Tema :

Cyber Security

Topik:

1. **Cloud Security**

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Cybersecurity Vulnerabilities and Remediation Through Cloud Security Tools | FNU Jimmy | Maret 2024 | Journal of Artificial Intelligence General Science (JAIGS) |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Studi ini membahas peningkatan ancaman cyber akibat digitalisasi, terutama pada keamanan cloud. Penelitian ini bertujuan untuk mengeksplorasi metodologi dan teknologi mutakhir untuk mendeteksi dan mengurangi serangan cyber yang semakin kompleks. | Jurnal ini mengimplementasikan metodologi analisis konseptual yang mengidentifikasi kerentanan keamanan, metodologi deteksi, serta strategi mitigasi menggunakan teknologi terkini. | Penelitian ini menggunakan pendekatan tinjauan literatur yang mendalam untuk menggali berbagai solusi teknis dan non-teknis dalam mengatasi kerentanan keamanan cloud. | Pemindaian Kerentanannya: Penggunaan pemindai kerentanannya seperti Nessus untuk mendeteksi celah.  Penilaian Risiko: Model statistik dan machine learning untuk menilai tingkat risiko ancaman. |

|  |  |
| --- | --- |
| Hasil | |
| Studi ini menghasilkan wawasan yang signifikan tentang solusi keamanan cyber, termasuk pemanfaatan teknologi baru seperti big data, blockchain, dan AI untuk memperkuat pertahanan cyber. Penelitian ini menekankan pentingnya solusi teknis dan non-teknis yang kolaboratif untuk meminimalkan risiko dalam lingkungan cloud dan jaringan. | |
| Kelebihan | Kekurangan |
| Fokus pada integrasi machine learning, deep learning, dan blockchain.  Cakupan luas tentang tantangan dan vektor serangan keamanan cyber.  Rekomendasi praktis terkait keamanan cloud dan jaringan. | Ketergantungan pada machine learning yang rentan terhadap taktik penghindaran dan bias dalam model algoritma. |
| Saran penulis | |
| Penulis menyarankan penggunaan teknologi canggih, seperti machine learning, big data analytics, dan blockchain, untuk mendeteksi serta mengatasi ancaman ini dengan lebih efektif | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Security Attacks in Cloud Computing and Corresponding Defending Mechanisms | Hesham Abusaimeh | Mei-Juni 2020 | International Journal of Advanced Trends in Computer Science and Engineering |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Jurnal mengkaji berbagai serangan keamanan pada cloud computing, termasuk serangan brute force, replay, phishing, man-in-the-middle, dan lainnya. | Jurnal ini mengimplementasikan metodologi analisis konseptual yang mengidentifikasi kerentanan keamanan, metodologi deteksi, serta strategi mitigasi menggunakan teknologi terkini. | Menggunakan pendekatan survei untuk meninjau serangan autentikasi di cloud dan studi-studi terkait pertahanan. | Menggunakan literatur untuk mengidentifikasi serangan dan solusi pertahanan terkait. |

|  |  |
| --- | --- |
| Hasil | |
| Kombinasi berbagai mekanisme protektif, seperti password berbasis gambar, dapat mengurangi risiko serangan autentikasi. | |
| Kelebihan | Kekurangan |
| Memberikan ulasan yang teliti tentang jenis serangan keamanan di cloud dan solusi untuk setiap jenis serangan. | Tidak mencakup solusi untuk semua jenis serangan dan tidak menguji efektivitas solusi. |
| Saran penulis | |
| disarankan implementasi langkah-langkah keamanan seperti multi-factor authentication (MFA), yang melibatkan OTP dan elemen autentikasi tambahan untuk melawan serangan brute force dan dictionary attacks | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Cloud Security Metrics and Measurement | Sina Ahmadi | April 2023 | Journal of Knowledge Learning and Science Technology |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Studi ini membahas kebutuhan metrik dan pengukuran yang efektif untuk menilai keamanan cloud. Jurnal ini mengeksplorasi bagaimana kerangka kerja saat ini, seperti NIST SP 800-53 dan ISO/IEC 27001, dapat membantu organisasi menerapkan protokol keamanan cloud yang kuat. Studi ini juga menyoroti kurangnya metrik standar untuk keamanan cloud dan tantangan dalam beradaptasi dengan ancaman yang terus berkembang. | Metode penelitian kualitatif dengan tinjauan pustaka. | Analisis studi dan kerangka kerja yang ada, termasuk ISO/IEC 27001 dan NIST SP 800-53, serta pendekatan tematik untuk mengidentifikasi metrik dan tantangan keamanan cloud yang sering muncul. | Bayesian Networks, entropi Shannon, dan simulasi Monte Carlo untuk menilai aspek kerahasiaan dan integritas dalam keamanan cloud. |

|  |  |
| --- | --- |
| Hasil | |
| Studi ini mengidentifikasi kebutuhan metrik yang dapat disesuaikan dan distandarisasi serta menunjukkan bagaimana model yang ada dapat mendukung evaluasi keamanan cloud, terutama dalam aspek kerahasiaan, integritas, dan ketersediaan. | |
| Kelebihan | Kekurangan |
| Memberikan pandangan menyeluruh mengenai kerangka kerja keamanan cloud dan mengusulkan metrik yang distandarisasi. Studi ini juga mengintegrasikan beberapa kerangka kerja yang memungkinkan pendekatan holistik terhadap keamanan cloud. | Mengandalkan tinjauan kualitatif tanpa validasi eksperimental; efektivitas studi ini di dunia nyata terbatas tanpa pengujian empiris. |
| Saran penulis | |
| penggunaan standar keamanan seperti CSA Cloud Controls Matrix dan ISO/IEC 27001 untuk memperkuat keamanan cloud. | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Cloud Security Issues in Present Day Context | Zhimin Guan, Dr. Rama Bhatia | Desember 2022 | ScienceOpen Preprints |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Isu utama keamanan cloud, multi-tenancy, dan risiko model layanan cloud seperti IaaS, PaaS, SaaS | Studi kualitatif berbasis literatur yang menggunakan pendekatan sistematis (PRISMA) untuk memilih artikel terkait cloud security dari sumber tepercaya seperti IEEE dan Springer. | Analisis teks untuk menyusun dan mengelompokkan ancaman keamanan cloud, tanpa penggunaan uji praktis atau alat AI. | Klasifikasi ancaman keamanan berdasarkan level layanan dan model penyebaran cloud. |

|  |  |
| --- | --- |
| Hasil | |
| Daftar ancaman cloud, teknik mitigasi seperti enkripsi dan pengelolaan kunci. | |
| Kelebihan | Kekurangan |
| Komprehensif dan terstruktur dalam klasifikasi ancaman keamanan. | Tidak ada uji praktis atau contoh implementasi mitigasi. |
| Saran penulis | |
| peningkatan enkripsi data untuk menjaga kerahasiaan, manajemen akses yang ketat untuk mencegah akses tidak sah, dan pemantauan berkelanjutan terhadap aktivitas jaringan untuk mendeteksi anomali. | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning | Ammar Aldallal, Faisal Alisa | Desember 2021 | MDPI Symmetry |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Mendeteksi dan melindungi data cloud dari serangan intrusi dengan sistem deteksi intrusi berbasis machine learning. | Studi berbasis eksperimen menggunakan dataset CICIDS2017 untuk menguji sistem deteksi intrusi yang diusulkan. | Menggabungkan algoritma Support Vector Machine (SVM) dan Genetic Algorithm (GA) untuk meningkatkan akurasi sistem. | Support Vector Machine (SVM) dan Genetic Algorithm (GA) digunakan secara paralel untuk memilih fitur dan meningkatkan akurasi. |

|  |  |
| --- | --- |
| Hasil | |
| Model ini menunjukkan peningkatan performa hingga 5.74% dibandingkan benchmark lain menggunakan dataset KDD CUP 99 dan NSL-KDD. | |
| Kelebihan | Kekurangan |
| Efisiensi tinggi dalam mendeteksi serangan cloud melalui kombinasi GA dan SVM, meningkatkan simetri antara keamanan data dan deteksi intrusi. | Hanya diuji menggunakan dataset CICIDS2017, tidak mencakup uji dunia nyata atau implementasi langsung di cloud. |
| Saran penulis | |
| Gunakan IDS berbasis pembelajaran mesin sebagai metode yang lebih efektif dalam menjaga keamanan cloud, terutama pada data yang sensitif seperti data medis. | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security | Adnan Qayyum, Aneeqa Ijaz, Muhammad Usama, Waleed Iqbal, Junaid Qadir, Yehia Elkhatib, Ala Al-Fuqaha | November 2020 | Frontiers in Big Data |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Keamanan Machine Learning as a Service (MLaaS) dan tantangan serangan serta pertahanan pada cloud ML/DL. | Tinjauan sistematis menggunakan protokol PRISMA untuk memilih artikel terkait dari delapan pustaka utama. | Analisis literatur pada serangan dan metode pertahanan untuk cloud-hosted ML/DL, dengan fokus pada serangan dan mitigasinya. | Tidak ada algoritma spesifik yang dikembangkan; penelitian mengkategorikan tipe serangan dan pertahanan terhadap cloud-hosted ML/DL. |

|  |  |
| --- | --- |
| Hasil | |
| Mengidentifikasi ancaman seperti serangan black-box, white-box, dan metode mitigasi seperti homomorphic encryption. | |
| Kelebihan | Kekurangan |
| Artikel ini menyajikan ikhtisar komprehensif mengenai serangan dan pertahanan pada cloud ML/DL, serta menyusun taksonomi yang terperinci. | Tidak ada eksperimen langsung untuk mengevaluasi efektivitas pertahanan yang diusulkan. |
| Saran penulis | |
| pengembangan sistem pertahanan yang lebih kuat seperti penerapan keamanan berbasis enkripsi, metode deteksi anomali, dan peningkatan privasi melalui federated learning untuk mengurangi risiko serangan terhadap model ML di cloud. | |

|  |  |
| --- | --- |
| Relavan | 5 |

1. **Phising Attack Detection**

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Phishing Attacks: A Recent Comprehensive Study and a New Anatomy | Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, dan Imtiaz Khan | Maret 2021 | Frontiers in Computer Science |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Jurnal ini menyoroti peningkatan serangan phishing, evolusi teknik-teknik phishing, dan mengkaji anatomi phishing yang kompleks. Masalah utama adalah bagaimana phishing berkembang menjadi ancaman keamanan yang signifikan di internet, yang mencakup cara untuk menipu pengguna agar mengungkapkan informasi sensitif. | Penelitian ini mengklasifikasikan jenis-jenis serangan phishing berdasarkan fase-fase anatomi serangan, tipe pelaku, kerentanan, dan teknik serangan yang digunakan. Mereka juga mengkaji langkah-langkah pencegahan. | Jurnal ini menggunakan pendekatan tinjauan literatur dan analisis kasus nyata untuk mendalami fase-fase serangan phishing serta menciptakan anatomi baru yang meliputi empat fase utama: perencanaan, persiapan, pelaksanaan serangan, dan akuisisi informasi berharga. | Penelitian ini lebih berfokus pada penyusunan tahapan dan teknik untuk pemahaman yang lebih mendalam tentang anatomi serangan phishing. |

|  |  |
| --- | --- |
| Hasil | |
| Hasil dari penelitian ini adalah penyusunan anatomi phishing yang rinci yang menggambarkan seluruh siklus hidup serangan phishing dari awal hingga akhir. Anatomi ini diharapkan dapat membantu pembaca memahami serangan phishing dengan lebih baik dan meningkatkan kesadaran serta pengembangan sistem anti-phishing. | |
| Kelebihan | Kekurangan |
| Jurnal ini memberikan pemahaman yang komprehensif mengenai anatomi serangan phishing dan mencakup aspek psikologis dan teknik-teknik sosial yang digunakan oleh pelaku untuk menyerang korban. Hal ini memberikan landasan yang baik untuk merancang langkah-langkah pencegahan yang lebih efektif. | Jurnal ini tidak memberikan algoritma deteksi spesifik atau solusi teknis yang mendalam, sehingga kurang relevan bagi yang mencari pendekatan berbasis machine learning atau algoritma untuk deteksi phishing. |
| Saran penulis | |
| langkah untuk melindungi dari phishing: meningkatkan pendidikan dan kesadaran pengguna, menggunakan teknologi deteksi berbasis kecerdasan buatan, menerapkan otentikasi multifaktor, dan memperkuat filter email untuk mengenali pengirim yang sah | |

|  |  |
| --- | --- |
| Relavan | 3.5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning | Eduardo Benavides-Astudillo, Walter Fuertes, Sandra Sanchez-Gordon, Daniel Nuñez-Agurto, Germán Rodríguez-Galán | April 2023 | MDPI, Applied Sciences |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Jurnal ini membahas masalah deteksi serangan phishing melalui model yang didasarkan pada analisis teks dari halaman web menggunakan Natural Language Processing (NLP) dan Deep Learning (DL) | Studi ini menggunakan metodologi bertahap yang meliputi pemrosesan teks, pra-pemrosesan NLP, ekstraksi fitur dengan embedding GloVe, dan penerapan model DL untuk mengklasifikasikan antara halaman phishing dan halaman yang sah (ham). Model ini menggunakan Keras Embedding dengan GloVe untuk representasi fitur, diikuti dengan perbandingan antara empat model DL: LSTM, BiLSTM, GRU, dan BiGRU | Penggunaan NLP dengan embedding GloVe dan empat model Deep Learning (LSTM, BiLSTM, GRU, BiGRU) untuk mendeteksi phishing dari teks halaman web | Empat algoritma Deep Learning yang digunakan: LSTM (Long Short-Term Memory), BiLSTM (Bidirectional LSTM), GRU (Gated Recurrent Unit), BiGRU (Bidirectional GRU) |

|  |  |
| --- | --- |
| Hasil | |
| Dari keempat algoritma, BiGRU mencapai akurasi tertinggi, yaitu 97,39%. BiGRU unggul karena pemrosesan bidirectional, yang mempertimbangkan konteks dari kata sebelum dan sesudah dalam kalimat | |
| Kelebihan | Kekurangan |
| Akurasi Tinggi: Algoritma BiGRU menunjukkan akurasi tinggi dalam deteksi phishing.  Pendekatan Berbasis Teks: Mampu mendeteksi phishing dari konten teks, bukan hanya URL | Biaya Komputasi Tinggi: Algoritma bidirectional (seperti BiGRU) membutuhkan waktu pelatihan lebih lama.  Keterbatasan Panjang Teks: Performa menurun pada teks dengan kurang dari 200 kata |
| Saran penulis | |
| peningkatan lebih lanjut pada algoritma deteksi untuk menjaga akurasi dalam menghadapi volume data cloud yang terus meningkat. disarankan penggunaan dataset yang lebih relevan dan terbaru agar metode yang digunakan tetap efektif dalam mendeteksi ancaman terkini di lingkungan cloud computing. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| A comprehensive survey of AI-enabled phishing attacks detection techniques | Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed | Oktober 2020 | Telecommunication Systems |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Artikel ini membahas perkembangan teknik berbasis AI untuk mendeteksi serangan phishing, yang berfokus pada keamanan digital, khususnya ancaman phishing terhadap data pribadi dan finansial. Phishing, sebagai salah satu serangan cyber yang paling umum, memerlukan metode deteksi yang canggih untuk mengurangi risiko pencurian data. | Penulis menggunakan metode literature review komprehensif dengan meninjau berbagai penelitian tentang deteksi phishing menggunakan teknologi kecerdasan buatan. Analisis difokuskan pada mengklasifikasikan teknik-teknik tersebut berdasarkan jenis dan efektivitasnya. | Artikel ini mencakup metode seperti pembelajaran mesin (machine learning), pembelajaran mendalam (deep learning), serta metode hybrid yang menggabungkan beberapa pendekatan. Teknik yang digunakan meliputi klasifikasi untuk membedakan antara email phishing dan non-phishing, serta deteksi pola untuk menganalisis ciri khas serangan phishing. | Algoritma yang dibahas termasuk teknik pembelajaran mesin seperti Support Vector Machine (SVM), Decision Trees, Random Forests, serta model pembelajaran mendalam seperti Convolutional Neural Networks (CNN) dan Recurrent Neural Networks (RNN), yang digunakan untuk mendeteksi pola spesifik dalam phishing. |

|  |  |
| --- | --- |
| Hasil | |
| Hasil penelitian ini menunjukkan bahwa teknik berbasis AI memiliki tingkat akurasi yang lebih tinggi dibandingkan metode tradisional dalam mendeteksi phishing. Namun, terdapat tantangan dalam mengadopsi teknik ini secara luas karena kecepatan perkembangan teknik serangan phishing. | |
| Kelebihan | Kekurangan |
| Kelebihan artikel ini adalah cakupan yang luas dan mendalam terkait metode deteksi phishing berbasis AI, memberikan wawasan komprehensif tentang kemajuan dan tantangan teknologi ini dalam keamanan cyber. | Kekurangannya adalah penelitian ini belum mencakup penerapan empiris di dunia nyata untuk menguji efektivitas teknik ini dalam berbagai konteks yang dinamis. |
| Saran penulis | |
| berbagai metode berbasis kecerdasan buatan untuk mendeteksi serangan phishing, seperti pembelajaran mesin, pembelajaran mendalam, dan metode hybrid. Direkomendasikan fokus pada peningkatan teknik AI , terutama melalui penggunaan model hybrid yang menggabungkan kelebihan dari beberapa pendekatan untuk mendeteksi ancaman phishing dengan lebih akurat dan efisien. | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| A Lightweight Multi-View Learning Approach for Phishing Attack Detection Using Transformer with Mixture of Experts | Yanbin Wang, Wenrui Ma, Haitao Xu, Yiwei Liu, Peng Yin | Juni 2023 | MPDI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Penelitian ini membahas deteksi serangan phishing menggunakan pendekatan pembelajaran multi-view yang ringan dengan model transformer dan Mixture of Experts (MoE) untuk mengidentifikasi serangan phishing secara lebih efisien. | Pendekatan menggunakan transformer dan Mixture of Experts (MoE) dalam deteksi phishing dengan memanfaatkan berbagai sumber data. | Transformer: Untuk ekstraksi fitur. MoE: Memilih ahli model berdasarkan tugas. Pembelajaran Multi-View: Menggabungkan berbagai fitur (teks, URL, metadata). | Transformer: Untuk ekstraksi fitur dan pemodelan urutan data. MoE untuk efisiensi komputasi. Pembelajaran Multi-View: Penggabungan beberapa tampilan data untuk meningkatkan kinerja model. |

|  |  |
| --- | --- |
| Hasil | |
| Peningkatan Akurasi: Pendekatan ini menunjukkan akurasi yang lebih tinggi dibandingkan dengan metode deteksi phishing lainnya. Efisiensi Komputasi: Model yang lebih ringan dan lebih cepat dalam pengolahan data. | |
| Kelebihan | Kekurangan |
| Efisien dalam Penggunaan Sumber Daya: Menggunakan MoE memungkinkan model hanya mengaktifkan ahli tertentu sesuai kebutuhan, menghemat sumber daya. Akurasi Tinggi: Menggabungkan beberapa tampilan data untuk mendeteksi phishing dengan lebih baik. | Kompleksitas Implementasi: Penggunaan MoE dan pembelajaran multi-view dapat membuat implementasi lebih kompleks. Keterbatasan Data: Diperlukan data yang cukup untuk melatih model agar dapat berfungsi dengan baik di berbagai skenario phishing. |
| Saran penulis | |
| Disarankan evaluasi lebih lanjut pada berbagai dataset untuk menilai konsistensi kinerja di skenario nyata | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Detecting Phishing Domains Using Machine Learning | Shouq Alnemari, Majid Alshammari | April 2023 | MPDI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Penelitian ini membahas serangan phishing yang dilakukan melalui domain palsu, di mana penyerang menyamar sebagai situs web tepercaya untuk mengelabui pengguna agar memberikan informasi sensitif mereka. | Penelitian ini mengembangkan dan membandingkan empat model pembelajaran mesin (ANN, SVM, DT, RF) untuk mendeteksi domain phishing, menggunakan dataset phishing UCI sebagai acuan. | Model Pembelajaran Mesin: Mencakup jaringan saraf tiruan (ANN), mesin vektor dukungan (SVM), pohon keputusan (DT), dan hutan acak (RF). Dataset: Dataset phishing UCI digunakan untuk mengevaluasi efektivitas model dalam mendeteksi domain phishing. | Model-model yang digunakan adalah: ANN (Artificial Neural Networks), SVM (Support Vector Machines), DT (Decision Trees), RF (Random Forest) |

|  |  |
| --- | --- |
| Hasil | |
| Model Random Forest menunjukkan akurasi terbaik dibandingkan dengan model lainnya dan lebih unggul dari solusi yang ada dalam literatur. | |
| Kelebihan | Kekurangan |
| Penelitian ini memberikan analisis komparatif berbagai algoritma pembelajaran mesin untuk deteksi phishing, yang membantu dalam memahami kelebihan dan kekurangan masing-masing model. | Kompleksitas Implementasi: Penggunaan MoE dan pembelajaran multi-view dapat membuat implementasi lebih kompleks. Keterbatasan Data: Diperlukan data yang cukup untuk melatih model agar dapat berfungsi dengan baik di berbagai skenario phishing. |
| Saran penulis | |
| disarankan pengembangan lebih lanjut menggunakan dataset yang lebih besar untuk mengikuti taktik phishing yang terus berkembang​ | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Improved Phishing Attack Detection with Machine Learning: A Comprehensive Evaluation of Classifiers and Features | Sibel Kapan, Efnan Sora Gunal | Desember 2023 | MPDI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Penelitian ini mengkaji penggunaan teknik pembelajaran mesin dalam mendeteksi serangan phishing dengan menilai berbagai fitur dan algoritma klasifikasi untuk menemukan pendekatan yang paling efektif. | Dataset phishing baru disiapkan, dan analisis dilakukan menggunakan berbagai fitur URL dan HTTP. Metode eksperimen dilakukan dengan menguji beberapa algoritma klasifikasi untuk mengevaluasi kinerja deteksi serangan phishing. | Pembelajaran mesin menggunakan beberapa algoritma klasifikasi, termasuk decision tree, untuk mendeteksi situs web phishing. | decision tree, KNN, dan SVM |

|  |  |
| --- | --- |
| Hasil | |
| Decision tree terbukti memberikan kinerja terbaik dengan F1-score 0,99 dan kecepatan tinggi dalam klasifikasi. | |
| Kelebihan | Kekurangan |
| Dataset baru yang disediakan untuk penelitian ini memungkinkan analisis mendalam dari berbagai fitur untuk deteksi phishing | Penelitian hanya berfokus pada dua jenis dataset dan tidak membahas konteks serangan phishing yang lebih luas |
| Saran penulis | |
| penelitian lanjutan fokus pada pengembangan dataset yang lebih kaya dan mencakup lebih banyak fitur terkait phishing untuk meningkatkan akurasi model deteksi. direkomendasikan pengujian dengan lebih banyak teknik klasifikasi dan kombinasi fitur untuk menemukan pendekatan yang lebih efektif dan efisien dalam menghadapi variasi taktik phishing yang terus berkembang | |

|  |  |
| --- | --- |
| Relavan | 5 |

1. **IOT**

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Cybersecurity Risk Analysis in the IoT: A Systematic Review | Thanaa Saad AlSalem, Mohammed Amin Almaiah, Abdalwali Lutfi | September 2023 | MDPI Electronics |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Artikel ini menyelidiki berbagai risiko keamanan cyber yang terkait dengan perangkat IoT, menyoroti kekhawatiran yang semakin meningkat terkait privasi dan banyaknya kejahatan cyber. Artikel ini juga mengatasi kekurangan yang ada dalam kerangka keamanan cyber untuk IoT saat ini. | Studi ini menggunakan tinjauan literatur sistematis untuk memeriksa 40 artikel yang mencakup tantangan dan serangan dalam keamanan cyber IoT, serta kerangka dan solusi yang diusulkan dalam literatur. | Tinjauan ini mengkategorikan berbagai jenis serangan dan mengevaluasi efektivitas berbagai pendekatan keamanan cyber, dengan fokus khusus pada teknik pembelajaran mesin untuk deteksi ancaman dan tindakan balasan. | Artikel ini membahas penerapan algoritma pembelajaran mesin, meskipun algoritma spesifik tidak dijelaskan secara mendalam dalam ringkasan. Fokusnya adalah pada kepraktisan algoritma ini dalam aplikasi dunia nyata. |

|  |  |
| --- | --- |
| Hasil | |
| Tinjauan menemukan bahwa masalah privasi dan kejahatan cyber adalah perhatian utama dalam keamanan IoT. Artikel ini juga menekankan potensi kecerdasan buatan untuk meningkatkan upaya keamanan cyber di masa depan. Namun, beberapa serangan, seperti yang menargetkan kerahasiaan dan koneksi server data, tetap kurang ditangani. | |
| Kelebihan | Kekurangan |
| Tinjauan literatur yang komprehensif yang mensintesis sejumlah besar penelitian. Menyoroti tren yang muncul dan kekurangan dalam lanskap penelitian saat ini, terutama dalam penilaian dampak ekonomi dan keamanan IoT industri. Menawarkan wawasan berharga tentang efektivitas pembelajaran mesin dalam meningkatkan keamanan IoT. | Beberapa serangan tetap kurang dieksplorasi dalam solusi yang ada, menunjukkan bahwa lebih banyak penelitian dan pengujian di dunia nyata diperlukan. Fokus pada tinjauan literatur dapat membatasi rekomendasi praktis untuk implementasi langsung di lingkungan IoT. |
| Saran penulis | |
| penggunaan solusi adaptif dan otomatis untuk menghadapi risiko keamanan di IoT, serta mengusulkan teknologi seperti blockchain untuk memperkuat keamanan jaringan. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Keamanan IoT dan Sistem Terdistribusi | Ahmadiki Firman Dwi Suryawan, Fauzan Graha Dwi Putra, Vanya Amanda Lovely, Aep Setiawan | Juni 2024 | Journal of Internet and Software Engineering |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Jurnal ini mengkaji tantangan yang dihadapi dalam mengamankan perangkat IoT dan sistem terdistribusi, termasuk risiko dan kerentanan yang dapat muncul akibat keterhubungan perangkat dalam jaringan yang luas. | Metodologi yang digunakan dalam penelitian ini mencakup analisis literatur terkait serta studi kasus pada implementasi IoT dalam berbagai aplikasi. | Penelitian ini menerapkan metode kualitatif, dengan fokus pada pengumpulan dan analisis data dari berbagai sumber yang relevan tentang keamanan IoT. | pentingnya protokol keamanan dalam komunikasi data antar perangkat. |

|  |  |
| --- | --- |
| Hasil | |
| Hasil dari penelitian menunjukkan bahwa meskipun IoT menawarkan banyak manfaat, implementasi yang aman masih menjadi tantangan besar, terutama dalam hal perlindungan data dan privasi pengguna. | |
| Kelebihan | Kekurangan |
| Kelebihan dari penelitian ini adalah pemaparan yang mendalam tentang isu - isu keamanan yang spesifik terhadap iot dan rekomendasi praktis untuk meningkatkan keamanan. | Kekurangan yang ada adalah kurangnya data empiris yang lebih konkret dari penerapan di lapangan yang dapat mendukung temuan analisis. |
| Saran penulis | |
| tantangan keamanan pada perangkat Internet of Things (IoT) dan sistem terdistribusi, serta strategi mitigasi yang bisa diterapkan untuk mengamankan perangkat-perangkat tersebut dari ancaman cyber. | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| A State of the Art Survey of Machine Learning Algorithms for IoT Security | Alan Fuad Jahwar, Subhi R. M. Zeebaree | Juni 2021 | Asian Journal of Research in Computer Science |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| penerapan algoritma Machine learning (ML) dan Deep learning (DL) dalam keamanan Internet of Things (IoT). Fokusnya adalah bagaimana algoritma-algoritma ini dapat mendeteksi dan mencegah ancaman keamanan seperti serangan Distributed Denial of Service (DDoS) dan penyusupan lainnya di jaringan IoT. | Artikel ini melakukan survei literatur secara menyeluruh untuk meninjau pendekatan ML dan DL yang digunakan dalam meningkatkan keamanan IoT. | Algoritma ML yang dibahas mencakup Support Vector Machine (SVM), K-Nearest Neighbors (K-NN), dan Decision Tree (DT) yang digunakan dalam deteksi penyusupan dan serangan malware pada jaringan IoT. Deep Learning juga dieksplorasi melalui penggunaan Convolutional Neural Networks (CNN) untuk deteksi objek dan serangan dalam IoT. | Algoritma ML yang dibahas meliputi SVM, K-NN, Decision Tree, dan Random Forest, sedangkan DL melibatkan CNN dan Recurrent Neural Networks (RNN). Algoritma ini diterapkan untuk mendeteksi berbagai serangan keamanan di jaringan IoT. |

|  |  |
| --- | --- |
| Hasil | |
| Algoritma pembelajaran mesin seperti SVM dan Random Forest efektif untuk deteksi penyusupan, sedangkan CNN dapat digunakan untuk deteksi intrusi di perangkat edge dalam IoT. Akurasi deteksi mencapai hingga 99% dalam beberapa kasus, terutama untuk serangan berbasis jaringan. | |
| Kelebihan | Kekurangan |
| Menggambarkan potensi besar algoritma dalam mencegah berbagai serangan pada jaringan IoT. | Tidak mengembangkan atau mengevaluasi algoritma spesifik yang diusulkan. |
| Saran penulis | |
| pemilihan algoritma machine learning yang sesuai dengan ancaman IoT, penggunaan dataset yang aman dan relevan, serta efisiensi komputasi agar sesuai dengan keterbatasan perangkat IoT. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Exploring Machine Learning Intrusion Detection: Addressing Security and Privacy Challenges in IoT - A Comprehensive Review | Gowrisankar Krishnamoorthy, Sai Mani Krishna Sistla | Oktober 2023 | Journal of Knowledge Learning and Science Technology |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Artikel ini meninjau tantangan keamanan dan privasi dalam ekosistem Internet of Things (IoT) dengan fokus pada penerapan sistem deteksi intrusi berbasis Machine learning. | Systematic Literature Review (SLR) berbasis PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) untuk mengidentifikasi literatur relevan dari database IEEE dan ProQuest dari 2011 hingga 2021. | teknik ML dan DL, seperti Supervised Learning, Unsupervised Learning, Semi-Supervised Learning, dan Reinforcement Learning. Teknologi keamanan yang diulas meliputi penggunaan federated learning, blockchain, dan kombinasi model ML dalam memitigasi serangan. | Algoritma ML yang dibahas mencakup Random Forest, Decision Tree, Support Vector Machine (SVM), serta deep learning seperti Convolutional Neural Networks (CNN). |

|  |  |
| --- | --- |
| Hasil | |
| Model DL, seperti CNN, memiliki akurasi tinggi dalam deteksi anomali dibandingkan dengan metode ML tradisional. | |
| Kelebihan | Kekurangan |
| Memberikan gambaran komprehensif tentang penerapan ML dalam keamanan IoT. | Memiliki keterbatasan terkait studi empiris pada kasus nyata |
| Saran penulis | |
| pengembangan algoritma machine learning yang efisien dan ringan untuk mengatasi keterbatasan perangkat IoT, serta perlindungan privasi dan keamanan data pengguna. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Better Safe Than Never: A Survey on Adversarial Machine Learning Applications towards IoT Environment | Sarah Alkadi, Saad Al-Ahmadi, Mohamed Maher Ben Ismail | Mei 2023 | Applied Sciences, MDPI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| mengeksplorasi aplikasi pembelajaran mesin yang bersifat adversarial (Adversarial Machine Learning, AML) di lingkungan IoT, dan teknik pertahanan untuk memperkuat Intrusion Detection Systems (IDS) pada IoT. | Studi literatur (2018-2022), Pendekatannya melibatkan analisis dan pemetaan teknik-teknik AML untuk memahami serangan dan mekanisme pertahanan pada IoT, berdasarkan data dari basis data akademis terkenal seperti Springer dan IEEE Xplore. | pendekatan AML, crafting methods untuk membuat adversarial examples seperti Fast Gradient Sign Method (FGSM), Projected Gradient Descent (PGD), dan metode yang menggunakan Generative Adversarial Networks (GAN). | FGSM, PGD, dan GAN. |

|  |  |
| --- | --- |
| Hasil | |
| Mengidentifikasi bahwa meskipun AML dapat digunakan untuk meningkatkan deteksi intrusi pada jaringan IoT, ada kekurangan dalam pengembangan mekanisme pertahanan yang kuat. | |
| Kelebihan | Kekurangan |
| Memberikan analisis yang mendalam tentang penerapan AML dalam meningkatkan keamanan IoT. | Fokus lebih pada literatur dan teori tanpa penerapan dalam skenario dunia nyata yang komprehensif. |
| Saran penulis | |
| pengembangan model machine learning yang lebih tangguh terhadap serangan adversarial, pengujian keamanan secara berkala, dan penerapan pendekatan keamanan berlapis untuk melindungi perangkat IoT. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues | Mohit Kumar, Ashwani Kumar, Sahil Verma, Pronaya Bhattacharya, Deepak Ghimire, Seong-heum Kim, A. S. M. Sanwar Hosen | April 2023 | Electronics, MDPI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| tantangan yang terkait dengan keamanan dan privasi data kesehatan. Fokusnya adalah pada potensi risiko keamanan dalam pengelolaan data pasien, khususnya saat data ditransfer atau disimpan di lingkungan berbasis IoT. | Systematic Review untuk merangkum literatur yang berkaitan dengan keamanan dan privasi pada H-IoT, termasuk penerapan big data, blockchain, machine learning, dan deep learning untuk mitigasi risiko. | platform kriptografi digunakan di lingkungan H-IoT, seperti blockchain untuk keamanan data, edge computing untuk mengurangi latensi, dan software-defined networks (SDN) untuk pengelolaan jaringan. | Support Vector Machines (SVM) dan Convolutional Neural Networks (CNN) |

|  |  |
| --- | --- |
| Hasil | |
| menunjukkan bahwa penerapan teknologi seperti blockchain, big data, dan edge computing dapat membantu mengatasi tantangan keamanan H-IoT. | |
| Kelebihan | Kekurangan |
| Artikel ini memberikan pandangan komprehensif tentang perkembangan dan tantangan H-IoT. | Artikel ini tidak mencakup studi empiris untuk menguji efektivitas teknologi yang diusulkan. |
| Saran penulis | |
| pengembangan perangkat H-IoT yang lebih aman dan efisien, mengingat peran pentingnya dalam industri kesehatan. disarankan peningkatan keamanan data pasien, mengatasi keterbatasan daya dan komputasi perangkat, serta perlunya regulasi dan standar keamanan yang ketat. | |

|  |  |
| --- | --- |
| Relavan | 4 |

1. **Ransomware dan Malware**

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Ransomware Detection Using the Dynamic Analysis and  Machine Learning: A Survey and Research Directions | Umara Urooj, Bander Ali Saleh Al-rimy 1, Anazida Zainal, Fuad A. Ghaleb, Murad A. Rassam | December 2021 | MDPI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Tantangan dalam mendeteksi ransomware secara efektif, memahami peran analisis dinamis dalam deteksi, serta bagaimana machine learning dan deep learning dapat digabungkan untuk meningkatkan akurasi deteksi. | Penelitian ini meliputi survei literatur tentang deteksi ransomware, analisis dinamis untuk memantau perilaku ransomware, dan penerapan algoritma machine learning dan deep learning seperti Decision Tree, Random Forest, SVM, dan Neural Networks untuk deteksi. | Metode deteksi ransomware menggunakan machine learning dan deep learning | Sistem menerapkan teknik Deep Learning dan Machine Learning yang meliputi algoritma Support Vector Machine, Logistic Regression, Naive Bayes, Deep Learning, Random Tree, K-Nearest Neighbor |

|  |  |
| --- | --- |
| Hasil | |
| Deteksi ransomware dapat ditingkatkan dengan kombinasi analisis dinamis dan teknologi machine learning serta deep learning, dengan mengembangkan taksonomi metode deteksi, memanfaatkan dataset pelatihan yang relevan, dan menyarankan penelitian lanjutan yang menggabungkan analisis statis dan dinamis untuk menghasilkan sistem deteksi yang lebih adaptif dan tangguh terhadap evasi ransomware. | |
| Kelebihan | Kekurangan |
| Penelitian ini berhasil mengeksplorasi dan membandingkan teknik-teknik machine learning dan deep learning yang berbeda, termasuk algoritma seperti Decision Tree, Random Forest, SVM, dan Neural Networks untuk deteksi ransomware. | Makalah ini lebih berfokus pada survei dan tinjauan literatur, tanpa melakukan eksperimen atau evaluasi praktis terhadap algoritma yang disebutkan. |
| Saran penulis | |
| pengembangan model machine learning yang efektif dan cepat untuk mendeteksi ransomware melalui analisis dinamis, yang memungkinkan respons real-time terhadap serangan. | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| AI-based Malware and Ransomware  Detection Models | Benjamin Marais, Tony Quertier, Stephane Morucci | November 2022 | arXiv |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Jurnal ini membahas peningkatan serangan ransomware, dan pentingnya deteksi malware dan ransomware yang efektif. Penelitian ini berfokus pada peningkatan model deteksi malware dan ransomware berbasis machine learning dan deep learning. | 3 dataset (Ember, Bodmas, PEMachineLearning) yang berisi berkas PE (Portable Executable), penelitian ini melatih dan menguji berbagai model ML dan DL untuk mendeteksi serta mengklasifikasi ransomware. Fitur utama diambil dari berkas PE menggunakan metode ekstraksi Ember dan Grayscale. | Menggunakan metode ember dan grayscale, 3 dataset(Ember, Bodmas, dan PEMachineLearning), dan bi- layered | LightGBM, XGBoost, DNN, dan CNN |

|  |  |
| --- | --- |
| Hasil | |
| Model XGBoost menunjukkan kinerja terbaik dalam deteksi malware secara keseluruhan. Model bi-layered memberikan hasil lebih baik dibandingkan model acuan, terutama dalam hal fleksibilitas untuk dikembangkan lebih lanjut. | |
| Kelebihan | Kekurangan |
| Model bi-layered dapat diperbarui secara mandiri sehingga fleksibel untuk pengembangan dan optimalisasi berkelanjutan.  Menggunakan metode yang fleksibel untuk deteksi malware dan ransomware secara bersamaan. | Model CNN menunjukkan kinerja yang lebih rendah dan kurang optimal dibandingkan model lainnya.  Diperlukan lebih banyak data dan optimisasi preprocessing untuk meningkatkan hasil deteksi. |
| Saran penulis | |
| pengembangan model deteksi malware dan ransomware berbasis AI yang lebih tangguh, dengan memfokuskan pada algoritma yang mampu mengidentifikasi pola ancaman secara akurat dan cepat. | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang | Saputra Dio Azmi, Stiawan Deris, Sutabri Tata | Juni 2023 | Indonesian Journal of Multidisciplinary on Social and Technology |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Penelitian ini membahas penggunaan Deep Packet Inspection (DPI) untuk mendeteksi serangan ransomware, khususnya ransomware WannaCry, pada jaringan SMK Negeri 1 Palembang, dan juga metode pengenalan pola serangan berdasarkan atribut-atribut paket data. | Penelitian ini menggunakan pendekatan eksperimental dengan DPI sebagai alat utama untuk mendeteksi pola serangan ransomware dalam jaringan. | Sistem menggunakan DPI yang didukung dengan Snort dan rule-based signature untuk mendeteksi paket data berbahaya yang terkait dengan serangan ransomware WannaCry. Proses deteksi melibatkan identifikasi atribut paket seperti protokol, port, dan TLS. | Penelitian menggunakan metode pattern matching untuk mendeteksi pola-pola serangan yang terdapat dalam paket data jaringan dan menghasilkan visualisasi serangan. |

|  |  |
| --- | --- |
| Hasil | |
| Sistem DPI mampu mendeteksi serangan WannaCry dengan memanfaatkan pola paket data seperti JA3 fingerprint, protokol TLS, dan informasi header paket lainnya. | |
| Kelebihan | Kekurangan |
| Penelitian ini memberikan solusi praktis untuk mendeteksi ransomware pada jaringan lokal dengan metode DPI, termasuk pemanfaatan Snort sebagai IDS. | Keterbatasan dalam mengidentifikasi tipe ransomware lain selain WannaCry dan kurangnya uji pada serangan dengan tingkat kompleksitas lebih tinggi |
| Saran penulis | |
| implementasi sistem deteksi ransomware dengan metode Deep Packet Inspection (DPI) yang dapat menganalisis lalu lintas jaringan secara mendalam untuk mengidentifikasi ancaman ransomware pada jaringan SMK Negeri 1 Palembang. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Ransomware Detection Using Machine Learning: A Survey | Amjad Alraizza, Abdulmohsen Algarni | Agustus 2023 | Big Data and Cognitive Computing (BDCC), MDPI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| tantangan dalam mendeteksi ransomware yang terus berkembang serta meningkatkan teknik pendeteksian menggunakan Machine learning. | Artikel ini menggunakan metode survei literatur untuk mengevaluasi berbagai pendekatan pembelajaran mesin dalam mendeteksi ransomware. | memfokuskan pada teknik deteksi berbasis pembelajaran mesin, termasuk deteksi berbasis signature-based detection, analisis statis, analisis dinamis, serta teknik berbasis perilaku. Membandingkan algoritma-algoritma machine learning yang digunakan dalam deteksi ransomware, seperti decision tree, random forest, support vector machine, dan jaringan neural. | Algoritma yang dibahas meliputi decision tree, random forest, support vector machine, dan jaringan neural |

|  |  |
| --- | --- |
| Hasil | |
| Penelitian ini mengidentifikasi bahwa pendekatan pembelajaran mesin efektif untuk mendeteksi ransomware, terutama melalui analisis pola perilaku file atau sistem. | |
| Kelebihan | Kekurangan |
| Menyediakan survei komprehensif mengenai teknik machine learning untuk deteksi ransomware, memberikan perbandingan dari berbagai algoritma untuk mendeteksi ransomware | Tidak ada eksperimen empiris langsung, lebih fokus ke teori. |
| Saran penulis | |
| pengembangan model deteksi ransomware berbasis machine learning yang lebih efisien dan akurat untuk menangani pola serangan ransomware yang semakin kompleks. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review | Latifa Albshaier, Seetah Almarri, M. M. Hafizur Rahman | Agustus 2024 | Information, MDPI |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Artikel ini mengevaluasi metode deteksi dini ransomware yang efektif dalam mencegah kerusakan lebih lanjut. Fokus utamanya adalah pada deteksi berdasarkan tanda-tanda, pola perilaku, dan teknik pembelajaran mesin untuk mendeteksi ransomware sebelum merusak sistem. Studi ini mencakup ulasan sistematis literatur dari tahun 2020 hingga 2024. | Systematic literature review (SLR) dengan mengumpulkan, menyaring, dan menilai literatur relevan mengenai deteksi ransomware. Proses seleksi menggunakan diagram PRISMA | Deteksi berbasis tanda tangan, pola perilaku, dan algoritma pembelajaran mesin untuk meningkatkan kemampuan deteksi ransomware. | Algoritma Machine learning yang dianalisis meliputi support vector machine, decision trees, dan jaringan neural, pendekatan hybrid yang menggabungkan beberapa metode deteksi. |

|  |  |
| --- | --- |
| Hasil | |
| Artikel ini menemukan bahwa metode deteksi berbasis perilaku dan machine learning memberikan akurasi tinggi dalam mendeteksi ransomware. | |
| Kelebihan | Kekurangan |
| Memberikan tinjauan komprehensif tentang berbagai teknik deteksi ransomware | Fokus pada analisis teoritis sehingga kurang aplikatif dalam implementasi praktis. |
| Saran penulis | |
| pemanfaatan algoritma machine learning yang mampu mendeteksi tanda-tanda ransomware pada tahap awal infeksi, serta penggunaan analisis perilaku yang akurat untuk mengenali pola-pola serangan. | |

|  |  |
| --- | --- |
| Relavan | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| An Improved Protection Approach for Protecting from  Ransomware Attacks | Ferhat Guvci, Ahmet Senol | Juli 2023 | Journal of Data Applications |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Artikel ini meneliti dampak serangan ransomware pada organisasi dan individu serta mengevaluasi efektivitas langkah-langkah perlindungan yang ada. | Penelitian ini menggunakan tinjauan literatur komprehensif, menganalisis literatur yang relevan dan data dari kejadian ransomware nyata untuk mengevaluasi metode pencegahan yang efektif. | Pendekatan multilayer defense yang diterapkan dalam penelitian ini mencakup langkah-langkah teknis, administratif, dan hukum. peran algoritma Machine learning seperti LightGBM dalam mendeteksi ransomware melalui analisis file dan pola. | LightGBM digunakan untuk membedakan antara file terenkripsi dan tidak terenkripsi berdasarkan berbagai fitur statistik. |

|  |  |
| --- | --- |
| Hasil | |
| Penelitian ini menunjukkan bahwa metode keamanan biasa (seperti antivirus dan firewall) tidak selalu efektif dalam mencegah ransomware. Pendekatan berbasis AI dan machine learning dapat mempercepat deteksi dan meningkatkan akurasi, terutama dalam mengidentifikasi ancaman yang belum dikenal. | |
| Kelebihan | Kekurangan |
| Membahas secara rinci metode pencegahan dengan menggunakan teknik yang berbasis pada pola perilaku. | Fokus utama pada analisis teoritis, tanpa studi kasus terperinci. |
| Saran penulis | |
| pengembangan metode pemantauan real-time yang dapat segera mendeteksi perilaku mencurigakan serta menerapkan enkripsi data yang kuat untuk mencegah akses ransomware. | |

|  |  |
| --- | --- |
| Relavan | 4 |

1. **Privacy and Data Security**

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| KEAMANAN DAN PRIVASI DATA DALAM LINGKUNGAN CLOUD  COMPUTING: TANTANGAN DAN SOLUSI | Suhada & Muhammad Irwan Padli Nasution, | Oktober 2023 | Jurnal Multidisiplin Saintek |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Jurnal ini mengkaji tentang tantangan dalam keamanan dan privasi data dalam cloud computing | Jurnal ini menggunakan literatur review dalam mengidentifikasi keamanan dan privasi dalam cloud computing serta solusi yang sudah diterapkan dalam berbagai penelitian terdahulu | Penelitian ini menggunakan metode literatur rivew yang menelibatkan  penelusuran dan pengumpulan literatur terkait yang relevan dengan topik penelitian  seperti jurnal ilmiah. Kemudian dilanjutkan dengan meninjau seluruh artikel yang  diproleh, mengkategorikannya sesuai dengan subtopik yang akan dibahas  selanjutnya menyusunnya agar dapat dijadikan referensi untuk mendalami teknologi  cloud computing. | Algoritma yang didukung seperti AES ( Advanced Encryption Standard ) yang berguna mengencrypt data yang ada dan NIDS ( Network Instrusion Detection System ) untuk mendeteksi pola yang mencurigakan |

|  |  |
| --- | --- |
| Hasil | |
| Studi ini mengidentifikasi tantangan utama seperti perlindungan data sensitif, akses tidak sah, kompromi identitas, dan risiko kehilangan data. Solusi yang diusulkan mencakup enkripsi data, autentikasi multifaktor, dan kebijakan keamanan yang ketat | |
| Kelebihan | Kekurangan |
| Memberikan pandangan komprehensif dan solusi terkait tantangan cloud | Tidak menyajikan studi kasus atau uji lapangan terkait efektivitas solusi |
| Saran penulis | |
| Perlu penelitian lanjutan untuk menguji efektivitas solusi di berbagai skenario cloud | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| ANALISIS DAMPAK REGULASI PRIVASI DATA TERHADAP MANAJEMEN  KEMANAN DATA DI SEKTOR BISNIS | Hanifa Salsabila & Irwan Padli Nasution | Oktober 2024 | Jurnal Multidisiplin Saintek |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Dampak regulasi privasi data, seperti GDPR, terhadap keamanan data di sektor bisnis | Penelitian ini menggunakan pendekatan kualitatif dengan studi kasus pada perusahaan yang terpengaruh regulasi GDPR. Studi kasus digunakan untuk memahami secara mendalam bagaimana implementasi regulasi memengaruhi kebijakan dan sistem keamanan data dalam perusahaan | Wawancara mendalam dilakukan untuk mendapatkan perspektif dari pengelola keamanan data mengenai tantangan dan perubahan kebijakan yang diakibatkan oleh regulasi serta mengobservasi langsung pada perusahaan untuk mengamati implementasi teknologi keamanan yang terkait dengan privasi data. | Menggunakan IDS (Instruction Detection System) yang mengidentifikasi akses yang tidak sah atau serangan pada jaringan perusahaan. IDS memantau lalu lintas jaringan untuk mendeteksi pola-pola yang mencurigakan dan mengirimkan peringatan jika ditemukan anomali. |

|  |  |
| --- | --- |
| Hasil | |
| Implementasi regulasi privasi mendorong perusahaan untuk meningkatkan standar keamanan, seperti enkripsi, deteksi intrusi, dan kebijakan respons insiden, yang secara keseluruhan meningkatkan keamanan data pelanggan dan mencegah kebocoran data | |
| Kelebihan | Kekurangan |
| Memberikan pandangan komprehensif mengenai dampak regulasi privasi data terhadap manajemen keamanan data di perusahaan | Implementasi sistem keamanan sering kali mahal dan membutuhkan waktu untuk menyesuaikan proses bisnis yang ada dengan regulasi yang berlaku |
| Saran penulis | |
| Perlu investasi dalam pelatihan berkelanjutan dan peningkatan teknologi keamanan | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Privasi dan Keamanan Penerapan IoT dalam Kehidupan Sehari-hari: Tantangan dan Implikasi | Fauzan Prasetyo Eka Putra, Selly Mellyana Dewi, Maugfiroh, Amir Hamzah | Juli 2023 | Jurnal Sistim Informasi dan Teknologi |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Tantangan privasi dan keamanan dalam penerapan Internet of Things (IoT) di sektor domestik dan bisnis | Penggunaan metodologi kualitatif, studi literatur dan observasi terhadap tantangan keamanan IoT serta implikasi bagi pengguna domestik dan bisnis | Metode yang digunakan seperti wawancara dan observasi langsung dimana data dari sumber primer melalui wawancara ahli IoT dan mengamati penggunaan teknologi IoT pada perangkat rumah tangga dan industri | Algoritma SSL/TLS digunakan untuk mengamankan transmisi data antar perangkat. Algoritma IDS memantau lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan |

|  |  |
| --- | --- |
| Hasil | |
| Peningkatan kebutuhan akan protokol keamanan seperti enkripsi data, otentikasi perangkat, dan pemantauan jaringan untuk menjaga privasi pengguna IoT | |
| Kelebihan | Kekurangan |
| Menghadirkan solusi keamanan yang relevan dan terkini untuk tantangan IoT | Kompleksitas implementasi teknologi keamanan dalam skala besar serta biaya tinggi untuk sistem perlindungan komprehensif |
| Saran penulis | |
| Pengembangan regulasi dan edukasi pengguna terkait pentingnya keamanan data dalam perangkat IoT | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Masalah Privasi dan Keamanan Data Pribadi pada Penerapan Kecerdasan Buatan | Andika M. Soemarno | Juni 2023 | Innovative: Journal of Social Science Research |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Tantangan dalam menjaga keamanan dan privasi data pribadi dalam penerapan Kecerdasan Buatan (AI) | Menggunakan studi literatur untuk menganalisis tantangan keamanan data pribadi yang dihadapi pengguna dalam aplikasi AI, dengan fokus pada bagaimana AI mengakses data tanpa izin pengguna | Menganalisis sumber literatur akademik yang relevan untuk memahami peran AI dalam mengakses dan mengolah data pribadi, menekankan kebutuhan regulasi yang melindungi privasi pengguna. | memanfaatkan analisis Big Data untuk mengumpulkan data dari pengguna, yang diolah dengan algoritma machine learning untuk menghasilkan prediksi atau personalisasi layanan, namun juga berpotensi melanggar privasi pengguna |

|  |  |
| --- | --- |
| Hasil | |
| Temuan menunjukkan bahwa AI dapat dengan mudah mengakses data pribadi melalui Big Data dan memanfaatkan data tanpa sepengetahuan pengguna, mengindikasikan kebutuhan mendesak untuk regulasi privasi yang lebih ketat. | |
| Kelebihan | Kekurangan |
| Memberikan wawasan mendalam tentang dampak AI terhadap privasi data pribadi, dan relevan dengan diskusi kebijakan privasi | Ketergantungan pada studi literatur membuat temuan kurang aplikatif dalam konteks praktis; perlu data empiris untuk memperkuat argumen |
| Saran penulis | |
| Rekomendasi untuk kolaborasi antara pemerintah, masyarakat, dan perusahaan teknologi guna memastikan keamanan data pribadi dalam penggunaan AI | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Pengaruh Keamanan Data Privasi Terhadap Minat Untuk Melakukan Transaksi Online | Sofatun Nisa, Muhammad Irwan Padli Nasution; | Juni 2023 | IJM: Indonesian Journal of Multidisciplinary |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Pengaruh keamanan dan privasi data terhadap kepercayaan dan minat konsumen dalam transaksi online | menggabungkan analisis peraturan dan observasi lapangan untuk memahami hubungan antara persepsi keamanan dan minat konsumen | Pengumpulan data primer melalui observasi langsung dan wawancara dengan para ahli untuk memahami dampak keamanan dan privasi terhadap minat konsumen | Algoritma enkripsi, berguna untuk melindungi data selama transmisi, lalu IDS untuk memantau akses tak sah pada sistem |

|  |  |
| --- | --- |
| Hasil | |
| Ditemukan bahwa persepsi positif terhadap keamanan dan privasi data mendorong kepercayaan konsumen dalam transaksi online dan meningkatkan minat untuk berbelanja online | |
| Kelebihan | Kekurangan |
| Memberikan perspektif komprehensif terkait pentingnya keamanan data dalam bisnis e-commerce | Tidak ada data kuantitatif empiris yang menguatkan hubungan antarvariabel; studi lebih lanjut diperlukan untuk penguatan data |
| Saran penulis | |
| Menyarankan kolaborasi antar industri untuk meningkatkan keamanan dan menerapkan kebijakan privasi yang transparan bagi konsumen | |

|  |  |
| --- | --- |
| Relavan | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Judul | Nama Penulis | Tahun/Bulan | Penerbit |
| Metaverse dan Implikasinya pada Privasi dan Keamanan Data Pengguna | Rachmat Adiaz Arrofi, Rahman Ajie, Dziqra Ananda Hersya, Tata Sutabri; | Januari 2024 | IJM: Indonesian Journal of Multidisciplinary |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah yang dikaji | Metodologi | Metode | Algoritma |
| Tantangan privasi dan keamanan data pengguna dalam lingkungan Metaverse | Penerapan deskriptif kualitatif untuk menggambarkan implikasi Metaverse terhadap privasi dan keamanan data. Studi ini menganalisis secara mendalam dampak teknologi Metaverse pada hak privasi pengguna | Data dikumpulkan melalui observasi lingkungan Metaverse dan wawancara dengan ahli untuk memahami bagaimana privasi dan keamanan data pengguna dapat terancam | Penggunaan enkripsi end-to-end untuk mengamankan data pengguna dalam transmisi serta sistem keamanan multi-tahap yang menjaga integritas data dari serangan siber |

|  |  |
| --- | --- |
| Hasil | |
| Temuan menunjukkan bahwa keterlibatan pengguna dalam lingkungan Metaverse menciptakan potensi ancaman terhadap privasi mereka, dengan banyaknya data pribadi yang dikumpulkan oleh platform. Pentingnya regulasi dan pendekatan keamanan proaktif sangat ditekankan | |
| Kelebihan | Kekurangan |
| Menyediakan pandangan kritis dan solusi konkret terkait tantangan privasi dan keamanan data dalam Metaverse | Memerlukan regulasi yang jelas dan implementasi teknologi yang cukup canggih untuk mengatasi tantangan yang diidentifikasi, membutuhkan kerjasama antar lembaga |
| Saran penulis | |
| Mengusulkan peningkatan regulasi yang mengatur penggunaan data pengguna serta edukasi kepada pengguna tentang keamanan digital dalam Metaverse | |

|  |  |
| --- | --- |
| Relavan | 5 |

**Tugas Akhir dari repository.mikroskil.ac.id**

|  |  |  |
| --- | --- | --- |
| Judul TA | Nama Penulis | Tahun |
| IMPLEMENTASI BLOC KCHAIN UNTUK MENDETEKSI PLAGIARISME GAMBAR PADA APLIKASI MEDIA SOSIAL | Jenny Kinata, Anggi Saputra Edwarsa Siregar, Louis | 2021 |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah | Tujuan | Metode | Algoritma |
| Jurnal ini membahas bagaimana mendeteksi dan mencegah terjadinya plagiarisme gambar. | Membuat dan mengembangkan aplikasi mobile dan web yang dapat mendeteksi plagiat pada gambar menggunakan teknologi Blockchain. | Metode yang digunakan di TA ini adalah analisis proses, kebutuhan fungsional, kebutuhan non fungsional, melakukan perancangan database, membuat rancangan dengan Mockup, membuat aplikasi web dan mobile, pengujian dengan blackbox testing, autentikasi menggunakan Probability of false negative dan Probability false positive. | AES-128, PIECES(Performance, Information, Economic, Control, Efficiency, dan Services), ERD, PFN, dan, PFP |

|  |
| --- |
| Metode Penyelesaian Masalah |
| Blockchain untuk menyimpan data autentikasi gambar untuk memastikan keaslian gambar, autentikasi dan enkripsi gambar menggunakan AES – 128, Kompresi dan Analisis DCT untuk mendeteksi plagiarisme, dan pengembangan aplikasi web dan mobile |
| Kesimpulan |
| TA ini dapat menjadi referensi untuk pembelajaran dan penelitian implementasi Blockchain untuk mendeteksi plagiarisme pada gambar di media sosial. |
| Saran |
| Untuk uji coba pada gambar mungkin bisa dicoba untuk variasi gambar yang lebih unik dan luas agar dapat mengukur akurasi pada proses deteksi |

|  |  |
| --- | --- |
| Rating | 5 |

|  |  |  |
| --- | --- | --- |
| Judul TA | Nama Penulis | Tahun |
| PENGAMANAN DATA MENGGUNAKAN ALGORITMA RANDOM KEY MAES DAN MLSB | Herman Wijaya, Putra Hardi, Edwin | 2019 |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah | Tujuan | Metode | Algoritma |
| Kelemahan pada metode AES dalam pengacakan kunci dan perhitungan MixColumns yang kompleks, serta keterbatasan metode LSB yang terlalu umum dan memiliki tingkat kompleksitas rendah. | Tujuan TA ini adalah mengembangkan aplikasi yang meningkatkan proteksi data melalui kombinasi algoritma RK-MAES dan metode steganografi MLSB, serta mengevaluasi keamanan kunci, waktu enkripsi-dekripsi, dan nilai PSNR serta MSE dari MLSB. | Penelitian ini menggunakan metode Random Key Modified AES (RK-MAES) untuk enkripsi, Modified Least Significant Bit (MLSB) untuk steganografi, dan pendekatan Waterfall dalam pengembangan sistem, meliputi analisis, perancangan, pembuatan, serta pengujian keamanan kunci, kecepatan enkripsi-dekripsi, dan kualitas citra stego dengan PSNR dan MSE. | Random Key Modified AES (RK-MAES) sebagai algoritma enkripsi yang dimodifikasi untuk meningkatkan keamanan, serta Modified Least Significant Bit (MLSB) sebagai algoritma steganografi untuk menyembunyikan data di dalam citra digital. |

|  |
| --- |
| Metode Penyelesaian Masalah |
| TA ini menggunakan pendekatan *Waterfall*, meliputi analisis kebutuhan, perancangan antarmuka, pengembangan sistem dengan C#, dan pengujian keamanan kunci RK-MAES, kecepatan enkripsi-dekripsi, serta kualitas citra stego MLSB menggunakan MSE dan PSNR. |
| Kesimpulan |
| TA ini mengembangkan aplikasi yang meningkatkan keamanan data menggunakan algoritma RK-MAES dan MLSB, dengan hasil baik dalam keamanan kunci, kecepatan enkripsi-dekripsi, serta kualitas citra stego. |
| Saran |
| Pada bagian pengujian dapat ditambahkan variasi serangan siber yang lain pada algoritma RK-MAES dan MLSB agar dapat mengukur ketahanan sistem secara lebih terperinci |

|  |  |
| --- | --- |
| Rating | 5 |

|  |  |  |
| --- | --- | --- |
| Judul TA | Nama Penulis | Tahun |
| IMPLEMENTASI BLOCKCHAIN DALAM PENGEMBANGAN APLIKASI CROWDFUNDING BERBASIS WEBSITE | Johnson Rouslie Junior, Hezkya Natanael Ramli, Jesslyn Lim | 2023 |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah | Tujuan | Metode | Algoritma |
| Sistem crowdfunding saat ini adalah masih bersifat tersentralisasi, sehingga kurang optimal dalam memenuhi kebutuhan transparansi dan keamanan data. | Aplikasi croudfunding yang memanfaatkan blockchain berbasis website dengan sistem yang terdesentralisasi agar dapat meningkatkan transparansi dan keamanan data. | Menggunakan cryptocurrency dan koin USDC.  Pengecekan transparansi data menggunakan tracker Solana(Solscan).  Pengujian keamanan data dilakukan menggunakan test case yang diuji langsung ke smart contract rancangan. | Algoritma menggunakan jaringan Blockchain Solana |

|  |
| --- |
| Metode Penyelesaian Masalah |
| Penggunaan blockchain Solana untuk keamanan dan desentralisasi, stable coin USDC untuk menjaga kestabilan nilai donasi, Solscan untuk verifikasi transparansi transaksi, dan pengujian smart contract. |
| Kesimpulan |
| Aplikasi crowdfunding yang memanfaatkan blockchain berbasis website dengan sifat sistem desentralisasi untuk meningkatkan transparansi dan keamanan data . |
| Saran |
| mempertimbangkan pengujian dengan skala pengguna yang lebih besar guna mengevaluasi performa dan keandalan aplikasi crowdfunding ini di kondisi nyata |

|  |  |
| --- | --- |
| Rating | 5 |

|  |  |  |
| --- | --- | --- |
| Judul TA | Nama Penulis | Tahun |
| FRAUD DETECTION PADA E-COMMERCE BERDASARKAN POLA AKTIVITAS KONSUMEN DENGAN MENGGUNAKAN METODE BAYESIAN NETWORK BERBASIS MOBILE DAN WEB | Riandy Irvan Winargo, Danny Tandean | 2019 |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah | Tujuan | Metode | Algoritma |
| Meningkatnya penipuan pada lingkungan e-commerce karena rendahnya mekanisme pencegahan penipuan pada lingkungan e-commerce | Aplikasi mobile dan web yang mengintergrasikan metode Bayesian Network untuk mendeteksi fraud | Studi pustaka, analisis kebutuhan, desain sistem, implementasi, pengujian unit, dan pengujian hasil. Studi pustaka dilakukan untuk mengumpulkan referensi tentang Bayesian Network dan dataset terkait fraud. Analisis kebutuhan menggunakan Use Case Diagram, PIECES, dan Flowchart. Desain sistem mencakup model data dengan ERD dan antarmuka dengan Mockup Balsamiq. | Bayesian Network digunakan untuk mendeteksi dan menganalisis pola perilaku pengguna terkait deteksi fraud pada transaksi e-commerce |

|  |
| --- |
| Metode Penyelesaian Masalah |
| Bayesian Network untuk mendeteksi fraud berdasarkan pola perilaku pengguna. User behavior detection diterapkan untuk memantau aktivitas mencurigakan, Conditional Probability Table (CPT) digunakan untuk mengukur akurasi deteksi fraud, dan BlackBox testing memastikan fungsionalitas aplikasi sesuai spesifikasi. |
| Kesimpulan |
| Bayesian Network pada deteksi fraud e-commerce dapat meningkatkan keamanan dan kepercayaan pengguna dengan mendeteksi aktivitas mencurigakan secara akurat. |
| Saran |
| Mempertimbangkan pengujian performa tambahan (seperti uji respons waktu) untuk memperkuat hasil dan efektifitas algoritma bayesian network |

|  |  |
| --- | --- |
| Rating | 5 |

|  |  |  |
| --- | --- | --- |
| Judul TA | Nama Penulis | Tahun |
| ANALISIS DAN PERANCANGAN APLIKASI PEMBAYARAN OTOMATIS | Ammar Yasir Nasution, Daniel Indra Octo Pardomuan | 2020 |

|  |  |  |  |
| --- | --- | --- | --- |
| Masalah | Tujuan | Metode | Algoritma |
| Proses pembayaran di supermarket masih menggunakan kasir, yang menyebabkan konsumen harus mengantri untuk menyelesaikan pembayaran.  Proses antrian menyebabkan pembayaran menjadi kurang efisien dan memakan waktu. | Menghasilkan perancangan aplikasi pembayaran otomatis dengan teknologi QR Code yang dapat dimanfaatkan oleh pihak supermarket untuk menggantikan penggunaan kasir dalam proses pembayaran. | Studi pustaka, Model Waterfall, analisis dengan kerangka PIECES, dan diagram fishbone | QR code, NFC untuk verifikasi saldo, validasi keamanan transaksi. |

|  |
| --- |
| Metode Penyelesaian Masalah |
| Menngidentifikasi masalah dengan diagram fishbone, menggunakan kerangka PIECES untuk analisis sistem, pengembangan sistem dengan model waterfall, perancangan sistem menggunakan mockup dan ERD.x |
| Kesimpulan |
| Aplikasi pembayaran otomatis dengan teknologi OR code agar dapat digunakan oleh pihak supermarket. |
| Saran |
| Diharapkan untuk bagian pemilihan metode diberikan alasan yang lebih rinci sebagai dasar penggunaan metode yang dipilih |

|  |  |
| --- | --- |
| Rating | 5 |

LOGBOOK ( Oktober 14 – November 10 )

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Bulan** | **Minggu** | **Tanggal** | **Hari** | **Apa yang didapatkan** | | **Kendala** |
| Oktober | Minggu 1 | 14 | Senin | Pembuatan Kelompok | | Kekurangan anggota |
| 15 | Selasa |
| 16 | Rabu |
| 17 | Kamis | Menentukan Tema, Topik | | - |
| 18 | Jumat |
| 19 | Sabtu |
| 20 | Minggu | Mulai mencari referensi melalui Google Scholar | Memasukan hasil pencarian dan hasil review ke dalam Excel | Ada beberapa Jurnal yang dikunci dibalik paywall ataupun ingin melakukan login untuk akses |
| Minggu 2 | 21 | Senin |
| 22 | Selasa |
| 23 | Rabu | Di beberapa Jurnal tidak tertulis metode & algoritma yang dipakai |
| 24 | Kamis |
| 25 | Jumat |
| 26 | Sabtu | Mencari Judul Skripsi dari Repository Mikroskil | Banyak Skripsi yang tidak sesuai dengan tema |
| 27 | Minggu |
| Minggu 3 | 28 | Senin |
| 29 | Selasa |
| 30 | Rabu |
| 31 | Kamis |
| November | 1 | Jumat |
| 2 | Sabtu | Penggunaan GitHub Repository  <https://github.com/Filburb/Metodologi_Penelitian_Tugas_Kelompok> | | Anggota tidak dapat melakukan Git-Push |
| 3 | Minggu |
| Minggu 4 | 4 | Senin | Pemindahan Table Excel ke Word | | Terjadi Duplication saat pemindahan |
| 5 | Selasa |
| 6 | Rabu | Memasukan sisa hasil pencarian ke dalam word | Melakukan double check & Finishing |  |
| 7 | Kamis |  |
| 8 | Jumat |  |
| 9 | Sabtu | - |
| 10 | Minggu |  |  |