Ancaman, Mitigasi dan Metode Kriptografi dalam Keamanan Data Digital

Restu Zuhur[*1] **Ramadhan Renaldy** [2]
[1,2] Informatika, Universitas PGRI Semarang, Kota Semarang

*Email: [1]zuhurrestu@gmail.com, [2]ramadhanrenaldy@upgris.ac.id

Abstract

Threats to digital data security include cyber attacks such as malware, phishing, Ddos, and zero day exploits that can steal or damage sensitive data. To overcome this threat, effective mitigation such as the use of antivirus, firewalls, data encryption and multi-factor authentication, involves the use of strong cryptographic methods, such as symmetric and asymmetric encryption, and hashing. This method ensures that data can only be accessed by authorized parties and is protected from unauthorized modification or disclosure. In addition, implementing security protocols such as SSL/TLS and strict key management policies are also crucial in maintaining the integrity and confidentiality of digital data.

Keyword : Digital data security, Data encryption, HTTPS security protocols, Multi-factor authentication, Phishing attacks, Systematic Literature Review

Abstrak

Ancaman terhadap keamanan data digital mencakup serangan siber seperti malware, phishing,Ddos, serta zero day exploit yang dapat mencuri atau merusak data sensitif. Untuk mengatasi ancaman ini, mitigasi yang efektif seperti penggunaan antivirus, firewall,enkripsi data serta autentikasi multi-faktor, melibatkan penggunaan metode kriptografi yang kuat, seperti enkripsi simetris dan asimetris, serta hashing. Metode ini memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang dan terlindungi dari modifikasi atau pengungkapan yang tidak sah. Selain itu, penerapan protokol keamanan seperti SSL/TLS dan kebijakan manajemen kunci yang ketat juga krusial dalam menjaga integritas dan kerahasiaan data digital.

Kata kunci : Keamanan data digital, Enkripsi data, Protokol keamanan HTTPS, Otentikasi multi-faktor, Serangan phishing, Systematic Literature Review

1. Pendahuluan

Dalam era digital saat ini, keamanan data telah menjadi salah satu perhatian utama bagi individu, perusahaan, dan pemerintah. Dengan meningkatnya penggunaan teknologi informasi dan komunikasi, volume data yang dipertukarkan dan disimpan secara elektronik juga meningkat secara signifikan[1]. Data ini mencakup informasi pribadi, keuangan, kesehatan, dan rahasia bisnis yang sangat penting bagi keberlangsungan operasional dan privasi[2][3].Namun, seiring dengan perkembangan teknologi, ancaman terhadap keamanan data juga semakin kompleks dan canggih[4].

Ancaman terhadap data digital dapat berasal dari berbagai sumber, termasuk peretas, malware, dan tindakan tidak etis dari dalam organisasi itu sendiri. Beberapa ancaman utama meliputi serangan malware yang dapat merusak atau mencuri data,[5] phishing yang mencoba untuk memperoleh informasi sensitif dengan menyamar sebagai entitas tepercaya,[6] dan serangan DDoS[7] yang dapat mengganggu layanan internet dengan membanjiri jaringan

dengan lalu lintas yang berlebihan. Selain itu, serangan seperti man-in-the-middle (MitM), SQL injection, dan serangan kata sandi juga menambah kompleksitas lanskap ancaman siber[8][9].

Untuk menghadapi ancaman-ancaman ini, diperlukan pendekatan yang komprehensif dalam keamanan data digital. Langkah-langkah mitigasi yang efektif meliputi penggunaan perangkat lunak antivirus dan antimalware,[10]firewall, dan protokol keamanan seperti HTTPS dan SSL/TLS.[11]Edukasi dan pelatihan keamanan siber juga penting untuk meningkatkan kesadaran dan keterampilan dalam mengenali serta menghindari ancaman siber[12].Selain itu, enkripsi data dan autentikasi multi-faktor (MFA)[13] adalah metode penting dalam memastikan bahwa data tetap aman selama transit dan penyimpanan[14].

Kriptografi berperan penting dalam melindungi data digital dengan menyediakan berbagai metode untuk enkripsi dan dekripsi informasi,fungsi hash untuk memastikan integritas data, serta tanda tangan digital untuk menjamin keaslian dan integritas dokumen[15].Metode enkripsi simetris seperti AES dan enkripsi asimetris seperti RSA[16] adalah dua contoh teknik yang banyak digunakan untuk melindungi data dari akses yang tidak sah. Fungsi hash seperti SHA-256 memastikan bahwa data tidak diubah selama proses pengiriman atau penyimpanan[17][18].

Pendahuluan ini menjelaskan latar belakang dan pentingnya keamanan data digital, serta menjabarkan ancaman-ancaman utama, strategi mitigasi, dan peran kriptografi dalam melindungi data. Tujuan dari penelitian ini adalah untuk mengetahui apa saja ancaman-ancaman yang sering digunakan pelaku dalam melakukan serangan, dan bagaimana langkah-langkah yang bisa kita gunakan untuk mencegah serangan tersebut, serta metode kriptografi yang sering digunakan dalam kemanan data digital.

2. Metode

Systematic Literature Review (SLR) ini bertujuan untuk mengidentifikasi, mengevaluasi, dan mensintesis literatur yang relevan mengenai Research Question(RQ). Ancaman terhadap keamanan data digital (RQ1), strategi mitigasi yang digunakan untuk melawan serangan tersebut (RQ2), serta metode-metode kriptografi yang diterapkan dalam melindungi data dari serangan siber (RQ3). Sumber informasi yang digunakan mencakup database akademik seperti IEEE Xplore, E-Jurnal, dan Google Scholar. Dengan menggunakan metodologi SLR, penelitian ini akan menyusun literatur yang ada untuk menyediakan pemahaman yang komprehensif tentang jenis-jenis ancaman yang ada, upaya mitigasi yang telah dilakukan, serta peran kriptografi dalam konteks perlindungan terhadap serangan terhadap keamanan data digital. Hasil dari SLR ini diharapkan dapat memberikan wawasan yang lebih dalam kepada para praktisi dan peneliti dalam bidang keamanan informasi untuk pengembangan strategi mitigasi yang lebih efektif.

Tabel 1. Tujuan dibentuk Research Question

ID	Research Question	Tujuan
RQ1	Apa saja jenis-jenis ancaman Kemanan data digital?	Mengetahui jenis-jenis ancaman yang sering digunakan pelaku
RQ2	Apa yang harus dilakukan untuk mengurangi resiko penyerangan?	Melakukan berbagai langkah pencegahan,perlindungan data sebagai antisipasi kemanan data
RQ3	Metode kriptgrofi yang digunakan dalam kemanan data digital?	Mengetahui metode apa saja yang digunakan dalam keamanan data digital

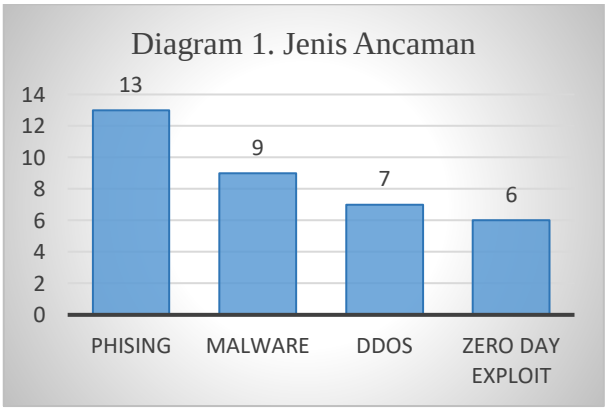
Dengan mempertimbangkan sumber informasi dari database akademik terpercaya seperti IEEE Xplore, E-Jurnal, dan Google Scholar, SLR ini diharapkan dapat menyajikan sintesis yang komprehensif tentang tantangan keamanan data digital, upaya mitigasi yang efektif, serta peran penting kriptografi dalam melindungi informasi sensitif dari serangan siber.

3. Hasil dan Pembahasan

Dengan menggunakan Systematic Literature Review (SLR), penulis dapat memaparkan hasil yang sudah dikaji dan disusun berdasarkan tiga Research Question (RQ) yang telah ditentukan.

3.1. Penyajian Hasil

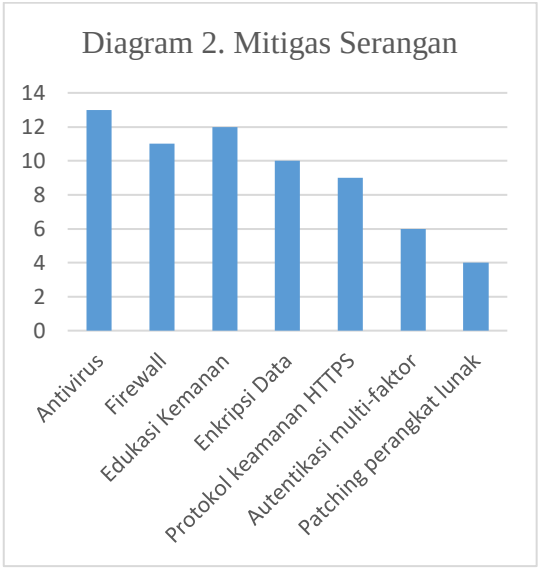
Dalam bagian ini, hasil disajikan dengan representatif dari penelitian berdasarkan tiga Research Question (RQ) yang telah ditentukan.



Gambar 1. Diagram JenisAncaman

Dari 31 jurnal yang saya review,ada beberapa ancaman yang sering digunakan yaitu seperti Phising, ada 13 jurnal yang membahasa tentang ancaman tersebut,kemudian dilanjut Malware dengan 9 jurnal yang membahasnya,DDos ada 7 jurnal pembahasan dan juga Zero day exploit dengan 6 jurnal pembahasan.

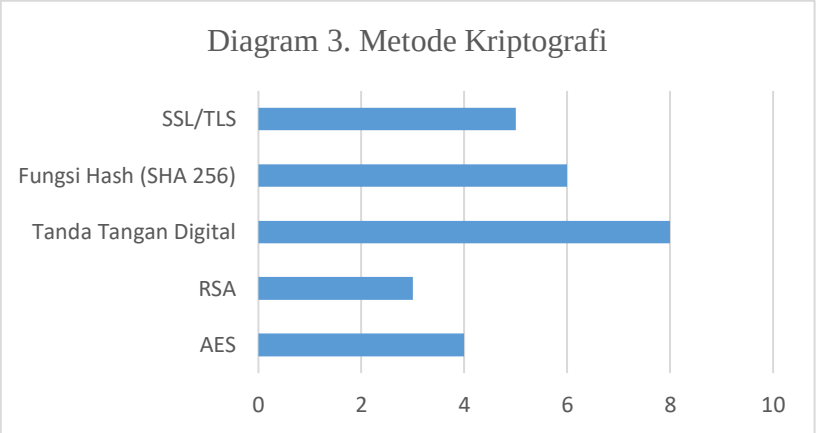
Diagram di atas memberikan contoh beberapa jenis ancaman utama terhadap keamanan data digital. Untuk SLR, diagram ini akan digunakan untuk mengorganisir dan menyajikan informasi yang relevan dari literatur yang dianalisis, memberikan pemahaman yang lebih baik tentang ragam ancaman yang ada dalam konteks keamanan data digital.



Gambar 2. Diagram Mitigas Serangan

Bisa dilihat bahwa penggunaan antivirus merupakan yang paling banyak digunakan untuk mengamankan data dengan 13 jurnal yang membahasnya,dilanjut dengan edukasi yaitu 12 jurnal, Firewall 11 jurnal, Enkripsi data 10 jurnal, protokol kemanan https 9,autentikasi multi-faktor 6 serta patching perangkat lunak 4 jurnal.

Diagram ini mencantumkan beberapa strategi mitigasi yang penting untuk melindungi keamanan data digital dari berbagai jenis ancaman, termasuk malware, serangan phishing, dan lainnya.



Gambar 3. Diagram Metode Kriptografi

Dari jurnal yang saya review,didapatkan paling banyak metode yang sering digunakan adalah Tanda tangan digital yaitu sebanyak 8 jurnal,dilanjut SHA 256 dengan 6 jurnal,SSL/TLS 4 jurnal, AES 4 jurnal serta RSA 3 jurnal.

Diagram diatas menyajikan beberapa metode kriptografi yang umum digunakan dalam melindungi data digital dari serangan siber.Digunakan dalam praktik untuk memastikan keamanan informasi. Diagram ini dapat digunakan dalam SLR untuk mengorganisir informasi tentang teknologi kriptografi yang relevan dalam konteks perlindungan data dari serangan cyber.

3.2. Pembahasan

RQ1 : Jenis Ancaman

Ancaman keamanan siber meliputi phishing, malware, DDoS, dan zero-day exploit[19]. Phishing adalah upaya penipuan untuk mendapatkan informasi sensitif dengan menyamar sebagai entitas tepercaya, sering melalui email atau situs web palsu[20].Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mencuri data, dengan jenis-jenis seperti virus, worm, trojan, ransomware, dan spyware[21].DDoS adalah serangan yang membanjiri layanan online dengan lalu lintas berlebihan dari berbagai sumber, menyebabkan layanan tidak dapat diakses[22].Zero-day exploit memanfaatkan kerentanan perangkat lunak yang belum diketahui atau diperbaiki oleh pengembang, sehingga sangat berbahaya. Pencegahan ancaman ini memerlukan kesadaran pengguna, teknologi keamanan yang canggih, serta kebijakan dan prosedur yang kuat[23].

RQ2 : Mitigasi Serangan

Mitigasi serangan keamanan siber melibatkan penggunaan berbagai langkah pencegahan dan perlindungan. Antivirus digunakan untuk mendeteksi, mencegah, dan menghapus malware dengan memindai file dan program untuk mencari tanda-tanda berbahaya[24].Firewall berfungsi memantau dan mengendalikan lalu lintas jaringan

berdasarkan aturan keamanan yang telah ditetapkan, mencegah akses tidak sah[25].Edukasi keamanan siber bertujuan meningkatkan kesadaran dan pengetahuan pengguna tentang praktik keamanan yang baik, seperti mengenali phishing dan menggunakan kata sandi yang kuat. Enkripsi data mengubah informasi menjadi format yang tidak dapat dibaca tanpa kunci dekripsi, melindungi informasi sensitif dari akses tidak sah[26].

Protokol keamanan HTTPS menggunakan sertifikat SSL/TLS untuk mengenkripsi data yang dikirim antara pengguna dan situs web, memastikan integritas dan kerahasiaan data. Autentikasi multi faktor (MFA)[27], memerlukan dua atau lebih bentuk identifikasi sebelum memberikan akses, seperti kata sandi dan kode yang dikirim ke ponsel[28].Patching perangkat lunak adalah proses memperbarui perangkat lunak untuk memperbaiki kerentanan keamanan dan bug, yang harus dilakukan secara teratur untuk melindungi dari ancaman yang telah diketahui. Dengan menggabungkan langkah-langkah ini, organisasi dan individu dapat mengurangi risiko serangan keamanan siber dan melindungi data serta sistem mereka dari berbagai ancaman.

RQ3 : Metode Kriptografi yang Digunakan

Metode kriptografi seperti AES, RSA, SHA-256, SSL/TLS, dan tanda tangan digital memainkan peran penting dalam keamanan data dan komunikasi[29].AES adalah algoritma enkripsi simetris yang cepat dan efisien, menggunakan kunci rahasia untuk enkripsi dan dekripsi. RSA adalah algoritma enkripsi asimetris yang menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi, memastikan hanya penerima yang memiliki kunci privat yang dapat mendekripsi pesan[30].SHA-256 adalah algoritma hashing yang menghasilkan nilai hash 256-bit unik untuk setiap input data, sangat aman dan banyak digunakan dalam tanda tangan digital dan blockchain[31].SSL/TLS adalah protokol yang menyediakan komunikasi terenkripsi melalui internet, melindungi data dari serangan man-in-the-middle dengan kombinasi enkripsi simetris dan asimetris. Tanda tangan digital memastikan keaslian dan integritas dokumen dengan mengenkripsi hash dokumen menggunakan kunci privat pengirim, yang kemudian dapat diverifikasi oleh penerima menggunakan kunci publik pengirim. Metode-metode ini melindungi data dan komunikasi dari akses tidak sah, manipulasi, dan penyadapan, memastikan privasi dan keamanan informasi.

4. Kesimpulan

Hasil dari SLR ini menunjukkan bahwa ancaman terhadap keamanan data digital sangat beragam dan semakin kompleks. Strategi mitigasi yang teridentifikasi efektif dalam mengurangi risiko dari berbagai serangan, dengan kriptografi memainkan peran penting dalam melindungi data selama transit dan penyimpanan.

Berdasarkan analisis dalam Systematic Literature Review (SLR) mengenai keamanan data digital, dapat disimpulkan bahwa ancaman terhadap informasi pribadi dan bisnis semakin meningkat dengan kemajuan teknologi. Untuk mengatasi risiko ini, langkah-langkah mitigasi seperti penggunaan antivirus, firewall, edukasi keamanan siber, dan implementasi enkripsi data sangat penting. Kriptografi, melalui metode seperti AES, RSA, SHA-256, SSL/TLS, dan tanda tangan digital, menunjukkan peran krusial dalam menjaga kerahasiaan, integritas, dan otentikasi data. Dengan memahami dan menerapkan kriptografi secara efektif, organisasi dapat meningkatkan tingkat perlindungan terhadap data digital mereka, mengurangi dampak dari serangan siber, dan memastikan keberlanjutan operasional serta privasi informasi yang sensitif.

5. Referensi

[1] V. Padamvathi, B. V. Vardhan, and A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," *Proc. - 6th Int. Adv. Comput. Conf. IACC 2016*, pp. 556–562, 2016, doi: 10.1109/IACC.2016.109.

[2] O. S. Althobaiti and M. Dohler, "Quantum-resistant cryptography for the internet of things based on location-based lattices," *IEEE Access*, vol. 9, pp. 133185–133203, 2021, doi: 10.1109/ACCESS.2021.3115087.

[3] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," *IEEE Int. Conf. IoT its Appl. ICIOT 2017*, 2017, doi: 10.1109/ICIOTA.2017.8073638.

[4] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.

[5] A. Dadheech, "Preventing Information Leakage from Encoded Data in Lattice Based Cryptography," *2018 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2018*, pp. 1952–1955, 2018, doi: 10.1109/ICACCI.2018.8554942.

[6] P. Kamble and A. Gawade, "Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks," *Proc. 4th Int. Conf. Contemp. Comput. Informatics, IC3I 2019*, pp. 69–73, 2019, doi: 10.1109/IC3I46837.2019.9055531.

[7] M. Moizuddin, J. Winston, and M. Qayyum, "A comprehensive survey: Quantum cryptography," *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 98–102, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905271.

[8] H. R. Pawar and D. G. Harkut, "Classical and Quantum Cryptography for Image Encryption Decryption," *Proc. 2018 3rd IEEE Int. Conf. Res. Intell. Comput. Eng. RICE 2018*, pp. 1–4, 2018, doi: 10.1109/RICE.2018.8509035.

[9] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 02, no. 01, pp. 31–42, 2020, doi: 10.54367/kakifikom.v2i1.666.

[10] P. Chyan, P. Studi, T. Informatika, F. T. Informasi, U. Atma, and J. Makassar, "Tanda Tangan Digital Dalam Mendukung Keamanan," pp. 39–46, 2018.

[11] J. Partala, T. H. Nguyen, and S. Pirttikangas, "Non-Interactive Zero-Knowledge for Blockchain: A Survey," *IEEE Access*, vol. 8, pp. 227945–227961, 2020, doi: 10.1109/ACCESS.2020.3046025.

[12] M. R. Khan *et al.*, "Analysis of Elliptic Curve Cryptography & RSA," *J. ICT Stand.*, vol. 11, no. 4, pp. 355–378, 2023, doi: 10.13052/jicts2245-800X.1142.

[13] A. Ariska and W. Wahyuddin, "Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard)," *J. Sintaks Log.*, vol. 2, no. 2, pp. 9–19, 2022, doi: 10.31850/jsilog.v2i2.1734.

[14] A. Aisiah Ibrahim, "Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)," *J. Tek. Inform. Stmik Antar Bangsa*, vol. III, no. 1, pp. 53–60, 2017.

[15] C. Irawan and E. H. Rachmawanto, "Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA," *Proceeding SENDIU*, vol. I, no. 2, pp. 978–979, 2021.

[16] S. Oktaviani, F. Rizky, and I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *J. Media Inform.*, vol. 4, no. 2, pp. 97–101, 2023, doi: 10.55338/jumin.v4i2.435.

[17] K. Mulyadi, "Penerapan Keamanan Data Menggunakan Kriptografi Dengan Berbagai Metode," *Researchgate.Net*, no. April, 2023, [Online]. Available: https://www.researchgate.net/profile/Kiki-Mulyadi-3/publication/370077480_Penerapan_Keamanan_Data_Menggunakan_Kriptografi_Dengan_Berbagai_Metode/links/643e965a2eca706c8b696ca7/Penerapan-Keamanan-Data-Menggunakan-Kriptografi-Dengan-Berbagai-Metode.pdf

[18] I. G. Indra, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force," *J. Media Inform.*, vol. 4, no. 2, pp. 102–109, 2023,

doi: 10.55338/jumin.v4i2.496.
[19] C. Program, S. Magister, K. Kunci, : Kriptografi, and K. Publik, "Keamanan Data Dengan Metode Kriptografi Kunci Publik," *J. TIMES*, vol. 2, no. 2, pp. 11–15, 2016.
[20] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.
[21] H. Wijaya, "Jurnal Akademika Penerbit Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection," *J. Akad.*, vol. 17, no. 1, pp. 8–13, 2020, [Online]. Available: https://www.ejournal.lppmunidayan.ac.id/index.php/akd
[22] H. Setiawan and A. Rizal, "Rancang Bangun Mobile Secure Chat dengan Mengimplementasikan Metodologi SSDLC-Agile dan Kriptografi," *J. Ilm. SINUS*, vol. 21, no. 1, p. 1, 2023, doi: 10.30646/sinus.v21i1.660.
[23] J. Simarmata, Sriadhi, and R. Rohim, *KRIPTOGRAFI Teknik Keamanan Data & Informasi*, no. April 2022. 2019.
[24] M. Az, S. F. Pane, and R. M. Awangga, "Cryptography: Perancangan Middleware Web Service Encryptor menggunakan Triple Key MD5. Base64, dan AES," *J. Tekno Insentif*, vol. 15, no. 2, pp. 65–75, 2021, doi: 10.36787/jti.v15i1.497.
[25] N. P. E. Merliana, "Pemanfaatan Teknologi Kriptografi dalam mengatasi kejahatan Cyber," *Satya Dharma J. Ilmu Huk.*, vol. 3, no. 2, pp. 23–40, 2020, [Online]. Available: https://ejournal.iahntp.ac.id/index.php/satya-dharma/article/view/678
[26] S. Anwar, "Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES," *J. Format*, vol. 6, no. 1, pp. 65–74, 2017.
[27] S. Anwar, M. I. Komputer, and U. B. Luhur, "Implementasi Pengamanan Data Dan Informasi Dengan," *Semin. Nas. Teknol. Inf. dan Multimed. 2017*, pp. 37–42, 2017.
[28] A. R. Tulloh *et al.*, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption," *J. Mat. UNISBA*, vol. Vol 2, no. 1, pp. 1–8, 2016.
[29] Peniarsih, "Sistem Keamanan Data Dengan Metode Cryptography," *J. Mitra Manaj.*, pp. 11–21, 2020, [Online]. Available: https://journal.universitassuryadarma.ac.id/index.php/jmm/article/viewFile/585/556
[30] N. A. Nanda, S. M. S. Silalahi, D. Fatricia Nasution, M. Sari, and I. Gunawan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data," *J. Media Inform.*, vol. 4, no. 2, pp. 90–93, 2023, doi: 10.55338/jumin.v4i2.428.
[31] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, "Multimedia Security Using Encryption: A Survey," *IEEE Access*, vol. 11, no. June, pp. 63027–63056, 2023, doi: 10.1109/ACCESS.2023.3287858.