02), 55-62.

Safitri, K. A. (2023). Strategi Keamanan Sistem Informasi untuk Melawan Serangan Ransomware. *ResearchGate, no. April*, 1-11.

Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. *Int. J. Comput. Sci. Netw. Secur, 19*(2), 136.

Adiputra, I. M. S., Trisnadewi, N. W., Oktaviani, N. P. W., Munthe, S. A., Hulu, V. T., Budiastutik, I., ... & Suryana, S. (2021). *Metodologi penelitian kesehatan.* Yayasan Kita Menulis.

Rusli, M. (2021). Merancang penelitian kualitatif dasar/deskriptif dan studi kasus. *Al-Ubudiyah: Jurnal Pendidikan Dan Studi Islam, 2*(1), 48-60.

Temara, S. (2024). The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. *Asian Journal of Advanced Research and Reports, 18(3)*, 1-16.

Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning*: A survey. Big Data and Cognitive Computing*, 7(3), 143.

Purbo, O. W. Mid 2020 *Cyber Security Threat, Tips dan Proposal Strategi Mitigasi Nasional.*

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, 5(1), tyz003.

Al-Rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 144-166.

Yamany, B., Elsayed, M. S., Jurcut, A. D., Abdelbaki, N., & Azer, M. A. (2022). A new scheme for ransomware classification and clustering using static features. *Electronics, 11*(20), 3307.

Yamany, B., Azer, M. A., & Abdelbaki, N. (2022, May). Ransomware clustering and classification using similarity matrix. *In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)* (pp. 41-46). IEEE.

Akhtar, M. S., & Feng, T. (2022). Malware analysis and detection using machine learning algorithms. *Symmetry*, 14(11), 2304.