Journal of International Multidisciplinary Research

Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi

Dola Ramalinda[1], Jayadi[2], Agung Rachmat Raharja[3]
Universitas Bandung[123], Bandung, Indonesia
dolaramalinda@bandunguniversity.ac.id[1], jayadi@bandunguniversity.ac.id[2],
agungmat@bandunguniversity.ac.id[3*]

Informasi Artikel
E-ISSN : 3026-6874
Vol: 2 No: 6 Juni 2024
Halaman : 665-671

Keywords:
Information Security
Cryptography
Cryptography Implementation

Abstract
Information security has become a top priority in the current digital era due to its critical role in safeguarding sensitive data from various threats such as malware, phishing, man-in-the- middle, and brute force attacks. In facing these challenges, cryptography emerges as a primary solution for data protection. This article outlines the types of threats to information systems, cryptographic techniques used in data protection, and the implementation of cryptography in information systems. The discussion includes the use of symmetric and asymmetric encryption, hashing, and digital signatures as measures to secure data from unauthorized access and ensure its integrity. Additionally, the article highlights the importance of risk assessment, selecting the appropriate cryptographic algorithms, secure key management, as well as regular testing and maintenance in cryptography implementation. By understanding and effectively implementing cryptographic techniques, organizations can mitigate the risk of data breaches and ensure optimal information security.

Abstrak
Keamanan informasi menjadi prioritas utama di era digital saat ini mengingat nilai pentingnya dalam melindungi data sensitif dari berbagai ancaman, seperti serangan malware, phishing, man-in-the-middle, dan brute force. Dalam menghadapi tantangan ini, kriptografi menjadi salah satu solusi utama untuk melindungi data sensitif. Artikel ini menguraikan jenis- jenis ancaman terhadap sistem informasi, teknik kriptografi yang digunakan dalam perlindungan data, serta implementasi kriptografi dalam sistem informasi. Diskusi meliputi penggunaan enkripsi simetris dan asimetris, hashing, dan tanda tangan digital sebagai langkah-langkah untuk melindungi data dari akses tidak sah dan memastikan integritasnya. Selain itu, artikel ini juga menyoroti pentingnya penilaian risiko, pemilihan algoritma kriptografi yang tepat, manajemen kunci yang aman, serta pengujian dan pemeliharaan rutin dalam implementasi kriptografi. Dengan memahami dan menerapkan teknik kriptografi secara efektif, organisasi dapat mengurangi risiko kebocoran data dan memastikan keamanan informasi yang optimal.

Kata Kunci: Keamanan Informasi, Kriptografi, Serangan, Implementasi Kriptografi

PENDAHULUAN

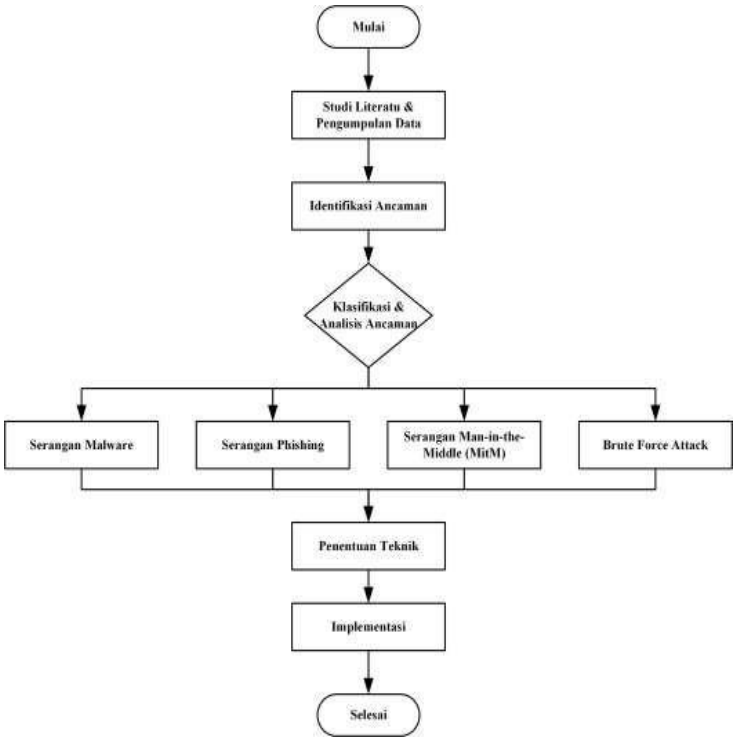
Di era digital yang terus berkembang dengan cepat, informasi dan data telah menjadi aset yang sangat penting. Hampir semua aspek kehidupan modern mengandalkan teknologi informasi dan komunikasi, mulai dari aktivitas sehari-hari individu hingga operasi bisnis berskala besar dan layanan pemerintahan. Oleh karena itu, perlindungan data dan keamanan informasi telah menjadi prioritas utama bagi organisasi di seluruh dunia. Keamanan informasi menjadi sangat krusial karena badan organsasi ataupun individu memiliki data sensitif yang tidak ingin diakses oleh orang lain(Raharja, Agung Rachmat, 2024)(Ramalinda et al., 2024)(Raharja et al., 2024)(Agung Rachmat Raharja, Jayadi, 2023)

Keamanan Informasi adalah upaya untuk melindungi aset informasi dari potensi ancaman. Keamanan informasi secara tidak langsung memastikan kelangsungan bisnis, mengurangi risiko yang muncul, dan memungkinkan Anda mengoptimalkan laba atas investasi (Puriwigati, 2020). Tantangan dalam menjaga keamanan informasi semakin kompleks seiring dengan meningkatnya ancaman siber. Hal ini dikarenakan Tingkat kekhawatiran terhadap serangan siber meningkat karena pelaku serangan tidak hanya menggunakan metode baru, tetapi juga semakin terstruktur dan mahir dalam menembus sistem.(Raharja et al., 2024)(Hariyanti et al., 2024)(Raharja et al., n.d.)

Dalam menghadapi tantangan ini(Dola Ramalinda, 2024), beberbagai metode dan teknologi telah dikembangan untuk meningkatkan keamanan informasi. Salah satu teknologi yang saat ini digunakan adalah Kriptografi. Kriptografi digunakan luas dalam keamanan komputer, komunikasi, sistem pembayaran elektronik, dan banyak aplikasi lainnya di mana perlindungan data sensitif sangat penting. Kriptografi digunakan dengan cara mengubah data menjadi bentuk yang tidak dapat dibaca dan mengembalikan data tersebut menjadi bentuk aslinya.

METODE

Metodologi penelitian adalah kerangka atau pendekatan sistematis yang digunakan peneliti untuk merencanakan, melakukan, dan menganalisis penelitian(Sutisna et al., 2024) Penelitian ini bertujuan untuk menganalisis berbagai jenis ancaman terhadap sistem informasi dan mengevaluasi efektivitas teknik kriptografi dalam melindungi data dari ancaman tersebut. Penelitian ini akan mencakup analisis ancaman malware, phishing, Man-in-the-Middle (MitM), dan brute force attack, serta penerapan teknik kriptografi seperti enkripsi, hashing, dan tanda tangan digital dalam sistem informasi



Gambar 1. Metode Penelitian

1. Pengumpulan Data

Data akan diperoleh melalui wawancara, survei, simulasi serangan, serta studi literatur(Muchsam et al., 2023) dan laporan keamanan siber. Pendekatan ini memungkinkan pengumpulan data primer dan sekunder yang komprehensif.

2. Klasisfikasi Analisis Ancaman

Penelitian akan menganalisis ancaman seperti malware, phishing, Man-in-the-Middle, dan brute force attack. Analisis ini bertujuan untuk mengidentifikasi potensi ancaman dan dampaknya terhadap sistem informasi.

3. Analisis Efektivitas Teknik Kriptografi

Evaluasi akan dilakukan terhadap teknik kriptografi seperti enkripsi, hashing, dan tanda tangan digital. Tujuannya adalah untuk mengukur seberapa baik teknik-teknik ini melindungi data dari ancaman serta menguji kinerja dan keamanannya.

4. Implementasi

Teknik kriptografi akan diimplementasikan berdasarkan penilaian risiko dan pemilihan algoritma yang tepat. Implementasi ini akan mempertimbangkan kebutuhan keamanan spesifik dari organisasi yang bersangkutan dengan memastikan sistem dapat merespons ancaman dengan efektif.

HASIL DAN PEMBAHASAN

JENIS-JENIS ANCAMAN TERHADAP SISTEM INFORMASI

1. Serangan Malware

Menurut (Manoppo et al., 2020)Malware, singkatan dari malicious software, adalah perangkat lunak yang dirancang untuk merusak, mengganggu, atau mengambil alih sistem komputer tanpa izin pengguna. Jenis-jenis malware meliputi virus, worm, trojan, dan ransomware(Maslan & others, 2020). Virus menyebar dengan menyisipkan kode mereka ke dalam program atau file lain, sementara worm dapat menyebar tanpa bantuan manusia melalui jaringan komputer. Trojan menyamar sebagai program yang berguna tetapi sebenarnya berisi kode berbahaya yang dapat mencuri informasi atau merusak sistem. Ransomware mengenkripsi data korban dan meminta tebusan untuk mendapatkan kunci dekripsi(Maslan & others, 2020).

Berdasarkan penelitian (Rahayu & Trianto, 2021)mengenai Analisis Malware dengan menggunakan metode analisis statis dan dinamis. Penelitian ini melibatkan lima spesimen malware yang diperoleh dari sensor Honeynet milik Badan Siber dan Sandi Negara (BSSN). Hasil analisis mengungkap bahwa kelima malware tersebut tergolong sebagai trojan yang sangat berbahaya karena mampu menghubungi domain-domain berbahaya untuk mengunduh program berpotensi merusak. Penelitian ini menunjukan bahwa dimungkinkan memasukan sebuah malware ke dalam sistem dengan tujuan yang merugikan. Malware memiliki kemampuan mengakses dan merusak data serta dapat mengiris informasi senmsitif ke pihak yang tidak berwenang. Dengan kehadiran malware dalam sebuah sistem dapat menyebabkan kerugian finansial, pencurian identitas, atau bahkan kebocoran informasi rahasia. Oleh karena ini, penting bagi indivodu atau oraganisasi untuk memahami dan menerpakan strategi perlingan yang efektif untuk mengurangi risiko serangan malware dan melindung kerahasian data mereka.

2. Serangan Phishing

Phising adalah penipuan online yang dilakukan melalui email, link, website, atau telepon palsu yang dibuat semirip mungkin dengan aslinya. Tujuannya yaitu untuk mendapatkan data dan informasi sensitif, seperti rekening bank atau username dan password(Faradilla, 2023). Penyerang sering menggunakan teknik sosial engineering untuk menipu korban agar mengungkapkan informasi pribadi mereka.

Penelitian yang dilakukan oleh (Ginanjar et al., 2018) mengenai analisis Analisis Serangan Web Phishing pada Layanan E-commerce dengan MetodeNetwork Forensic Process, ditemukan fake domain (host phishing) IP Address, DNS serta berbagai protokol yang terlibat dalam trasmisi. Hal ini menunjukan bahwa terdapat aktivitas Phising yang terjadi. Temuan ini menunjukkan bahwa aktivitas phishing aktif terjadi dalam lingkungan layanan e-commerce yang diselidiki. Akibatnya, aktivitas

phishing tersebut dapat menyebabkan kerugian finansial dan kehilangan informasi sensitif bagi organisasi atau individu yang menjadi target serangan phishing.

Ketika menghadapi ancaman seperti serangan phishing, implementasi teknologi kriptografi dapat menjadi salah satu langkah yang efektif dalam melindungi data sensitif. Dengan menerapkan kriptografi, informasi sensitif seperti kata sandi, informasi keuangan, dan data pengguna dapat dienkripsi sebelum dikirim melalui jaringan. Ini akan membuat data menjadi tidak dapat dimengerti bagi pihak yang tidak memiliki kunci dekripsi yang benar. Dengan demikian, meskipun data tersebut direbut oleh penyerang selama serangan phishing, informasi tersebut tetap terlindungi dan tidak dapat disalahgunakan.

3. Serangan Man-in-the-Middle (MitM)

Serangan man-in-the-middle (MitM) adalah jenis serangan siber di mana peretas menyadap data yang ditransfer antara dua pihak. Hal ini memungkinkan penyerang mengontrol komunikasi, mengelabui pihak-pihak yang sah agar percaya bahwa komunikasi mereka aman dan tidak terputus(Wiz Experts Team, 2024). Penyerang dapat memantau dan bahkan memanipulasi komunikasi antara kedua pihak tersebut tanpa sepengetahuan mereka. Ini dapat mengakibatkan pencurian informasi sensitif atau bahkan pemalsuan transaksi.

Penelitian yang dilakukan oleh (Aman, 2023) mengenai Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack Di Sekolah didapatkan bahwa simulasi serangan MitM menggunakan alat hacking Lapara Wifi Master, terungkap potensi ancaman yang dapat dimanfaatkan oleh pihak yang tidak berwenang untuk memantau atau memanipulasi komunikasi di dalam jaringan. Man in the middle attack memungkinkan peretas menempatkan dirinya di tengah-tengah percakapan para korban. Dalam hal ini, pelaku dapat melihat, mendengarkan, atau menyamar sebagai salah satu pihak dan membuatnya terlihat seperti pertukaran informasi yang berlangsung dengan normal. MITM attack ini juga mengincar data-data penting pengguna seperti kredensial login, informasi akun dan nomor kartu kredit.

4. Brute Force Attack

Brute force adalah upaya mendapatkan akses sebuah akun dengan menebak username dan password yang digunakan(Putri Aprilia, 2022). Serangan ini memerlukan waktu dan daya komputasi yang besar, tetapi dapat berhasil jika kata sandi atau kunci tersebut lemah atau mudah ditebak.

Hasil penelitian yang dilakukan oleh (Wardhana & Seta, 2021) mengenai Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ menunjukan bahwa terdapat Kerentanan yang dapat menyebabkan terjadinya bruce force attack pada halaman login. Dalam konteks ini, kriptografi dapat memainkan peran penting dalam memperkuat keamanan sistem dan mengurangi risiko brute force attack. Salah satu cara untuk mengatasi kerentanan tersebut adalah dengan menggunakan teknik kriptografi yang lebih kuat dalam proses autentikasi dan penyimpanan kata sandi.

TEKNIK KRIPTOGRAFI DALAM PERLINDUNGAN DATA

1. Enkripsi Simetris dan Asimetris

Enkripsi dapat melindungi data dari akses tidak sah akibat malware. Dengan enkripsi, data yang dicuri oleh malware tetap tidak bisa dibaca oleh penyerang tanpa kunci dekripsi yang benar. Enkripsi asimetris dapat mengamankan komunikasi antara pengguna dan server, memastikan bahwa data yang dikirim melalui email atau situs web palsu tidak bisa dibaca atau dimanipulasi oleh penyerang. Selain itu, enkripsi asimetris juga melindungi data selama transmisi dengan memastikan bahwa hanya penerima yang memiliki kunci pribadi yang dapat mendekripsi data, mencegah penyerang di tengah-tengah dari membaca atau mengubah data tersebut. Penggunaan enkripsi yang kuat dengan kunci panjang dan algoritma yang aman membuat serangan brute force sangat sulit dan memakan waktu, sehingga melindungi data sensitif dari upaya dekripsi oleh penyerang.

2. Hashing

Hashing adalah proses mengubah data menjadi nilai hash yang unik menggunakan fungsi hash tertentu. Nilai hash ini tidak dapat diubah kembali menjadi data asli. Hashing sering digunakan untuk memastikan integritas data, karena bahkan perubahan kecil pada data akan menghasilkan nilai hash yang berbeda. Hashing dapat memverifikasi integritas file dan program, memastikan bahwa malware tidak dapat menyusup atau mengubah data asli. Fungsi hash juga dapat digunakan untuk memverifikasi keaslian pesan dan situs web, membantu mengidentifikasi dan menghindari situs web phishing yang memalsukan domain yang sah. Dengan menggunakan hashing yang kuat dan menambahkan salt, kata sandi dapat dilindungi dari serangan brute force. Salt memastikan bahwa kata sandi yang sama menghasilkan hash yang berbeda, membuat penyerangan menjadi lebih sulit.

3. Digital Signature

Tanda tangan digital digunakan untuk memastikan keaslian dan integritas pesan atau dokumen. Ini dilakukan dengan membuat tanda tangan digital menggunakan kunci pribadi pengirim, yang kemudian dapat diverifikasi oleh penerima menggunakan kunci publik pengirim. Tanda tangan digital memastikan bahwa pesan atau dokumen berasal dari sumber yang sah dan belum diubah, membantu pengguna mengidentifikasi pesan phishing. Tanda tangan digital juga melindungi integritas pesan yang dikirim, memastikan bahwa pesan tidak diubah oleh penyerang di tengah-tengah. Tanda tangan digital dengan algoritma yang kuat membuat upaya brute force untuk memalsukan tanda tangan digital menjadi tidak praktis.

IMPLEMENTASI KRIPTOGRAFI DALAM SISTEM INFORMASI

1. Penilaian Risiko

Sebelum mengimplementasikan teknik-teknik kriptografi, sangat penting untuk melakukan penilaian risiko yang mendetail dan komprehensif. Tujuan dari penilaian ini adalah untuk mengidentifikasi aset-aset penting yang perlu dilindungi serta potensi ancaman yang mungkin dihadapi. Dengan memahami berbagai risiko yang ada, organisasi dapat merancang dan mengembangkan strategi perlindungan data yang lebih efektif dan tepat sasaran. Ini juga membantu dalam prioritas perlindungan terhadap aset yang paling kritis dan rentan.

2. Pemilihan Algoritma

Setelah menyelesaikan penilaian risiko, langkah berikutnya adalah memilih algoritma kriptografi yang paling sesuai dengan kebutuhan keamanan dan performa sistem. Beberapa faktor yang perlu dipertimbangkan dalam pemilihan algoritma ini meliputi tingkat keamanan yang dibutuhkan, kecepatan enkripsi dan dekripsi, serta ketersediaan dan dukungan untuk implementasi algoritma tersebut. Penting untuk memilih algoritma yang tidak hanya memenuhi persyaratan keamanan saat ini tetapi juga cukup kuat untuk menghadapi ancaman di masa depan.

3. Manajemen Kunci

Manajemen kunci adalah komponen krusial dalam implementasi kriptografi. Kunci enkripsi harus disimpan dan dikelola dengan aman, hanya boleh diakses oleh pihak-pihak yang berwenang. Untuk memastikan keamanan kunci, organisasi harus menerapkan praktik- praktik terbaik dalam manajemen kunci, seperti menggunakan kunci yang kuat, melakukan rotasi kunci secara berkala untuk mencegah kompromi, dan menyimpan kunci dalam bentuk terenkripsi. Selain itu, penting untuk memastikan bahwa proses pengelolaan kunci mudah diterapkan dan diaudit untuk meminimalkan risiko kebocoran atau penyalahgunaan kunci.

4. Pengujian dan Pemeliharaan

Setelah mengimplementasikan sistem kriptografi, perlu dilakukan pengujian menyeluruh untuk memastikan bahwa sistem tersebut benar-benar aman. Pengujian ini harus mencakup evaluasi fungsionalitas, kinerja, dan keamanan sistem secara keseluruhan. Pengujian fungsionalitas memastikan bahwa semua komponen sistem bekerja sesuai dengan yang diharapkan, sementara pengujian kinerja

memastikan bahwa sistem dapat beroperasi dengan efisien tanpa mengalami bottleneck. Selain itu, pengujian keamanan diperlukan untuk mengidentifikasi dan mengatasi potensi kerentanan. Setelah sistem diimplementasikan, pemeliharaan rutin dan pembaruan keamanan harus dilakukan secara berkala untuk menanggulangi ancaman-ancaman baru yang mungkin muncul. Ini termasuk memperbarui algoritma dan protokol enkripsi sesuai dengan perkembangan teknologi dan ancaman.

KESIMPULAN

Dalam era digital, sistem informasi menghadapi berbagai ancaman serius seperti malware, phishing, Man-in-the-Middle (MitM), dan brute force attack, yang dapat menyebabkan kerugian finansial dan kebocoran data. Malware merusak sistem atau mencuri data sensitif, sebagaimana ditemukan dalam penelitian Rahayu & Trianto (2021) tentang trojan yang mengunduh program berbahaya. Phishing menipu korban agar mengungkapkan informasi pribadi, seperti diungkap oleh Ginanjar et al., (2018) yang menemukan aktivitas phishing di layanan e-commerce. MitM memungkinkan penyerang menyusup dan memanipulasi komunikasi, sebagaimana ditunjukkan oleh Aman, (2023) dalam studi tentang serangan MitM di jaringan sekolah. Brute force attack mencoba semua kemungkinan kata sandi atau kunci enkripsi, seperti yang ditemukan oleh Wardhana & Seta (2021) dalam sistem pembelajaran online.

Teknik kriptografi seperti enkripsi simetris dan asimetris, hashing, dan tanda tangan digital sangat penting untuk melindungi data dari ancaman ini. Implementasi kriptografi memerlukan penilaian risiko yang detail, pemilihan algoritma yang tepat, manajemen kunci yang aman, serta pengujian dan pemeliharaan rutin. Dengan strategi perlindungan yang efektif dan pembaruan keamanan terus-menerus, individu dan organisasi dapat mengurangi risiko serangan dan melindungi data mereka dari berbagai ancaman.

REFERENCES

Agung Rachmat Raharja, Jayadi, Z. G. (2023). DESIGN AND IMPLEMENTATION OF ATTENDANCE USING RFID CARDS USING C# AT BANDUNG UNIVERSITY. *ABDITEK NUSANTARA*, *2*, 1–9. http://ojs.uninus.ac.id/index.php/Abditek%0ADESIGN

Aman, A. (2023). Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack Di Sekolah XYZ. *Digital Transformation Technology*, *3*(2), 824–831.

Faradilla. (2023). *Apa Itu Phising? Pengertian, Jenis, dan Cara Mengenalinya*. Hostinger Tutorial. https://www.hostinger.co.id/tutorial/phising-adalah

Ginanjar, A., Widiyasono, N., & Gunawan, R. (2018). Analisis Serangan Web Phishing pada Layanan E-commerce dengan MetodeNetwork Forensic Process. *JUTEI Edisi Volume.2 No.2 Oktober 2018*.

Manoppo, V. A., Lumenta, A. S. M., & Karouw, S. D. S. (2020). Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro Dan Komputer*, *9*(3), 181–188.

Maslan, A., & others. (2020). KEAMANAN JARINGAN DARI SERANGAN PAKET DATA SNIFFING DI PT RADEN SYAID KANTOR POS PIAYU KOTA BATAM. *Computer and Science Industrial Engineering (COMASIE)*, *3*(5), 107–117.

Munir, R. (2019). *Kriptografi* (Kedua). Penerbit Informatika.

Purbo, O. (2010). Keamanan Jaringan Komputer. *Handry Pratama. Jakarta*.

Puriwigati, A. N. (2020). Sistem Manajemen Basis Data. *Sistem Informasi & Manajemen Basis Data*, *April*.

Putri Aprilia. (2022). *Brute Force: Pengertian dan Cara Ampuh Mencegahnya!* Niagahoster. https://www.niagahoster.co.id/blog/brute-force-adalah/

Rahayu, Y. D. P., & Trianto, N. (2021). Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1. *Jurnal Info Kripto*.

Wardhana, A. W., & Seta, H. B. (2021). Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ. *Informatik: Jurnal Ilmu Komputer*, *17*(3), 226–237.

Whitman, M. E., & Mattord, H. J. (2019). *Management of information security*. Cengage Learning.

Wiz Experts Team. (2024). *Apa yang dimaksud dengan serangan man-in-the-middle?* Wiz.Io. https://translate.google.com/translate?u=https://www.wiz.io/academy/man-in-the-middle-attack&hl=id&sl=en&tl=id&client=srp&prev=search

Hariyanti, I., & Raharja, A. R. (2024). Perbandingan Algoritma Decision Tree dan Naive Bayes dalam Klasifikasi Data Pengaruh Media Sosial dan Jam Tidur Terhadap Prestasi Akademik Siswa. Technologia: Jurnal Ilmiah, 15(2), 332-340.

Erwis, F., Jixiong, C. ., Rahayu, N. ., Raharja, A. R. ., & Zebua, R. S. Y. . (2024). Use of Augmented Reality (AR) in Mobile Learning for Natural Science Lessons. Journal of Social Science Utilizing Technology, 2(1), 338–348. https://doi.org/10.55849/jssut.v2i1.784

Penerapan Algoritma Decision Tree dalam Klasifikasi Data "Framingham" Untuk Menunjukkan Risiko Seseorang Terkena Penyakit Jantung dalam 10 Tahun Mendatang. (2024). Technologia Journal, 1(1). https://doi.org/10.62872/cwgzp962

ANALISIS DIMENSI MUTU TERHADAP TINGKAT KEPUASAN PELAYANAN KESEHATAN PADA ERA PANDEMI COVID-19 (Di Puskesmas Cikembar Tahun 2020). (2024). Journal of Ostetricia, 1(1). https://nawalaeducation.com/index.php/JOO/article/view/59

Muchsam, Y., Sucipto, B., Rismawati, R., Rusdianti, I. S., & Raharja, A. R. (2023). Forming the Character of a Physically Healthy Young Generation Through Military Education. TGO Journal of Community Development, 1(2), 90-95.

Dola Ramalinda, A. R. R. (2024). Decision Support System for Selecting of. *International Journal of …*, *42*(1), 17–24. https://jicnusantara.com/index.php/jicn/article/view/535

Hariyanti, I., Al-husaini, M., & Raharja, A. R. (2024). *Perbandingan Algoritma Decision Tree dan Naive Bayes dalam Klasifikasi Data Pengaruh Media Sosial dan Jam Tidur Terhadap Prestasi Akademik Siswa*. *15*(2), 332–340. https://doi.org/dx.doi.org/10.31602/tji.v15i2.14381

Muchsam, Y., Sucipto, B., Rismawati, R., Rusdianti, I. S., & Raharja, A. R. (2023). Forming the Character of a Physically Healthy Young Generation Through Military Education. *TGO Journal of Community Development*, *1*(2), 90–95. https://doi.org/10.56070/jcd.2023.015

Raharja, Agung Rachmat, H. I. (2024). *Design of EMR (Electronic Medical Record) Applications Using RFID Cards to Record Patient Medical Record Data at The Sukajadi Bandung Health Center*. 66–72.

Raharja, A. R., Pramudianto, A., & Muchsam, Y. (2024). Penerapan Algoritma Decision Tree dalam Klasifikasi Data " Framingham " Untuk Menunjukkan Risiko Seseorang Terkena Penyakit Jantung dalam 10 Tahun Mendatang. *nawalaeducation*, *1*(1). https://doi.org/10.62872/cwgzp962

Raharja, A. R., Ramalinda, D., & Hariyanti, I. (n.d.). *ALGORITMA DAN PEMROGRAMAN MENGGUNAKAN PYTHON DENGAN APLIKASI GOOGLE COLLABS*. Mafy Media Literasi.

Ramalinda, D., Agung ,Rachmat Raharja, Sali Setiatin, M. H., & Angga Pramudianto, J. (2024). PENGANTAR TEKNOLOGI INFORMASI PADA REKAM MEDIS. In *Mafy Media Literasi*. Mafy Media Literasi.

Sutisna, T., Raharja, A. R., Hariyadi, E., Hafizh, V., & Putra, C. (2024). *Penggunaan Computer Vision untuk Menghitung Jumlah Kendaraan dengan Menggunakan Metode SSD (Single Shoot Detector)*. *4*, 6060–6067. https://doi.org/doi.org/10.31004/innovative.v4i2.10071