|  |  |
| --- | --- |
| **Judul Penelitian:** | Pengujian Keamanan Website Sistem Informasi Akademik Universitas X menggunakan Teknik Penetration Testing berdasarkan OWASP TOP 10 |
| **Urain Pokok Masalah:** | Uraian pokok masalahnya adalah meningkatnya kompleksitas teknologi informasi dan ancaman siber yang membuat keamanan sistem informasi menjadi sangat penting, terutama setelah beberapa website milik Universitas X mengalami serangan peretasan yang menyebabkan deface. Situs penting seperti Sistem Informasi Akademik rentan terhadap celah keamanan yang dapat menyebabkan kerugian finansial, merusak reputasi, dan melanggar privasi data mahasiswa. Oleh karena itu, penting dilakukan pengujian keamanan Sistem Informasi Akademik untuk mengevaluasi tingkat keamanannya. |
| **Solusi** | Solusi yang diusulkan adalah melakukan pengujian keamanan lebih mendalam terhadap website Sistem Informasi Akademik menggunakan OWASP Testing Framework. Dengan menggunakan kerangka kerja ini, diharapkan dapat memberikan struktur yang lebih terorganisir dan komprehensif dalam menemukan berbagai celah keamanan yang lebih rinci dan terperinci pada sistem yang diuji. Selain itu, implementasi standar keamanan seperti OWASP Top 10 juga dapat membantu dalam mengidentifikasi dan mengevaluasi celah keamanan yang signifikan pada sistem, serta memberikan arah yang tepat dalam meningkatkan tingkat keamanan pada website Sistem Informasi Akademik. |
| **Sumber** | JATI (Jurnal Mahasiswa Teknik Informatika) Vol. 8 No. 1, Februari 2024. |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Tantangan dan Strategi Manajemen Keamanan Siber di  Indonesia berbasis IoT |
| **Urain Pokok Masalah:** | Isu-isu utama yang dibahas dalam penelitian tentang manajemen keamanan siber di Indonesia berbasis IoT meliputi:   1. Meningkatnya Risiko Keamanan Siber: Meningkatnya adopsi teknologi IoT telah meningkatkan risiko keamanan siber secara signifikan, yang mengarah ke lebih banyak rute dan kerentanan potensial serangan. Hal ini menjadi tantangan bagi bisnis untuk beradaptasi dengan lanskap global dengan mengintegrasikan metode produksi tradisional dengan teknologi canggih. 2. Kekhawatiran Keamanan Informasi: Keamanan informasi telah menjadi fokus utama bagi bisnis di seluruh dunia karena operasi mereka di pasar global, ketergantungan yang tinggi pada teknologi informasi, dan kehadiran online dan digital yang merajalela. Mengelola keamanan informasi sangat penting untuk mencegah ancaman keamanan dan pelanggaran privasi dalam sistem informasi dan infrastruktur jaringan. 3. Kompleksitas Keamanan IoT: Sistem IoT rentan terhadap serangan siber karena keragaman perangkat dan teknik ancaman yang canggih. Serangan-serangan ini sulit untuk dideteksi dan dimitigasi karena interaksi yang kompleks di seluruh jaringan yang didukung IoT. Ancaman dapat menggunakan berbagai metode seperti komunikasi terenkripsi, malware polimorfik, injeksi SQL, dan serangan spoofing untuk mem-bypass deteksi tanda tangan. 4. Kerentanan Elemen Manusia: Terlepas dari kemajuan teknologi, elemen manusia tetap menjadi kerentanan yang signifikan dalam keamanan IoT. Organisasi perlu menerapkan program pendidikan yang komprehensif untuk meningkatkan kesadaran pengguna akan risiko keamanan siber IoT. Ini termasuk pelatihan tentang praktik terbaik keamanan, taktik rekayasa sosial, prosedur akses fisik, dan penanganan data di seluruh titik kontak IoT.   Isu-isu utama ini menyoroti kebutuhan kritis akan strategi keamanan siber yang proaktif, teknologi canggih seperti AI dan blockchain, serta upaya edukasi dan kesadaran yang berkelanjutan untuk memitigasi risiko keamanan siber dalam ekosistem IoT di Indonesia. |
| **Solusi** | Solusi yang diusulkan untuk mengatasi tantangan manajemen keamanan siber di Indonesia berbasis IoT antara lain:   1. Tindakan Keamanan Terpadu: Menerapkan pendekatan keamanan yang komprehensif yang mencakup kontrol akses yang ketat, enkripsi data, deteksi anomali, pembaruan firmware, dan pemantauan berkelanjutan. Kolaborasi lintas departemen dapat meningkatkan kesadaran situasional dan memastikan langkah-langkah keamanan tertanam dan diperkuat di seluruh lanskap teknologi IoT. 2. Program Pendidikan dan Kesadaran: Organisasi harus melakukan program pendidikan yang komprehensif untuk meningkatkan kesadaran pengguna akan risiko keamanan siber IoT. Pelatihan tentang kebersihan keamanan, taktik rekayasa sosial, prosedur akses fisik, dan penanganan data di semua titik kontak IoT dapat meningkatkan ketahanan organisasi di lingkungan IoT yang terus berkembang. 3. Teknologi Keamanan Tingkat Lanjut: Memanfaatkan teknologi yang sedang berkembang seperti blockchain, mikrosegmentasi, dan jaringan pendeteksi penipuan untuk meningkatkan langkah-langkah keamanan. Teknologi ini menawarkan metode baru untuk verifikasi, kompartementalisasi, dan deteksi serangan dini, memperkuat ketahanan terhadap serangan multi-vektor kontemporer. 4. Strategi Keamanan Siber yang Proaktif: Mengembangkan strategi keamanan siber yang holistik dan proaktif yang mencakup pengenalan ancaman, pelatihan pengguna, pengembangan kebijakan, pemantauan dan deteksi dini, enkripsi data, manajemen akses, pencadangan data, dan kolaborasi dengan lembaga keamanan lainnya. Strategi-strategi ini harus dapat menjawab tantangan di era Revolusi Industri Keempat, dengan fokus pada berbagai aspek seperti pengetahuan, teknologi, ekonomi, sosial, dan politik.   Dengan menerapkan solusi-solusi ini, organisasi di Indonesia dapat meningkatkan postur keamanan siber mereka, memitigasi risiko yang terkait dengan teknologi IoT, serta memastikan keamanan dan integritas sistem informasi dan jaringan mereka dalam menghadapi ancaman siber yang terus berkembang. |
| **Sumber** | Zetroem. Vol 06 No 01. ISSN (Online): 2656-081X. Page -116. 2024 |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Penerapan Teknologi Blockchain dalam Industri Keuagan Syariah: Tantangan dan Peluang |
| **Urain Pokok Masalah:** | Isu-isu utama yang dibahas dalam penelitian tentang penerapan teknologi blockchain dalam industri keuangan syariah meliputi:   1. Kurangnya transparansi dalam industri ini. 2. Risiko penipuan dan masalah keamanan. 3. Inefisiensi dalam sistem keuangan saat ini. 4. Tantangan yang terkait dengan kepatuhan hukum dan prinsip-prinsip Syariah. 5. Kebutuhan akan standarisasi protokol dan regulasi dalam mengimplementasikan teknologi blockchain. 6. Keterbatasan teknologi saat ini dalam merealisasikan potensi manfaat blockchain dalam keuangan syariah. |
| **Solusi** | Solusi yang diusulkan untuk mengatasi masalah dalam penerapan teknologi blockchain di industri keuangan Islam meliputi:   1. Meningkatkan transparansi melalui sifat teknologi blockchain yang tidak dapat diubah dan terdesentralisasi. 2. Mengurangi risiko penipuan dengan menyediakan transaksi yang aman dan transparan. 3. Meningkatkan efisiensi dengan menyederhanakan proses dan mengurangi biaya administrasi. 4. Memastikan kepatuhan terhadap prinsip-prinsip Syariah melalui mekanisme tinjauan dan implementasi yang tepat. 5. Menetapkan protokol dan peraturan standar untuk mengatur penggunaan teknologi blockchain dalam keuangan syariah. 6. Mengatasi keterbatasan teknologi melalui inovasi dan pengembangan berkelanjutan di bidang teknologi blockchain. |
| **Sumber** | Jurnal Ekonomi dan Bisnis Islam. Vol 03, No 01, Maret 2024. E-ISSN: 2829-2995. https://ejournal.stais.ac.id/index.php/j-ebi/index |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Sistem Informasi Rekam Medik Pasien Sebagai  Implementasi Big Data Dengan NIK di Pelayanan  Kesehatan Kota Tegal |
| **Urain Pokok Masalah:** | Pokok Permasalahan:   1. Tidak dapatnya pasien mengakses data rekam medik mereka oleh seluruh pelayan kesehatan yang tersebar di wilayah tertentu. 2. Kesulitan dalam penelusuran riwayat penyakit dan obat pasien tanpa integrasi Nomor Induk Kependudukan (NIK) dalam sistem. 3. Keterbatasan dalam pengelolaan data puskesmas, dokter, dan pasien tanpa aplikasi yang memadai. 4. Kebutuhan akan evaluasi sistem informasi rekam medis pasien di Pelayanan Kesehatan Kota Tegal. 5. Perlunya metode penelitian dan pengembangan yang tepat untuk meningkatkan efektivitas dan efisiensi sistem informasi rekam medis. 6. Pentingnya perawatan rutin untuk menjaga kinerja maksimal sistem informasi rekam medis. |
| **Solusi** | Solusi yang dapat diusulkan untuk mengatasi pokok permasalahan yang telah disebutkan adalah:   1. Implementasi sistem informasi rekam medis yang memungkinkan akses data pasien secara terintegrasi oleh seluruh pelayan kesehatan di wilayah tersebut. 2. Integrasi Nomor Induk Kependudukan (NIK) dalam sistem online untuk memudahkan penelusuran riwayat penyakit dan obat pasien. 3. Pengembangan aplikasi yang memungkinkan pengelolaan data puskesmas, dokter, dan pasien secara efisien dan efektif. 4. Melakukan evaluasi sistem informasi rekam medis secara berkala untuk memastikan kualitas dan keefektifan sistem. 5. Menggunakan metode penelitian dan pengembangan yang tepat untuk meningkatkan kinerja sistem informasi rekam medis. 6. Melakukan perawatan rutin dan pemeliharaan sistem informasi rekam medis untuk mencegah kerusakan dan menjaga kinerja optimal sistem.   Dengan menerapkan solusi-solusi tersebut, diharapkan dapat meningkatkan efisiensi, akurasi, dan kualitas pelayanan kesehatan di Kota Tegal melalui implementasi Big Data dalam Sistem Informasi Rekam Medik Pasien. |
| **Sumber** | TRANSFORMATIKA. 2021. Vol: 18. Hal: 143-150. ISSN: 1693-3656 |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Sistem Deteksi Serangan Ddos pada Software Defined Network Menggunakan Metode Entropy |
| **Urain Pokok Masalah:** | Permasalahan utama yang diangkat dalam penelitian ini adalah deteksi serangan DDoS pada Software Defined Network (SDN) menggunakan metode Entropy. Penelitian ini bertujuan untuk mengidentifikasi serangan DDoS dengan memanfaatkan nilai threshold, windows size, dan count sebagai parameter deteksi. Penelitian ini penting karena jaringan SDN rentan terhadap serangan DDoS dan perlu adanya mekanisme deteksi yang efektif. |
| **Solusi** | Solusi yang diusulkan dalam penelitian ini adalah menggunakan metode Entropy untuk mendeteksi serangan DDoS pada Software Defined Network (SDN). Metode ini memanfaatkan nilai threshold, windows size, dan count sebagai parameter deteksi serangan DDoS. Dengan demikian, diharapkan sistem deteksi yang dikembangkan dapat efektif mengidentifikasi serangan DDoS pada jaringan SDN. |
| **Sumber** | Smart Comp. Hal: 615-628. Vol. 11 No. 4 Oktober 22. P-ISSN: 2089-676X. E-ISSN: 2549-0796 |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Analisis dan Verifikasi Protokol Kriptografi Aplikasi  Manajemen Kunci Menggunakan Scyther: Studi Kasus  Aplikasi XYZ |
| **Urain Pokok Masalah:** | Penelitian ini fokus pada analisis keamanan protokol aplikasi XYZ, dengan penekanan pada aspek autentikasi. Ditemukan bahwa protokol memiliki kelemahan dalam hal synchronization dan agreement, yang dapat membahayakan keamanan data. Untuk mengatasi masalah ini, penulis merekomendasikan penerapan lisensi dan cryptographic nonce sebagai solusi. Dengan implementasi ini, hasil pengujian menunjukkan bahwa protokol telah berhasil memenuhi properti keamanan yang diinginkan, khususnya terkait dengan autentikasi. |
| **Solusi** | Solusi untuk mengatasi kelemahan pada protokol aplikasi XYZ adalah dengan menerapkan shared secret dan rangkaian cryptographic nonce. Dengan penerapan ini, protokol dapat meningkatkan keamanan autentikasi dan mengurangi risiko kebocoran data yang disebabkan oleh kelemahan dalam synchronization dan agreement. |
| **Sumber** | Smart Comp. Hal: 563-573. Vol. 12 No. 2 April 2023. P-ISSN: 2089-676X. E-ISSN: 2549-0796 |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Pengaruh IoT pada Transformasi Jaringan Multimedia: Literatur Review |
| **Urain Pokok Masalah:** | * Pengaruh Internet of Things (IoT) terhadap transformasi jaringan multimedia. * Perubahan mendasar dalam arsitektur, kapabilitas, dan keamanan jaringan multimedia akibat integrasi IoT. * Tantangan terkait keamanan dan privasi data yang muncul. * Perlindungan data dan implementasi kebijakan keamanan sebagai aspek penting yang perlu diperhatikan. * Pentingnya kajian literatur sebagai landasan esensial untuk memahami peran krusial IoT dalam mengubah wajah jaringan multimedia. * IoT memainkan peran penting dalam transformasi jaringan multimedia. * Studi tentang IoT dalam konteks transformasi jaringan multimedia sebagai fokus perhatian yang semakin mendalam di era digital. * Peran krusial IoT dalam merintis perubahan signifikan dalam paradigma jaringan multimedia. * Dampak dan implikasi dari integrasi IoT terhadap evolusi jaringan multimedia. * Pengaruh IoT pada model bisnis pendidikan, pengabdian masyarakat di sekolah menengah atas, peran manajemen sumber daya manusia dalam era digital, akselerasi transformasi digital untuk pendidikan berkualitas, transformasi media dan dinamika komunikasi dalam era digital, dan pengaruh penggunaan media digital dalam menulis artikel populer. * Tantangan terkait keamanan dan privasi data yang perlu diperhatikan dalam integrasi IoT dalam jaringan multimedia. * Integrasi IoT dalam jaringan multimedia sebagai revolusi teknologi dan transformasi yang mengubah cara interaksi antar perangkat dan landscape multimedia. * Metode penelitian yang digunakan adalah literatur review. * Implementasi teknologi dalam proses produksi untuk efisiensi operasional. |
| **Solusi** | Beberapa solusi untuk mengatasi permasalahan yang muncul akibat integrasi Internet of Things (IoT) dalam transformasi jaringan multimedia antara lain meningkatkan pelatihan keterampilan SDM dalam mengadopsi teknologi efektif, mengintegrasikan teknologi ke dalam kurikulum pendidikan untuk mempersiapkan generasi mendatang, serta melakukan review literatur mendalam untuk pemahaman yang lebih baik tentang pengaruh IoT dalam transformasi jaringan multimedia.  Selain itu, perlunya upaya serius dalam pengembangan kebijakan keamanan dan privasi data menjadi sangat penting. Integrasi IoT dalam berbagai sektor, seperti industri, pendidikan, dan masyarakat, juga diperlukan untuk menghadapi tantangan dan memanfaatkan peluang yang muncul. |
| **Sumber** | Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI  Volume 7, Nomor 1, Tahun 2024, Hal 173-181  ISSN 2723- 6129 (media online)  Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Analisis StringMatching Method Pada Pengembangan Aplikasi E-Submission V2.0 Menggunakan Algoritma Boyer Moore |
| **Urain Pokok Masalah:** | Penelitian ini didasari oleh kebutuhan untuk meningkatkan efisiensi pencarian data dalam aplikasi e-submission. Algoritma Boyer-Moore dipilih sebagai solusi karena efisiensinya dalam mengidentifikasi pola dalam teks berdasarkan kata kunci dengan waktu yang lebih singkat. Dalam konteks penggunaan mesin pencari, algoritma Boyer-Moore dianggap sebagai alat pencocokan string yang kuat. Metode penelitian Systematic Literature Review digunakan untuk mengumpulkan informasi dari 18 artikel terkait, termasuk taksonomi literature yang menyajikan kumpulan penelitian terdahulu tentang penggunaan search engine dengan metode string matching dan algoritma Boyer-Moore. Hasil penelitian menunjukkan bahwa penggunaan algoritma Boyer-Moore dalam string matching dapat meningkatkan efektivitas proses pencarian data. Saran yang diberikan adalah melakukan benchmark dengan metode lain yang mendukung string matching dan menerapkan string matching pada aplikasi Esubmission v2. |
| **Solusi** | Solusi dari permasalahan efisiensi pencarian data dalam aplikasi e-submission adalah dengan menggunakan algoritma Boyer-Moore. Algoritma ini efisien dalam mengidentifikasi pola dalam teks berdasarkan kata kunci dengan waktu yang lebih singkat, sehingga dapat meningkatkan efektivitas proses pencarian data. Selain itu, benchmark dengan metode lain yang mendukung string matching dan menerapkan string matching pada aplikasi Esubmission v2 juga dapat membantu dalam meningkatkan efisiensi pencarian data. |
| **Sumber** | JATI (Jurnal Mahasiswa Teknik Informatika) Vol. 7 No. 3, Juni 2023. Hal 1806-1811 |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Relasi Sosiodemografi Terhadap Kesadaran Keamanan dan Privasi Data Pengguna WhatsApp di Provinsi Jawa Barat |
| **Urain Pokok Masalah:** | Masalah keamanan dan privasi dalam penggunaan media sosial, termasuk WhatsApp, menjadi perhatian karena risiko kebocoran data dan penyalahgunaan informasi pengguna yang dapat menyebabkan kejahatan online. Kondisi seperti membagikan terlalu banyak informasi pribadi dan mengklik tautan yang tidak aman dapat meningkatkan risiko keamanan informasi. Penyadaran akan pentingnya perlindungan data pribadi dan kesadaran keamanan informasi perlu ditingkatkan melalui edukasi dan literasi privasi. Sosiodemografi pengguna juga dapat memengaruhi kesadaran dan tindakan terkait keamanan informasi dalam penggunaan WhatsApp. |
| **Solusi** | Untuk mengatasi masalah keamanan dan privasi dalam penggunaan WhatsApp, beberapa solusi yang dapat dilakukan antara lain adalah:   1. Edukasi dan literasi privasi yang lebih intensif kepada pengguna untuk meningkatkan kesadaran akan pentingnya perlindungan data pribadi. 2. Mendorong pengguna untuk menggunakan pengaturan privasi dan keamanan yang disediakan oleh platform WhatsApp untuk mengendalikan informasi pribadi yang dibagikan. 3. Memperkuat regulasi dan pengawasan terhadap penyedia layanan media sosial untuk mencegah penyalahgunaan data pengguna. 4. Melakukan pembaruan secara teratur pada aplikasi WhatsApp untuk memperbaiki kerentanan keamanan yang ada.   Dengan implementasi solusi-solusi tersebut, diharapkan dapat meningkatkan keamanan dan privasi pengguna dalam penggunaan WhatsApp. |
| **Sumber** | JURNAL STUDI KOMUNIKASI DAN MEDIA Vol. 27 No. 1 (Januari – Juni 2023) Hal: 93 – 108 ISSN: 1978-5003 e-ISSN: 2407-6015 |

|  |  |
| --- | --- |
| **Judul Penelitian:** | Theory and practice in secure software development lifecycle: A comprehensive survey |
| **Urain Pokok Masalah:** | Latar belakang masalah yang dibahas dalam dokumen tersebut terkait dengan berbagai aspek keamanan, tata kelola, dan pengembangan dalam konteks teknologi yang sedang berkembang seperti Internet of Things (IoT), komputasi awan, dan sistem perangkat lunak. Dokumen ini mencakup topik-topik seperti tantangan keamanan dalam komputasi awan, pemodelan ancaman untuk sistem berbasis 5G, keamanan dalam siklus pengembangan perangkat lunak, protokol otentikasi untuk IoT, pencegahan pelanggaran data perusahaan, dan tata kelola TI dalam lingkungan DevOps. Selain itu, dokumen ini juga membahas isu-isu yang berkaitan dengan kualitas perangkat lunak, kepuasan kerja, akuntansi berkelanjutan, inovasi terbuka, pelestarian privasi di Internet of Drones, dan lingkungan yang berkelanjutan untuk mencegah kejenuhan dan gesekan dalam manajemen proyek. Dokumen ini juga membahas tentang operasionalisasi etika dalam kecerdasan buatan untuk perawatan kesehatan, tata kelola AI, dan dampak model bahasa besar untuk pendidikan. |
| **Solusi** | Solusi yang diusulkan untuk tantangan keamanan yang dibahas dalam dokumen tersebut meliputi:   1. Memitigasi risiko dan mendorong kontrol internal dalam lingkungan DevOps. 2. Membangun dan mengamankan Pusat Operasi Keamanan (SOC) modern. 3. Cluster dengan ketersediaan tinggi: Taksonomi, survei, dan arah masa depan. 4. Kerangka kerja misi pencarian dan penyelamatan dengan bantuan komputasi UAV untuk mitigasi bencana dan lingkungan yang keras. 5. Kerangka kerja pemodelan ancaman untuk sistem komunikasi bergerak. 6. Pada keamanan kontainer: Pemodelan ancaman, analisis serangan, dan strategi mitigasi. 7. Pemodelan ancaman sistem siber-fisik - Studi kasus sistem microgrid. 8. Grafik Properti Privasi: Menuju ancaman privasi otomatis. 9. Studi pemetaan sistematis tentang pendekatan keamanan dalam rekayasa perangkat lunak yang aman. 10. Investigasi tentang ancaman & solusi keamanan data. 11. Memahami keamanan perangkat lunak dari desain hingga penerapan. 12. Membangun sistem yang aman dan andal: Praktik terbaik untuk merancang, mengimplementasikan, dan memelihara sistem. 13. Protokol Kunci Simetris Berbasis MAC untuk Penerusan Lalu Lintas yang Aman di Drone. 14. Tata kelola adaptif untuk Internet of Things: Mengatasi risiko keamanan yang muncul. 15. Sebuah survei tentang tantangan keamanan dalam komputasi awan: Masalah, ancaman, dan solusi. 16. Pendekatan Berlapis untuk Pemodelan Ancaman untuk Sistem Berbasis 5G. 17. Praktik terbaik untuk memastikan keamanan di DevOps: Pendekatan studi kasus. |
| **Sumber** | World Journal of Advanced Research and Reviews, 2023, 18(03), 053–078. Publication history: Received on 11 April 2023; revised on 30 May 2023; accepted on 01 June 2023 . Article DOI: https://doi.org/10.30574/wjarr.2023.18.3.0944 |