SISTEM DOMPET DOKUMEN BERBASIS WEB DENGAN *CLIENT-SIDE ENCRYPTION* MENGGUNAKAN ALGORITMA ASCON DAN *AUTENTIKASI MNEMONIC SEED PHRASE*

SKRIPSI

UIN SUNAN AMPEL
S U R A B A Y A

Disusun Oleh:

M SYAFIQ UBAIDILLAH
09040622067

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL
SURABAYA

2026

PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini,

NAMA	:	M Syafiq Ubaidillah
NIM	:	09040622067
Program Studi	:	Sistem Informasi
Angkatan	:	2022

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul: "SISTEM DOMPET DOKUMEN BERBASIS WEB DENGAN *CLIENT-SIDE ENCRYPTION* MENGGUNAKAN ALGORITMA ASCON DAN *AUTENTIKASI MNEMONIC SEED PHRASE*". Apabila suatu saat nanti terbukti saya melakukan tindakan plagiat, maka saya bersedia menerima sanksi yang telah ditetapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 6 Mei 2026
Yang menyatakan,

(M Syafiq Ubaidillah)
NIM. 09040622067

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi Oleh

NAMA	:	M Syafiq Ubaidillah
NIM	:	09040622067
JUDUL	:	Sistem Dompet Dokumen Berbasis Web Dengan *Client-Side Encryption* Menggunakan Algoritma Ascon Dan *Autentikasi Mnemonic Seed Phrase*

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 6 Mei 2026

Dosen Pembimbing 1	Dosen Pembimbing 2
(Mujib Ridwan, S.Kom., M.T)	(Muhammad Andik Izzudin, M.T)
NIP. 198604272014031004	NIP. 198403072014031001

PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi M Syafiq Ubaidillah ini telah dipertahankan
di depan tim penguji skripsi

di Surabaya, 3 Juni 2026

Mengesahkan,
Dewan Penguji

Dosen Penguji 1	Dosen Penguji 2
Ahmad Yusuf, M.Kom	Dr. Moch Yasin, M.Kom, M.B.A., MTCNA
NIP. 199001202014031003	NIP. 198808302014031001

Dosen Penguji 3	Dosen Penguji 4
Mujib Ridwan, S.Kom., M.T	Muhammad Andik Izzudin, M.T
NIP. 198604272014031004	NIP. 198403072014031001

Mengetahui,

Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

Dr. A. Saepul Hamdani, M.Pd.
NIP. 196507312000031002

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama : M Syafiq Ubaidillah
NIM : 09040622067
Fakultas/Jurusan : Sains dan Teknologi/Sistem Informasi
E-mail address : syafiqubaidillahh@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
☑ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul :

SISTEM DOMPET DOKUMEN BERBASIS WEB DENGAN CLIENT-SIDE ENCRYPTION MENGGUNAKAN ALGORITMA ASCON
DAN AUTENTIKASI MNEMONIC SEED PHRASE

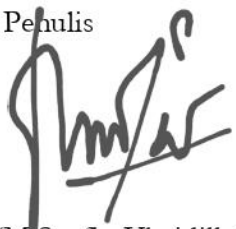
beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 22 Mei 2026

Penulis



(M Syafiq Ubaidillah)

ABSTRAK

SISTEM DOMPET DOKUMEN BERBASIS WEB DENGAN *CLIENT-SIDE ENCRYPTION* MENGGUNAKAN ALGORITMA ASCON DAN *AUTENTIKASI MNEMONIC SEED PHRASE*

Oleh:

M Syafiq Ubaidillah

Perkembangan digitalisasi dokumen meningkatkan efisiensi akses dan penyimpanan, namun juga memunculkan risiko kebocoran data akibat lemahnya perlindungan pada sistem berbasis *cloud* serta adanya *trade-off* antara keamanan dan kemudahan penggunaan, di mana sistem yang mudah digunakan sering kali mengorbankan aspek keamanan. Penelitian ini bertujuan merancang dan mengimplementasikan sistem dompet dokumen berbasis web dengan menerapkan *client-side encryption* menggunakan algoritma Ascon serta autentikasi *mnemonic seed phrase* sebagai solusi yang menyeimbangkan kedua aspek tersebut. Metode yang digunakan adalah model pengembangan *waterfall* meliputi analisis, perancangan, implementasi, dan pengujian. Sistem mengenkripsi data di sisi klien sebelum disimpan ke server sehingga hanya pemilik kunci yang dapat mengaksesnya, dengan Ascon dipilih karena efisien dan ringan, serta *seed phrase* sebagai *autentikasi* yang lebih aman dibandingkan *password* konvensional. Hasil penelitian menunjukkan bahwa sistem mampu meningkatkan keamanan dokumen digital tanpa mengurangi kemudahan penggunaan secara signifikan, yang dibuktikan melalui pengujian *System Usability Scale* (SUS) dengan hasil kategori baik. Dengan demikian, penelitian ini memberikan kontribusi dalam pengembangan sistem pengelolaan dokumen digital yang aman, efisien, dan berorientasi pada pengguna.

Kata Kunci: keamanan data, *client-side encryption*, Ascon, *mnemonic seed phrase*, *trade-off* keamanan dan *usability*

ABSTRACT

WEB-BASED DOCUMENT WALLET SYSTEM WITH CLIENT-SIDE ENCRYPTION USING THE ASCON ALGORITHM AND MNEMONIC SEED PHRASE AUTHENTICATION

By:

M Syafiq Ubaidillah

The rapid growth of digital document management improves accessibility and efficiency but also introduces significant risks of data breaches due to weak cloud security mechanisms and the inherent trade-off between security and *usability*, where more user-friendly systems often compromise security. This study aims to design and implement a web-based document wallet system by applying client-side encryption using the Ascon algorithm and mnemonic seed phrase authentication to balance these aspects. The research adopts the waterfall development model, including analysis, design, implementation, and testing phases. The system encrypts data on the client side before storing it on the server, ensuring that only the key owner can access the data; Ascon is selected for its efficiency and lightweight performance, while mnemonic seed phrases provide stronger authentication compared to conventional password-based methods. The results indicate that the proposed system enhances digital document security without significantly reducing *usability*, as demonstrated by System *Usability* Scale (SUS) testing results in the good category. Therefore, this study contributes to the development of a secure, efficient, and user-oriented digital document management system.

Keywords: data security, client-side encryption, Ascon, mnemonic seed phrase, security-*usability* trade-off

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. *Symmetry*, *11*(6), 774. https://doi.org/10.3390/sym11060774

Ahsana, S. H., Syahputra, M. B., Putri, A. F. F. M., & Prasetyo, A. A. (2023a). ANALISIS PERBANDINGAN PERFORMA ANTARA MySQL dan PostgreSQL. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi (SITASI)*. https://repository.upnjatim.ac.id/28497/

Ahsana, S. H., Syahputra, Putri, A. F. F. M., & Prasetyo, A. A. (2023b). ANALISIS PERBANDINGAN PERFORMA ANTARA MySQL dan PostgreSQL. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi (SITASI)*. https://repository.upnjatim.ac.id/28497/

Akbar, I., Budiman, Niqotaini, Z., & Fauzi, A. R. (2023). ANALISIS DAN PERANCANGAN SISTEM PENJUALAN PADA TOKO XYZ BERBASIS WEB DAN MOBILE MENGGUNAKAN UML. *NUANSA INFORMATIKA*, *17*(2), 71–82. https://doi.org/10.25134/ilkom.v17i2.13

Alfauzain, A., Wisandra, A., & Azzahra, P. S. (2023). Perancangan Sistem Informasi Pendaftaran Online Pasien Rawat Jalan Pada Puskesmas Menggunakan Metode Prototype. *Jurnal Testing Dan Implementasi Sistem Informasi*, *1*(2), 122–136. https://doi.org/10.55583/jtisi.v1i2.548

Alfiah, F., Sudarji, R., & Al Fatah, D. T. (2020). Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake. *ADI Bisnis Digital Interdisiplin Jurnal*, *1*(1), 22–34. https://doi.org/10.34306/abdi.v1i1.114

Amelia, F., & Hartejo, B. W. (2025). Developing a Prototype for Enhancing Data Security in LoRaBased Theft Detection Systems Using ASCON-128 Encryption. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *13*(1), 110–124. https://doi.org/10.52549/ijeei.v13i1.6021

Ananda, S. P., Lukman, S., & Irfan. (2022). Analisa Metode Kriptografi Modem Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan

Mendekripsi File Dokumen Digital: Array. *Jurnal Ilmiah Komputasi*, *21*(3), 333–344. https://doi.org/10.32409/jikstik.21.3.2973

Arafat, M., Trimarsiah, Y., & Susantho, H. (2022). Rancang Bangun Sistem Informasi Pemesanan Online Percetakan Sriwijaya Multi Grafika Berbasis Website. *INTECH*, *3*(2), 58–63. https://doi.org/10.54895/intech.v3i2.1691

Arianti, T., Fa'izi, A., Adam, S., & Wulandari, M. (2022). *PERANCANGAN SISTEM INFORMASI PERPUSTAKAAN MENGGUNAKAN DIAGRAM UML (UNIFIED MODELLING LANGUAGE)*. *1*.

Ariska, A., & Wahyuddin, W. (2022). Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard). *Jurnal Sintaks Logika*, *2*(2), 9–19. https://doi.org/10.31850/jsilog.v2i2.1734

Arwen. (2025, February 7). Understanding Sequence Diagrams. *PlantText*. https://blog.planttext.com/2025/02/07/sequence-diagrams/

Atara, I., Syallomeita, S., & Haksoro, R. A. B. (2025). *ANALISIS KRIMINOLOGI TERHADAP PENCURIAN DATA PRIBADI DI ERA DIGITAL: STUDI KASUS KEBOCORAN DATA PENGGUNA APLIKASI MYPERTAMINA TAHUN 2023*.

Brooke, J. (1996). *SUS - A quick and dirty usability scale*.

Brooke, J. (2013). SUS: A Retrospective. *Journal of Usability Studies*, *08*(02).

Burlingham, J. (2023, January 10). How to Recover Your Lost Seed Phrase. *Professional Crypto Recovery*. https://www.professionalcryptorecovery.com/blog/recover-seed-phrase/

Chauhan, A., & Verma, D. (2024). *Harnessing Lightweight Ciphers for PDF Encryption* (arXiv:2409.09428). arXiv. https://doi.org/10.48550/arXiv.2409.09428

Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. *Information*, *14*(12), 641. https://doi.org/10.3390/info14120641

Djong, H. S., & Siswanto, S. (2022). *IMPLEMENTASI KRIPTOGRAFI DENGAN MENGGUNAKAN METODE RC4 DAN AES-256 UNTUK MENGAMANKAN FILE DOKUMEN PADA PT VARNION TECHNOLOGY SEMESTA*.

Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing. *Journal of Cryptology*, *34*(3), 1–42. https://doi.org/10.1007/s00145-021-09398-9

Edler, D. (2023). *Client side encryption in the browser and key management*. https://doi.org/10.13140/RG.2.2.20799.38567

Eleshin, F., Sun, Q., Ye, M., Das, S., & Hong, J. I. (2025). Of Secrets and Seedphrases: Conceptual Misunderstandings and Security Challenges for Seed Phrase Management among Cryptocurrency Users. *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–19. https://doi.org/10.1145/3706598.3713209

Fachri, B., & Rizal, C. (2024). *Penerapan Metode Waterfall Dalam Perancangan Sistem Informasi Merdeka Belajar Kampus Merdeka Berbasis Web*. *2*(3).

Fardiansyah, H., Rizkia, N., Sattar, Umiyati, H., & Badriati, T. (2023). *Manajemen Arsip*.

Fauziah, Wibowo, Y. A., & Irwansyah, I. P. (2024). SISTEM INFORMASI PENJUALAN DAN PEMESANAN KERTAS PERCETAKAN BERBASIS WEB STUDI KASUS pada CV. XYZ. *INFORMATIKA SAINS TEKNOLOGI*, *2*(1), 22–29.

Fawa'ati, T. M., & Sukri, H. (2022). APPLICATION OF ARTIFICIAL INTELLIGENCE (AI) IN SEARCH ENGINE OPTIMIZATION (SEO). *Jurnal Alih Teknologi Sistem Informasi (JATSI)*, *2*(1). https://jurnal.umitra.ac.id/index.php/JATSI/article/view/902

Hakim, M. A. R., Fatmawati, N. M., Kahfi, N. S., & Lutfiyah, L. (2025). Keselamatan Nasabah Pinjaman Online dalam Perspektif Hukum Islam: Studi Kasus Berdasarkan Konsep Hifdz al-Mal dan Maqasid al- Shariah. *Journal of Sharia Economic Law*, *3*(1), 1–14. https://doi.org/10.37680/jshel.v3i1.6216

Hananiya, P., Badau, K. M., & Awodoyin, F. O. (2024). *INFORMATION SYSTEMS IN ORGANIZATIONS*.

Handoyo, J., & Subakti, Y. M. (2020). KEAMANAN DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION

STANDARD (AES). *Jurnal SITECH : Sistem Informasi dan Teknologi*, *3*(2), 143–152. https://doi.org/10.24176/sitech.v3i2.5865

Hanggara, B. T., Nasrullah, M. H., & Pramono, D. (2024). Analisis Perbandingan Performa Framework NestJS dan Lumen Pada Studi Kasus Aplikasi Berbasis REST API. *J-INTECH (Journal of Information and Technology)*, *12*(1), 181–189. https://doi.org/10.32664/j-intech.v12i1.1354

Hendriana, D., & Subarkah, M. A. (2023). PERAN ILMU PENGETAHUAN DAN PENGARUH KEMAJUAN TEKNOLOGI DIGITAL DALAM PELAKSANAAN TUGAS KEKHALIFAHAN MANUSIA. *Rausyan Fikr : Jurnal Pemikiran Dan Pencerahan*, *19*(1). https://doi.org/10.31000/rf.v19i1.7730

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum*, *37*(2), 119. https://doi.org/10.26532/jh.v37i2.16272

Kalvin, F., Sa'ad, M. I., & Pukeng, A. F. (2025a). *Implementasi Seed Phrase Dalam Keamanan Dompet Kripto Pada Metamask*. *6*(2).

Kalvin, F., Sa'ad, M. I., & Pukeng, A. F. (2025b). Implementasi Seed Phrase Dalam Keamanan Dompet Kripto Pada Metamask. *Bulletin of Information Technology (BIT)*, *6*(2), 136–147. https://doi.org/10.47065/bit.v6i2.2026

Karanam, R. (2020, June 6). *Server Side vs Client Side Encryption—KMS-S3—AWS Certification Cheat Sheet*. In28minutes Cloud. https://cloud.in28minutes.com/aws-certification-server-side-vs-client-side-encryption-kms-s3

Kim, C., Kim, S., Sohn, K., Son, Y., Kumar, M., & Kim, S. (2025). Secure and Scalable File Encryption for Cloud Systems via Distributed Integration of Quantum and Classical Cryptography. *Applied Sciences*, *15*(14), 7782. https://doi.org/10.3390/app15147782

Kim, J.-H., Newberry, P., & Wagman, L. (2025). Trading off convenience and privacy in social login. *Economics Letters*, *254*, 112409. https://doi.org/10.1016/j.econlet.2025.112409

Kristianti, L., & Nurcahyani, I. (2023, January 19). *BSSN ungkap serangan keamanan siber di 2022 turun dibanding 2021*. Antara News.

https://www.antaranews.com/berita/3356178/bssn-ungkap-serangan-keamanan-siber-di-2022-turun-dibanding-2021

Lantu, J., Santa, K., Sangkop, F., & Kembuan, O. (2025). Pengembangan Sistem Enkripsi File Berbasis Web Dengan Menggunakan Metode Advanced Encryption Standard. *JOURNAL OF INFORMATICS, BUSINESS, EDUCATION AND INNOVATION TECHNOLOGY*, *3*(5), 97–109.

Lin, S., Cui, L., & Ke, N. (2024). End-to-End Encrypted Message Distribution System for the Internet of Things Based on Conditional Proxy Re-Encryption. *Sensors*, *24*(2), 438. https://doi.org/10.3390/s24020438

Lubis, A. S., & Ginting, M. P. A. (2024). Pengujian Aplikasi Berbasis Web Data Ska Menggunakan Metode Black Box Testing. *Cosmic Jurnal Teknik*, *1*(1), 41–48.

Maharani, P. (2025). Pengembangan Website PT. Rantangin Digital Indonesia Menggunakan Framework Next Js dan Tailwind CSS. *Repeater : Publikasi Teknik Informatika dan Jaringan*, *3*(1), 129–137. https://doi.org/10.62951/repeater.v3i1.355

Margaretha, J., & Voutama, A. (2023). Perancangan Sistem Informasi Pemesanan Tiket Konser Musik Berbasis Web Menggunakan Unified Modeling Language (UML). *JOINS (Journal of Information System)*, *8*(1), 20–31. https://doi.org/10.33633/joins.v8i1.7107

Mustakim, D. T., Kusyanti, A., & Trisnawan, P. H. (2025). IMPLEMENTASI ALGORITMA ENKRIPSI SPECK UNTUK PENGAMANAN MNEMONIC PHRASE PADA CRYPTOCURRENCY WALLET. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *12*(3), 525–532. https://doi.org/10.25126/jtiik.2025129463

Naja, S., Akbar, R., & Ismail. (2024). Sistem Informasi Pengelolaan Arsip Digital Pada Kantor Dinas Pertanian Provinsi Aceh Berbasis Web. *Jurnal Sistem Komputer (SISKOM)*, *4*(2), 60–71. https://doi.org/10.35870/siskom.v4i2.813

Nawali, I., & Suteja, D. B. R. (2023). PEMBUATAN SISTEM APLIKASI BERBASIS WEBSITE KONSULTASI ORANG TUA DENGAN

PSIKOLOG UNTUK KESEHATAN MENTAL ANAK. *Jurnal STRATEGI - Jurnal Maranatha*, *5*(1), 110–129.

Nisa, Z. (2023). *PROGRAM STUDI ILMU AL-QUR'AN DAN TAFSIR FAKULTAS USHULUDDIN, ADAB DAN DAKWAH UNIVERSITAS ISLAM NEGERI K.H. ABDURRAHMAN WAHID PEKALONGAN 2023*.

Novalia, E., & Voutama, A. (2022). Black Box Testing dengan Teknik Equivalence Partitions Pada Aplikasi Android M-Magazine Mading Sekolah. *Syntax : Jurnal Informatika*, *11*(01), 23–35. https://doi.org/10.35706/syji.v11i01.6413

Nurhidayat, N., Dhiauhaq, F., Andriani, N., & Dewi, D. S. (2024). Keamanan Informasi dan Kepatuhan Sistem Informasi Manajemen di MA Al-Furqon Cimerak. *Jurnal Ilmiah Al-Muttaqin*, *9*(2), 72–77. https://doi.org/10.37567/al-muttaqin.v9i2.2643

Nurjayanti, R., & Novratilova, S. (2025). Evaluasi Penggunaan Aplikasi Mobile Jaminan Kesehatan Nasional (MJKN) Pada Pendaftaran Rawat Jalan Menggunakan Metode TAM. *JURNAL KESEHATAN TROPIS INDONESIA*, *3*(3), 161–173. https://doi.org/10.63265/jkti.v3i3.112

Patria, M., & Andriati, D. A. (2025). Analisis Komparatif Performa AES-GCM dan ChaCha20-Poly1305 dalam Enkripsi Dokumen PDF Berbasis AEAD. *Arcitech: Journal of Computer Science and Artificial Intelligence*, *5*(1), 49–69. https://doi.org/10.29240/arcitech.v5i1.13645

Platinus, M., Rusnak, P., & Voisine, A. (2025, September 29). *BIP 39: Mnemonic code for generating deterministic keys*. https://bips.dev/39/?utm_source=chatgpt.com

Pote, P., & Bansode, R. (2025). *Performance Evaluation of Post-Quantum Cryptography: A Comprehensive Framework for Experimental Analysis*. https://www.researchgate.net/publication/388845887_Performance_Evaluation_of_Post-Quantum_Cryptography_A_Comprehensive_Framework_for_Experimental_Analysis/link/67a9f13a645ef274a4794a24/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

Pressman, R. S. (2010). *Software engineering: A practitioner's approach* (7th ed). McGraw-Hill.

Putra, M. G. L., & Octantia, H. (2021). Analisis dan Perencangan Aplikasi E-Learning Berbasis Gamification (Studi Kasus Program Studi Sistem Informasi Institut Teknologi Kalimantan). *Jurnal Teknologi Informasi dan Ilmu Komputer*, *8*(3), 571–578. https://doi.org/10.25126/jtiik.2021834368

Putra, W., & Yudistira, B. (2025). *Analisis Komparatif Efektivitas Client-Side Encryption Cryptomator dan Rclone Crypt pada Google Drive*. *2*(21).

Ramalinda, D., Jayadi, & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, *2*(6), 665–671. https://doi.org/10.62504/jimr679

Ramdany, S. W., Kaidar, S. A., Aguchino, B., Putri, C. A. A., & Anggie, R. (2024). *Penerapan UML Class Diagram dalam Perancangan Sistem Informasi Perpustakaan Berbasis Web*.

Redaksi NU Online. (n.d.-a). *Surat Al-Anfal Ayat 27: Arab, Latin, Terjemah dan Tafsir Lengkap | Quran NU Online*. Retrieved October 2, 2025, from https://quran.nu.or.id/al-anfal/27

Redaksi NU Online. (n.d.-b). *Surat An-Nur Ayat 27: Arab, Latin, Terjemah dan Tafsir Lengkap | Quran NU Online*. Retrieved October 2, 2025, from https://quran.nu.or.id/an-nur/27

Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World from Edge to Core*.

Rifandi, F., Adriansyah, T. V., & Kurniawati, R. (2022). Website Gallery Development Using Tailwind CSS Framework. *Jurnal E-Komtek*, *6*(2), 205–214. https://doi.org/10.37339/e-komtek.v6i2.937

Rohandi, M., Husain, N., & Bay, I. W. (2021). *Usability* testing of intensive course mobile application using the *usability* scale system. *ILKOM Jurnal Ilmiah*, *13*(3), 252–258. https://doi.org/10.33096/ilkom.v13i3.821.252-258

Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability*, *15*(7), 6019. https://doi.org/10.3390/su15076019

Saputra, M. W. A., Ashari, S. A., & Larosa, E. (2024). Keamanan Data Sistem Informasi Akademik ITEkes Mahardika: Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES. *Inverted: Journal of Information Technology Education*, *4*(1), 79–85. https://doi.org/10.37905/inverted.v4i1.22969

Sarasa Laborda, V., Hernández-Álvarez, L., Hernández Encinas, L., Sánchez García, J. I., & Queiruga-Dios, A. (2025). Study About the Performance of Ascon in Arduino Devices. *Applied Sciences*, *15*(7), 4071. https://doi.org/10.3390/app15074071

Sari, A. S., & Hidayat, R. (2022). Designing website vaccine booking system using golang programming language and framework react JS. *Journal of Information System, Informatics and Computing*, *6*(1), 22–39. https://doi.org/10.52362/jisicom.v6i1.760

Setyaningsih, E. (2020). Keamanan file dokumen menggunakan algoritme Advanced Encryption Standard pada aplikasi berbasis Android. *JNANALOKA*, 11–23. https://doi.org/10.36802/jnanaloka.2020.v1-no1-11-23

Sitorus, J. H. P., & Sakban, M. (2021). *Perancangan Sistem Informasi Penjualan Berbasis Web Pada Toko Mandiri 88 Pematangsiantar*. *05*.

Sommerville, I. (2016). *Software engineering* (Tenth edition). Pearson.

Sudarsana, F., Suryana, S., & Saprialman. (2024). *ANALISIS DIGITALISASI ARSIP DI DINAS ARSIP DAN PERPUSTAKAAN KABUPATEN KARAWANG*. *7*.

Sugiarto, A. J., Lie, G., & Putra, M. R. S. (2024). Perlindungan Kepada Nasabah Bank Terhadap Kebocoran Data (Studi Kasus Kebocoran Data pada Bank Indonesia). *Journal of Accounting Law Communication and Technology*, *2*(1), 107–114. https://doi.org/10.57235/jalakotek.v2i1.4298

Suherni, P. (2023). Aplikasi Sistem Informasi Transaksi Pelayanan Obat Diapotek Menggunakan Metode Waterfall. *Jurnal SANTI - Sistem Informasi Dan Teknik Informasi*, *1*(2), 23–31. https://doi.org/10.58794/santi.v1i2.323

Taufik, C. I. N., & Juhana, A. (2025). The Privacy Paradox of Students' Personal Data Security in the Digital Age. *SATESI: Jurnal Sains Teknologi Dan Sistem Informasi*, *5*(1), 1–6. https://doi.org/10.54259/satesi.v5i1.3417

Turan, M. S. (2023). *Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process*. https://doi.org/10.6028/NIST.IR.8454

Turan, M. S., Mckay, K. A., Chang, D., Kang, J., & Kelsey, J. (2025). *Ascon-Based Lightweight Cryptography Standards for Constrained Devices* (NIST SP 800-232; p. NIST SP 800-232). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-232

Wahyudin, Y., & Rahayu, D. N. (2020). Analisis Metode Pengembangan Sistem Informasi Berbasis Website: A Literatur Review. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi dan Komunikasi*, *15*(3), 26–40. https://doi.org/10.35969/interkom.v15i3.74

walker, greg. (2025). *Derivation Paths | Locating Keys and Addresses in HD Wallets*.

Welda, W., Putra, D. M. D. U., & Dirgayusari, A. M. (2020). *Usability* Testing Website Dengan Menggunakan Metode System *Usability* Scale (Sus)s. *International Journal of Natural Science and Engineering*, *4*(3), 152–161. https://doi.org/10.23887/ijnse.v4i2.28864

Widodo, B. E., & Purnomo, A. S. (2020). IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77. https://doi.org/10.20884/1.jutif.2020.1.2.21

Widyatmoko, W., & Pamungkas, N. (2022). Pemodelan Unified Modeling Language pada Sistem Aplikasi Pariwisata (SiAP). *Jurnal Bumigora Information Technology (BITe)*, *4*(1), 73–84. https://doi.org/10.30812/bite.v4i1.1871

Yosey, B. W. O., Putri, I. A. J., Ratnaningsih, D., Arisusanty, D. J., Nofandi, F., & Amrullah, R. A. (2024). Pengaruh Teknologi Digital dalam Pengelolaan Dokumen Crewchange di PT. Equinox Bahari Utama. *Journal of Business, Finance, and Economics (JBFE)*, *5*(2), 282–292. https://doi.org/10.32585/jbfe.v5i2.5734

Yulianto, N. A. (2025). *Sistem pemendek url berbasis pretrained language model guided multi-level attention network untuk pendeteksian url berbahaya* [Undergraduate, UIN Sunan Ampel Surabaya]. http://digilib.uinsa.ac.id/80150/

Yunita, I. R., Pramono, A., Waluyo, R., & . S. (2022). Implementasi Metode Waterfall Pada Perancangan Aplikasi Rekam Medis Berbasis Website dan Whatshap Gateway. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, *5*(1), 8–16. https://doi.org/10.20895/inista.v5i1.852