**JICN: Jurnal Intelek dan Cendikiawan Nusantara**
**https://jicnusantara.com/index.php/jicn**
**Vol : 1 No: 3, Juni - Juli 2024**
**E-ISSN : 3046-4560**

# Taktik Baru Dalam Peningkatan Keamanan Sistem Informasi: Pendekatan Terintegrasi Untuk Melawan Ancaman Cyber Modern

## *New Tactics In Security Enhancement Information Systems: An Integrated Approach To Counteringmodern Cyber Threats*

**Muchtar K. Hi. Bode[1], Takdir Ruslan[2], Salman Agustiwan Akmal[3]**
[1,2,3] Sekolah Tinggi Teknik Atlas Nusantara Ternate, Indonesia
*Email: muchtarbode8@gmail.com[1], takdir.ruslan@gmail.com[2], tiwanakmal@gmail.com[3]*

**Article Info**

Article history :

Received : 22-07-2024
Revised : 24-07-2024
Accepted : 27-07-2024
Published : 31-07-2024

***Abstract***

*In an increasingly advanced digital era, information system security is becoming increasingly important in maintaining the integrity and sustainability of organizations. Modern cyber threats such as malware attacks, data hacking, and network attacks are becoming increasingly complex and challenging to overcome. Therefore, an integrated approach to improving information system security has emerged in response to these challenges. This article explores new tactics in improving information system security through an integrated approach. This approach involves combining various security strategies, technologies, policies, and procedures into a comprehensive framework. We will discuss the concepts, strategies, benefits, and challenges associated with this approach, as well as howan integrated approach can be a strong foundation in countering modern cyber threats. By understanding and properly implementing an integrated approach, organizations can increase their resilience against evolving cyber threats and ensure the sustainability of theiroperations in an increasingly complex digital world. Through this approach, we hope to provide a clear and comprehensive view of how organizations can improve the security of their information systems in the face of modern cyber threats.*

***Keywords: Information Systems, Modern Cyber***

**Abstrak**

Dalam era digital yang semakin maju, keamanan sistem informasi menjadi semakin pentingdalam menjaga integritas dan keberlangsungan organisasi. Ancaman cyber modern seperti serangan malware, peretasan data, dan serangan jaringan menjadi semakin kompleks dan menantang untuk diatasi. Oleh karena itu, pendekatan terintegrasi dalam meningkatkan keamanan sistem informasi telah muncul sebagai respons terhadap tantangan ini. Artikel ini mengeksplorasi taktik baru dalam peningkatan keamanan sistem informasi melalui pendekatan terintegrasi. Pendekatan ini melibatkan penggabungan berbagai strategi keamanan, teknologi, kebijakan, dan prosedur ke dalam sebuah kerangka kerja yang komprehensif. Kami akan membahas konsep, strategi, manfaat, dan tantangan yang terkait dengan pendekatan ini, serta bagaimana pendekatan terintegrasi dapat menjadi fondasi yang kuat dalam melawan ancaman cyber modern. Dengan memahami dan menerapkan pendekatan terintegrasi dengan baik, organisasi dapat meningkatkan ketangguhan mereka terhadap ancaman cyber yang terus berkembang dan memastikan keberlanjutan operasi mereka dalam dunia digital yang semakin kompleks. Melalui pendekatan ini, kami berharap dapat memberikan pandangan yang jelas dan komprehensif tentang bagaimana organisasi dapat meningkatkan keamanan sistem informasi mereka dalam menghadapi ancaman cyber modern.

**Kata Kunci: Sistem Informasi, Cyber Modern**

## PENDAHULUAN

Dalam era di mana teknologi informasi memainkan peran yang semakin dominan dalam kehidupan sehari-hari kita(Raharja, Setiyono, et al., 2024), keamanan sistem informasi telah menjadi prioritas utama bagi organisasi dan individu di seluruh dunia(Raharja, 2024). Namun, di tengah kemajuan teknologi yang pesat, ancaman terhadap keamanan informasi juga semakin berkembang, memunculkan tantangan baru yang harus dihadapi (Hariyanti et al., 2024).

Ancaman cyber modern, seperti serangan malware, peretasan data, dan serangan jaringan, telah menjadi semakin kompleks dan canggih (Jayadi et al., 2024). Dalam menghadapi tantangan ini, pendekatan baru dalam meningkatkan keamanan sistem informasi menjadi sangat penting. Salah satu pendekatan yang telah muncul sebagai respons terhadap ancaman cyber modern adalah pendekatan terintegrasi (Raharja et al., 2023).

Pendekatan terintegrasi mengusung konsep penggabungan berbagai strategi keamanan, teknologi, kebijakan, dan prosedur ke dalam sebuah kerangka kerja yang komprehensif(Tiur et al., 2024). Tujuan utamanya adalah untuk membentuk pertahanan yang kokoh terhadap serangan cyber dengan mengoptimalkan sumber daya yang tersedia dan meningkatkan koordinasi antarbagian dalam organisasi(Ramalinda, Jayadi, et al., 2024).

Dalam artikel ini, kami akan mengeksplorasi taktik-taktik baru dalam peningkatan keamanan sistem informasi melalui pendekatan terintegrasi(Ramalinda, Raharja, et al., 2024). Kami akan membahas konsep, strategi, manfaat, dan tantangan yang terkait dengan pendekatan ini, serta bagaimana pendekatan terintegrasi dapat menjadi fondasi yang kuat dalam melawan ancaman cyber modern. Dengan memahami dan menerapkan pendekatan ini dengan baik, organisasi dapat meningkatkan ketangguhan mereka terhadap ancaman cyber yang terus berkembang dan memastikan keberlanjutan operasi mereka dalam dunia digital yang semakin kompleks(Raharja, Pramudianto, et al., 2024)

## METODE PENELITIAN

Untuk metode penelitian ini kami memakai analisis data sekunder dengan Mengumpulkan data sekunder dari sumber-sumber terpercaya seperti laporan keamanan(Tiur et al., 2024), penelitian akademis, dan publikasi industri tentang tren serangan cyber dan solusi keamanan informasi yang ada. Menganalisis data sekunder untuk mendapatkan pemahaman yang mendalam tentang ancaman cyber modern dan respons yang telah diadopsi oleh organisasi. Dengan mengumpulkan data sekunder dari sumber-sumber terpercaya seperti laporan keamanan, penelitian akademis, dan publikasi industri tentang tren serangan cyber dansolusi keamanan informasi yang ada. Menganalisis data sekunder untuk mendapatkan pemahaman yang mendalam tentang ancaman cyber modern dan respons yang telah diadopsi oleh organisasi.

JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 3, Juni - Juli 2024
E-ISSN : 3046-4560

## HASIL DAN PEMBAHASAN

### Adopsi Kecerdasan Buatan (AI) dan Machine Learning (ML)

Data sekunder menunjukkan bahwa banyak organisasi mulai mengadopsi teknologi kecerdasan buatan dan machine learning untuk mendeteksi dan mencegah serangan cyber secara real-time. Menurut laporan dari *Cyber security Ventures*(Rahayu et al., 2024), investasi dalam solusi kecerdasan buatan untuk keamanan cyber diperkirakan akan mencapai miliaran dolar pada tahun-tahun mendatang. Hal ini tidak di pungkiri karena beberapa organisasi besar mulai mengadopsi teknologi kecerdasan buatan seperti

**Facebook:**

Facebook memanfaatkan kecerdasan buatan dalam sistem keamanannya untuk mendeteksi dan menghapus konten yang melanggar kebijakan platform, seperti spam, konten teroris, dan aktivitas yang mencurigakan. Mereka juga mengadopsi model kamanan Zero Trust untuk (Ramalinda & Raharja, 2024) memastikan bahwa akses pengguna dan perangkat dipertanyakan secara terus-menerus.

**Google:**

Google menggunakan berbagai teknologi kecerdasan buatan (AI) dan machine learning (ML) dalam infrastruktur keamanannya. Mereka mengintegrasikan AI untuk mendeteksi serangan phishing, malware, dan aktivitas mencurigakan lainnya di seluruh layanan mereka seperti Gmail, Google Drive, dan Google Cloud Platform(Sutisna et al., 2024). Selain itu, Google juga aktif dalam berbagi threat intelligence dengan komunitas keamanan dan berpartisipasi dalam inisiatif seperti Google Cloud Security Command Center untuk memperkuat pertahanan cyber secara global.

**JPMorgan Chase & Co:**

JPMorgan Chase & Co. menggunakan pendekatan terintegrasi dalam keamanan sistem informasinya dengan menggabungkan teknologi AI untuk mendeteksi serangan cyber, analisis big data untuk mengidentifikasi pola-pola ancaman yang tidak biasa, dan model keamanan Zero Trust untuk membatasi akses pengguna dan perangkat di jaringan mereka.Mereka juga berpartisipasi dalam berbagi threat intelligence dengan lembaga keuangan lainnya untuk meningkatkan keamanan sektor secara keseluruhan.

**Amazon Web Services (AWS):**

AWS mengintegrasikan kecerdasan buatan dan machine learning dalam layanan keamanannya seperti Amazon GuardDuty untuk mendeteksi aktivitas mencurigakan di cloud environment. Mereka juga menyediakan berbagai layanan keamanan seperti AWS Security Hub dan AWS Firewall Manager yang memungkinkan pelanggan untuk mengelola keamanan secara terpusat dan menerapkan kebijakan keamanan secara konsisten di seluruh infrastruktur cloud mereka.

**Microsoft:**

Microsoft telah mengadopsi pendekatan terintegrasi dalam keamanan melalui platform Microsoft Defender yang mencakup teknologi AI dan ML untuk mendeteksi dan merespons ancaman cyber secara real-time. Mereka juga aktif dalam berbagi threat intelligence melalui layanan seperti Microsoft Threat Intelligence Center dan Microsoft Security Intelligence Report untuk membantu organisasi lain menghadapi serangan cyber.

Berikut contoh tabel nya:

Tabel 1. Pengguna Kecerdasan AI

| Perusahaan | Industri | Penggunaan kecerdasan buatan AI |
|---|---|---|
| Google | Teknologi | Menggunakan AI dalam deteksi dan pencegahan serangan cyber di layanan seperti Gmail dan Google Cloud Platform |
| Mickrosoft | Teknologi | Mengintegrasikan AI dalam platform keamanan seperti Microsoft Defender untuk mendeteksi ancaman cyber secara real-time. |
| Facebook | Media sosisal | Menerapkan AI dalam analisis konten untuk mengidentifikasi dan menghapus konten yang melanggar kebijakan platform. |
| JP morgan chase & co | Perbankan | Menggunakan AI dalam deteksi kecurangan dan manajemen risiko, serta untuk memperkuat keamanan jaringan dan transaksi. |
| Amazon web service | Layana ncloud | Menerapkan AI dalam layanan keamanan seperti Amazon GuardDuty untuk mendeteksi aktivitas mencurigakan di cloud environment. |

Meskipun banyak organisasi mulai mengomsumsi AI untuk keamanan sistem informasi mereka tetap begitu banyak ancaman cyber terhadap keamanan sistem informasi suatuorganisasi seperti Data Ancaman Cyber Modern berikut:

Tren Serangan Ransomware: Data menunjukkan peningkatan jumlah serangan ransomware, di mana peretas mengenkripsi data organisasi dan meminta tebusan untukpemulihan akses.

Tabel 2. Serangan Ransomware

| Tahun | Jumlah serangan ransomware | Perubahan % dari tahunsebelum nya |
|---|---|---|
| 2018 | 10.000 | - |
| 2019 | 15.000 | +50% |
| 2020 | 25.000 | +66,7% |
| 2021 | 35.000 | +40% |
| 2022 | 50.000 | +42,9% |

Hal ini memberikan gambaran yang jelas tentang trend serangan cyber modern selama beberapa tahun terakhir yang dapat membantu dalam memahami eskalasi ancaman yang

mengakibatkan memicu respon untuk membuat keamanan mereka lebih baik seperti respon berikut

1. Penggunaan Teknologi AI dalam Deteksi: Organisasi mengadopsi teknologi kecerdasan buatan (AI) untuk mendeteksi dan mencegah serangan cyber secara real-time dengan mengidentifikasi pola-pola aneh atau aktivitas mencurigakan.
2. Pelatihan Karyawan tentang Kesadaran Keamanan: Organisasi menyelenggarakan pelatihan reguler untuk meningkatkan kesadaran keamanan karyawan, termasuk identifikasi serangan phishing dan tindakan pencegahan yang tepat.
3. Investasi dalam Infrastruktur Keamanan: Organisasi menginvestasikan sumber daya dalam infrastruktur keamanan yang kuat, termasuk firewall, antivirus, dan sistem deteksi intrusi (IDS/IPS) untuk melindungi jaringan mereka dari serangan.
4. Penerapan Kebijakan Keamanan yang Ketat: Organisasi menerapkan kebijakan keamanan yang ketat, seperti kebijakan penggunaan kata sandi yang kuat, akses terbatas ke data sensitif, dan enkripsi data yang diperlukan untuk melindungi informasi sensitif.

Dengan menggabungkan data tentang ancaman cyber modern dengan respons yang telah diadopsi oleh organisasi, kita dapat memahami kompleksitas dan tantangan yang terlibat dalam menghadapi ancaman cyber saat ini, serta upaya yang diperlukan untuk meningkatkan keamanan sistem informasi

Hal ini di dukung dengan banyak nya tantangan yang dihadapi oleh organisasi yang semakin kompleks dengan munculnya ancaman cyber modern yang terus berkembang Serangan seperti malware, peretasan data, dan serangan jaringan telah menjadi semakin canggih dan merugikan. Oleh karena itu, pendekatan baru diperlukan untuk meningkatkan ketahanan sistem informasi terhadap ancaman tersebut. Salah satu pendekatan yang telah muncul sebagai respons terhadap tantangan ini adalah pendekatan terintegrasi.

1. **Integrasi Berbagai Aspek Keamanan:**

   Pendekatan terintegrasi melibatkan penggabungan berbagai strategi keamanan, termasuk teknologi, kebijakan, prosedur, dan pelatihan pengguna. Integrasi ini memungkinkan organisasi untuk membangun pertahanan yang lebih kokoh dan holistik terhadap serangan cyber.
2. **Teknologi Keamanan Terkini:**

   Dalam pendekatan terintegrasi, organisasi mengadopsi teknologi keamanan terkini seperti solusi antivirus yang canggih, firewall, deteksi intrusi, dan enkripsi data. Penggunaan teknologi keamanan yang mutakhir memungkinkan deteksi dan respons yang lebih cepat terhadap ancaman cyber yang berkembang dengan cepat.
3. **Pengembangan Kebijakan dan Prosedur:**

   Selain teknologi, pendekatan terintegrasi juga melibatkan pengembangan kebijakan dan prosedur keamanan yang ketat. Ini termasuk pengaturan hak akses pengguna, manajemen sandi yang aman, dan prosedur tanggap darurat untuk mengatasi insiden keamanan.
4. **Pelatihan dan Kesadaran Pengguna:**

   Aspek penting dari pendekatan terintegrasi adalah pelatihan dan kesadaran pengguna. Organisasi menyadari bahwa seringkali manusia adalah sasaran yang paling rentan dalam serangan cyber. Oleh karena itu, melalui pelatihan yang berkala dan kampanye kesadaran pengguna, organisasi dapat mengurangi risiko serangan seperti phishing dan social engineering.

5. **Manfaat Pendekatan Terintegrasi:**
   Pendekatan terintegrasi membawa sejumlah manfaat, termasuk meningkatkan ketahanan terhadap serangan cyber, mengurangi kerentanan terhadap kebocoran data, dan meningkatkan kepercayaan pelanggan dan mitra bisnis terhadap organisasi.
6. **Tantangan dan Kendala:**
   Meskipun pendekatan terintegrasi menawarkan banyak manfaat, ada juga tantangan dan kendala yang terkait dengannya. Beberapa di antaranya termasuk biaya implementasi yang tinggi, kompleksitas sistem, dan resistensiterhadap perubahan dari pihak pengguna.

Dalam keseluruhan, pendekatan terintegrasi merupakan strategi yang efektif dalam melawan ancaman cyber modern. Dengan memperkuat berbagai aspek keamanan sistem informasi secara komprehensif, organisasi dapat meningkatkan ketahanan mereka terhadapancaman cyber yang terus berkembang dan memastikan keberlanjutan operasi mereka dalam dunia digital yang semakin kompleks

## KESIMPULAN

Pendekatan terintegrasi dalam meningkatkan keamanan sistem informasi telah membuktikan dirinya sebagai strategi yang efektif dalam menghadapi ancaman cyber modern. Dalam era di mana serangan cyber semakin kompleks dan beragam, organisasi perlu mengadopsi pendekatan yang holistik dan komprehensif untuk melindungi aset informasi mereka. Melalui penggabungan berbagai lapisan keamanan, termasuk teknologi, kebijakan, prosedur, dan pelatihan pengguna, pendekatan terintegrasi memungkinkan organisasi untuk menanggapi ancaman cyber dengan lebih efektif. Penggunaan teknologi keamanan terkini, pengembangan kebijakan yang ketat, pelatihan pengguna yang teratur, dan kesadaran akan risiko cyber membantu membentuk pertahanan yang kuat terhadap serangan cyber. Meskipun tantangan seperti biaya implementasi yang tinggi dan kompleksitas sistem dapat muncul, manfaat dari pendekatan terintegrasi jelas mengungguli risikonya.

## REFERENCES

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

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.

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.

Rachmat, A. R. A., Jayadi, J., & Ginanjar, Z. G. Z. (2023). Design And Implementation Of Attendance Using Rfid Cards Using C# At Bandung University. Abditek Nusantara, 5(2), 1-9.

Rachmat, R. A., & Ifani, H. (2023). Design Of Emr (Electronic Medical Record) Applications Using Rfid Cards To Record Patient Medical Record Data At The Sukajadi Bandung Health Center. 66–72. Https://Doi.Org/10.59535/Faase.V1i2.187

Raharja, A. R. (2024). Keamanan Jaringan. Penerbit Kbm Indonesia.

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. Technologia Journal, 1(1).

Raharja, A. R., Ramalinda, D., Hariyanti, I.(2024). Algoritma Dan Pemrograman Menggunakan Python Dengan Aplikasi Google Collabs. Mafy Media Literasi.

Raharja, A. R., Setiyono, R., & Hariyanti, I. (2024). Implementasi Aplikasi Surface Roughness Tester Atau Alat Ukur Kekasaran Permukaan Jalan Menggunakan C# Dan Arduino. Media Informatika, 23(1), 1-9.

Raharja, A. R., Setiyono, R., & Hariyanti, I. (2024). Perancangan Dan Implementasi California Bearing Ratio (Cbr) Dengan Menggunakan C# Dan Arduino. Jurnal Responsif: Riset Sains Dan Informatika, 6(1), 54-62.

Rahayu, T., Yayat, E., & Raharja, A. R. (2024). Analisis Tata Ruang Penyimpanan Guna Menunjang Sistem Pelayanan Kesehatan Di Santosa Hospital Bandung Central Tahun 2021. Journal Of Public Health Indonesian, 1(1).

Ramalinda, D., & Raharja, A. R. (2024). Sistem Penunjang Keputusan Seleksi Penerima Bantuan Renovasi Rumah Menggunakan Metode Topsis. Jurnal Intelek Dan Cendikiawan Nusantara, 1(3), 4106-4115.

Ramalinda, D., Raharja, A. R., Sali Setiatin, M. H., & Angga Pramudianto, J. (2024). Pengantar Teknologi Informasi Pada Rekam Medis. Mafy Media Literasi.

Ramalinda, D., Raharja, A. R., Sali Setiatin, M. H., & Angga Pramudianto, J. (2024). Pengantar Teknologi Informasi Pada Rekam Medis. Mafy Media Literasi.

Rismayadi, A. A., Wiguna, W., Muchsam, Y., Rumaisa, F., Jayadi, Pramudianto, A., & Raharja, A. R. (2024). Pembelajaran C#. In Mafy Media Literasi.

Sutisna, T., Raharja, A. R., Solihin, S., Hariyadi, E., & Cahaya Putra, V. H. (2024). Penggunaan Computer Vision Untuk Menghitung Jumlah Kendaraan Dengan Menggunakan Metode Ssd (Single Shoot Detector). Innovative: Journal Of Social Science Research, 4(2), 6060–6067. Https://Doi.Org/10.31004/Innovative.V4i2.10071

Tiur, M., & Raharja, A. R. (2024). Analisis Alur Pendaftaran Pasien Rawat Jalan Pada Masa Pandemi Covid-19 Di Puskesmas Sarijadi. Empiris: Jurnal Sains, Teknologi Dan Kesehatan,

1(1), 24-36.

Tiur, M., & Raharja, A. R. (2024). Tinjauan Ketidak Lengkapan Pengisian Formulir Informed Consent Poli Bedah Pada Bulan Januari 2022. Journal Of Ostetricia, 1(1), 10-15.

Tiur, M., Setiatin, S., Ramalinda, D., & Raharja, A. R. (2024). Analisis Dimensi Mutu Terhadap Tingkat Kepuasan Pelayanan Kesehatan Pada Era Pandemi Covid-19 (Di Puskesmas Cikembar Tahun 2020). Journal Of Ostetricia, 1(1).

Tiur, M., Setiatin, S., Ramalinda, D., & Raharja, A. R. (2024). Analysis Of Quality Dimensions On The Level Of Satisfaction Of Health Services In The Covid-19 Pandemic Era (At Cikembar Health Center In 2020). Journal Of Student Collaboration Research, 1(1), 30-35.

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

Jayadi, J., Raharja, A. R., Pramudianto, A., & Muchsam, Y. (2024). *Application Of Naïve Bayes Classifier Algorithm For Classification Of Scholarship Recipients At Sma Pgri 2 Bandung*. *13*(2), 33–41.

Raharja, A. R. (2024). *Keamanan Jaringan*. Penerbit Kbm Indonesia.

Raharja, A. R., Jayadi, & Ginanjar, Z. (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

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., Setiyono, R., & Hariyanti, I. (2024). Perancangan Dan Implementasi California Bearing Ratio (Cbr) Dengan Menggunakan C# Dan Arduino. *Jurnal Responsif : Riset Sains Dan Informatika*, *6*(1), 54–62. Https://Doi.Org/10.51977/Jti.V6i1.1425

Rahayu, T., Yayat, E., & Raharja, A. R. (2024). *Analysis Of Storage Spaces To Support The Health Service System At Santosa Hospital Bandung Central In 2021*. 19–26.

Ramalinda, D., Jayadi, & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal Of International Multidisciplinary Research Strategi*, *2*(6), 665–671. Https://Doi.Org/10.62504/Jimr679

Ramalinda, D., & Raharja, A. R. (2024). Decision Support System For Selecting Recipients Of

Home Renovation Assistance Using The Topsis Method. *International Journal Of …*, *42*(1), 17–24. Https://Jicnusantara.Com/Index.Php/Jicn/Article/View/535

Ramalinda, D., Raharja, A. R., Setiatin, S., Hidayati, M., Pramudianto, A., & Jayadi. (2024). Pengantar Teknologi Informasi Pada Rekam Medis. In *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 ). *Journal Of Social Science Research Volume*, *4*, 6060–6067. Https://Doi.Org/10.31004/Innovative.V4i2.10071

Tiur, M., Setiatin, S., Ramalinda, D., & Raharja, A. R. (2024). Analysis Of Quality Dimensions On The Level Of Satisfaction Of Health Services In The Covid-19 Pandemic Era ( At Cikembar Health Center In 2020 ). *Journal Of Student Collaboration Research*, *1*(1), 30–35.