

Vol. 4 No. 2 September 2025

E-ISSN : 2962-8628

PROSIDING

SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI (SENAFTI)

"Agentic AI: Dampak Pada Interaksi Manusia dan Mesin"

- **Cyber Security**
- **Programming**
- **Artificial Intelligence**
- **Information System**

STEERING COMMITTEE

Pelindung

Prof. Dr. Agus Setyo Budi, M.Sc

Penanggung Jawab

Dr. Ir. Achmad Solichin, S.Kom., M.T.I

Ketua Pelaksana

Dr. Moh. Syafrullah, M.Kom., M.Sc

Wakil Ketua Pelaksana

Bima Cahya Putra, S.Kom, M.Kom

Sekretaris

Retno Wulandari, S.Kom., M.Kom.

Bendahara

1. Widodo MS, S.Kom
2. Noni Juliasari, S.Kom., M.Kom.

Humas, Publikasi, Dokumentasi dan Desain

1. Reva Ragam Santika, S.Kom., M.M., M.Kom
2. Rizka Tiaharyadini, S.Kom., M.M., M.Kom
3. Fahmi AkhtarRakaiz

Acara

1. Dr. Indra, S.Kom., M.T.I
2. Windarto, S.Kom., M.Kom
3. Agnes Aryasanti, S.Kom., M.Kom

Pengelola Makalah dan Mitra Bestari

1. Wahyu Pramusinto, S.Kom., M.Kom
2. Kukuh Harsanto, S.Kom., M.Kom
3. Dian Anubhakti, S.Kom., M.Kom

Pengelola Editor dan Jurnal

1. Rizky Pradana, S.Kom., M.Kom
2. Indah Puspasari Handayani, S.Kom., M.Kom
3. Yesi Puspita Dewi, S.Kom., M.Kom
4. Hadidtyo Wisnu Wardani, S.Kom., M.Kom
5. Sri Wahyuningsih, S.Kom., M.Kom
6. Ikhsan Rahdiana, S.Kom., M.Kom
7. Jeremy Jonathan, S.Kom., M.Kom
8. Anwar Rifai, M.Kom
9. Iman Permana, S.Kom, M.Kom

Pengelola Teknologi Informasi

1. Sovan Dianarto, S.Kom.
2. Dolly Virgian Shaka Yudha Shakti, S.Kom., M.Kom.

REDAKSI

Pelindung : Prof. Dr. Agus Setyo Budi, M.Sc
Penanggung Jawab : Dr. Ir. Achmad Solichin, S.Kom., M.T.I
Ketua Pelaksana : Dr. Moh. Syafrullah, M.Kom., M.Sc
Wakil Ketua Pelaksana : Bima Cahya Putra, S.Kom, M.Kom

Wakil Ketua Redaksi :

1. Wahyu Pramusinto, S.Kom., M.Kom
2. Kukuh Harsanto, S.Kom., M.Kom
3. Dian Anubhakti, S.Kom., M.Kom

Redaksi Pelaksana :

1. Rizky Pradana, S.Kom, M.Kom
2. Indah Puspasari Handayani, S.Kom., M.Kom.
3. Devit Setiono, S.Kom., M.Kom.
4. Jeremy Jonathan, S.Kom., M.Kom.
5. Yesi Puspita Dewi, S.Kom., M.Kom.
6. Hadidtyo Wisnu Wardani, S.Kom., M.Kom.
7. Sri Wahyuningsih, S.Kom, M.Kom.
8. Anwar Rifai, M.Kom
9. Iman Permana, S.Kom, M.Kom

MITRA BESTARI

1. Prof. Dr. Edy Winarno, S.T., M.Eng. (Universitas Muhammadiyah Semarang)
2. Dr. Suwanto raharjo, S.Si., M.Kom (IST AKPRIND Yogyakarta)
3. Dr. EH. Riyadi, MTL. (Badan Pengawas Tenaga Nuklir)
4. Dr. Budi Rahmani, S.Pd., M.Kom. (STMIK Banjarbaru)
5. Dr. Hamdani (Universitas Mulawarman)
6. Dr. Ir. Didit Suprihanto, S.T., M.Kom., IPM (Univ. Mulawarman)
7. Dr. Nanang Triagung Edi Hermawan, M.T. (BAPETEN)
8. Dr. Khoerul Anwar, ST, MT (STMIK PPKIA PRADNYA PARAMITA)
9. Dr. Ir. Ridowati Gunawan, S.Kom., M.T. (Universitas Sanata Dharma)
10. Dr. Ir. Mardi Hardjianto, M.Kom. (Universitas Budi Luhur)
11. Dr. Ir. Goenawan Brotosaputro, S.Kom., M.Sc. (Institut Sains dan Bisnis Atma Luhur)
12. Dr. Achmad Solichin, S.Kom., M.T.I (Universitas Budi Luhur)
13. Dr. Ir. Deni Mahdiana, S.Kom, M.M, M.Kom (Universitas Budi Luhur)
14. Dr. Darwan, M.Kom. (IAIN Syekh Nurjati Cirebon)
15. Dr. Ir. Gandung Triyono, S.Kom., M.Kom (Universitas Budi Luhur)
16. Dr. Aji Supriyanto, S.T., M.Kom (Universitas Stikubank)
17. Dr. Jumi, S.Kom, M.Kom. (Politeknik Negeri Semarang)
18. Dr. Aris Sugiharto, S.Si, M.Kom (Universitas Diponegoro)
19. Dr. Anindita Septiarini, S.T., M.Cs. (Universitas Mulawarman)
20. Dr. Imelda, M.Kom (Universitas Budi Luhur)
21. Dr. Ir. Utomo Budiyanto, M.Kom., M.Sc (Universitas Budi Luhur)
22. Dr. Ir. Jan Everhard R MT (Universitas Budi Luhur)
23. Dr. Ir. Hari Soetanto, S.Kom, M.Sc (Universitas Budi Luhur)
24. Dr. Abdiansah, S.Kom., M.CS. (Universitas Sriwijaya)
25. Dr. Indra, M.T.I (Universitas Budi Luhur)
26. Dr. Heriyanto, A.Md, S.Kom, M.Cs (UPN Veteran Yogyakarta)
27. Dr. Lilis Susanti Setianingsih, S.T., M.S. (Badan Pengawas Tenaga Nuklir)
28. Dr. Linda Nur Afifa, S.T., M.T (Universitas Darma Persada)
29. Dr. Helna Wardhana, M.Kom. (Universitas Bumigora)
30. Dr. Khasnur Hidjah, S.Kom., M.Cs. (Universitas Bumigora Mataram)
31. Dr. Hendra Cipta, M.Si (Universitas Islam Negeri Sumatera Utara Medan)
32. Dr. Yulianto Triwahyuadi Polly, S.Kom., M.Cs (Universitas Nusa Cendana)
33. Dr. Mohammad Syafrullah, M.Kom, M.Sc (Universitas Budi Luhur)
34. Dr. Ir. Aslan Alwi, S.Si., M.Cs (Universitas Muhammadiyah Ponorogo)
35. Dr. Gamma Kosala, S.Si (Telkom University)
36. Dr. Ir. Lasmedi Afuan, ST.,M.Cs (Universits Jenderal Soedirman)
37. Dr. Rahmad Hidayat S.Kom., M.Cs (Politeknik Negeri Lhokseumawe)
38. Dr. Indra Riyanto, S.T., M.T (Universitas Budi Luhur)
39. Dr. Ir. Nurul Hidayat, SPt., M.Kom (Universitas Jenderal Soedirman)
40. Dr. Muhammad Syaukani, ST, SH, M.Cs,M.Kom (Institut Teknologi Bisnis dan Bahasa Dian Cipta Cendikia)
41. Ts. Setyawan Widyarto, MSc., PhD. (Universiti Selangor, Universitas Budi Luhur)
42. Dr.Eng. Akhmad Unggul Priantoro (Universitas Budi Luhur)
43. Dr. Dedi Trisnawarman, S.Si., M.Kom (Universitas Tarumanagara)
44. Windarto, S.Kom, M.Kom (Universitas Budi Luhur)
45. Agus Umar Hamdani, M.Kom (Universitas Budi Luhur)
46. Irawan, S.Kom., M.Kom. (Universitas Budi Luhur)

47. Hendri Irawan, S.Kom., M.T.I. (Universitas Budi Luhur)
48. Yuliazmi S.Kom, M.Kom (Universitas Budi Luhur)
49. Grace Gata, S.Kom., M.kom (Universitas Budi Luhur)
50. Dolly Virgian Shaka Yudha Sakti, M.Kom (Universitas Budi Luhur)
51. Kelik Sussolaikah, S.Kom., M.Kom (Universitas PGRI Madiun)
52. Anita Ratnasari, S.Kom, M.Kom (Universitas Dian Nusantara)
53. Dwi Pebrianti, S.T., M. Eng., Ph.D, Eng. Tech., SMIEEE, IPU (Universitas Budi Luhur)
54. Arita Witanti S.T.,M.T (Universitas Mercu Buana Yogyakarta)
55. Wiwien Hadikurniawati, S.T., M.Kom. (Universitas Stikubank)
56. Reva Ragam Santika, M.Kom (Universitas Budi Luhur)
57. Agnes Aryasanti, M.Kom (Universitas Budi Luhur)
58. Atik Ariesta, S.Kom., M.Kom. (Universitas Budi Luhur)

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT dan hanya karena rahmat dan karunia-Nya, Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Ke-6 pada Tahun 2025 dapat terlaksana dengan baik. Prosiding seminar ini merupakan kumpulan makalah hasil penelitian para akademisi dan peneliti yang sebelumnya telah dipresentasikan pada SENAFI ke-4 secara daring (*online*) pada tanggal 20 September 2025 dengan tema “Agentic AI: Dampak Pada Interaksi Manusia dan Mesin”. SENAFI ke-6 telah menerima dan menerbitkan artikel ilmiah dari beberapa perguruan tinggi yang berasal dari 3 provinsi di Indonesia, yaitu DKI Jakarta, UPN Veteran Yogyakarta (Yogyakarta), Universitas Stikubank (Jawa Tengah) dan Univ. Muhammadiyah Metro (Lampung).

Penyusunan prosiding ini bertujuan untuk penyebarluasan hasil-hasil penelitian dan kajian dalam bidang teknologi informasi. Selain itu, penyusunan prosiding ini juga dimaksudkan agar masyarakat luas dapat mengetahui berbagai informasi terkait dengan penyelenggaraan SENAFI ke-6. Buku prosiding ini berisi 4 (empat) topik yaitu: Cyber Security, Artificial Intelligence, Programming, Information System.

Pada kesempatan ini kami menyampaikan terima kasih yang sebesar-besarnya kepada para akademisi dan peneliti atas hasil karya dan sumbangan pemikiran yang dipresentasikan dalam bentuk makalah dan presentasi ilmiah. Juga kami sampaikan terima kasih kepada para mitra bestari yang telah mereview semua makalah sehingga kualitas isi dari makalah dapat terjaga dan dipertanggungjawabkan. Tak lupa kepada semua pihak yang telah memberikan dukungan bagi terselenggaranya SENAFI dan atas tersusunnya prosiding ini. Harapan kita bersama, semoga prosiding ini dapat menambah khasanah pengembangan ilmu pengetahuan dan teknologi informasi di Indonesia.

Jakarta, September 2025

Tim Penyusun

DAFTAR ISI

STEERING COMMITTEE	i
REDAKSI.....	3
MITRA BESTARI.....	4
KATA PENGANTAR.....	6
DAFTAR ISI.....	7

CYBER SECURITY

IMPLEMENTASI AES-256 UNTUK MENGAMANKAN DOKUMEN KREDENSIAL KLIEN (STUDI KASUS: PT STUDIO INOVASI TEKNOLOGI) Iqbal Syafiudin, Titin Fatimah	1-10
PERBANDINGAN ALGORITMA KRIPTOGRAFI AES-128 DAN DES UNTUK KEAMANAN DOKUMEN PADA PT JASA RAHARJA PUTERA Sultan Nabil, Hari Soetanto.....	11-20
IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN DATA PENJUALAN DI TOKO DIAH KEMASAN KOSMETIK Danang Pandya Pangestu; Dolly Virgian Shaka Yudha Sakti	21-28
IMPLEMENTASI ENKRIPSI DATA SISWA DAN TRANSAKSI PAUD AI-HANIF MENGGUNAKAN ALGORITMA RC4 BERBASIS WEB Muhamad Salamun, Reva Ragam Santika	29-38
IMPLEMENTASI KRIPTOGRAFI ALGORITMA VIGENERE CIPHER DAN RC4 MODIFIKASI UNTUK MENGAMANKAN DATA Galih Sadewo, Dolly Virgian Shaka Yudha Sakti.....	39-48
IMPLEMENTASI AES-128 EFISIEN PADA APLIKASI WEB UNTUK PENGAMANAN DOKUMEN BANTUAN SOSIAL DI TINGKAT KELURAHAN Rizki Apriansyah Wijaya, Sri Mulyati.....	49-58
PENERAPAN ALGORITMA NAIVE BAYES UNTUK ANALISIS SENTIMEN APLIKASI SPOTIFY PADA GOOGLE PLAY STORE Novrian Novrian, Hari Soetanto	59-68
PENERAPAN KRIPTOGRAFI AES-128 UNTUK KEAMANAN DATA PEGAWAI PADA PERUSAHAAN LOGISTIK DI JAKARTA Prasetyo Ari Nugroho, Rizky Pradana	69-76

PENERAPAN ALGORITMA AES-CBC DAN AES-GCM UNTUK PENGAMANAN DOKUMEN	GEREJA
Leonard Reinhard Roscott, Subandi	77-84
IMPLEMENTASI ALGORITMA AES-192 UNTUK MENGAMANKAN FILE DATA DI POJOK	UMKM KOTA CILEDUG
Ahmad Dhani Yazid Saputro, imelda	85-94
IMPLEMENTASI AES-256 BERBASIS WEB PADA DATA PENJUALAN HARIAN DI TOKO	KOPI TUKU JOGLO
Hanifah, Dewi Kusumaningsih	95-103
IMPLEMENTASI HYBRID ENCRYPTION ECC-AES UNTUK PENGAMANAN KOMUNIKASI DAN BERBAGI FILE BERBASIS WEB	
Risqi Rahman Pratama, Dolly Virgian Shaka Yudha Sakti	104-113
OPTIMALISASI KEAMANAN DATA DENGAN PENERAPAN ALGORITME KRIPTOGRAFI	AES-128 BERBASIS WEB
Rafli Adhies Attha, Titin Fatimah	114-121
PROTOTIPE SISTEM MONITORING SUHU DAN KELEMBABAN RUANG SERVER BERBASIS	IOT ESP32 DAN DHT22
Fahrul Kusuma, Sejati Waluyo	122-129
OTOMASI PENGATURAN JARINGAN LAN BERBASIS MIKROTIK DENGAN BAHASA	PEMROGRAMAN PYTHON
Hadi Prasetyo, Gunawan Pria Utama	130-137
IMPLEMENTASI KEAMANAN FILE BERBASIS WEB DENGAN METODE ADVANCED ENCRYPTION	STANDARD (AES)-256 COUNTER MODE
Ahmad Najib Syafi'I, Noni Juliasari	138-145
MANAJEMEN JARINGAN BEBASIS WEB MENGGUNAKAN SNMP UNTUK FAKULTAS	EKONOMI DAN BISNIS UNIVERSITAS TRISAKTI
Aris Wiyono; Reva Ragam Santika	146-154
IMPLEMENTASI AES-128 UNTUK PENGAMANAN FILE TRANSAKSI PENJUALAN PADA	CV. DNN BERBASIS WEB
Fransiskus Aldi Jebadu, Sejati Waluyo	155-163
PENERAPAN AUTENTIKASI DUA FAKTOR MENGGUNAKAN TIME-BASED ONE TIME PASSWORD (TOTP) BERBASIS EMAIL DAN GOOGLE AUTHENTICATOR	PADA APLIKASI MANAJEMEN PERANGKAT MIKROTIK
Izhar Nurkholis Sukma, Achmad Solichin	164-173

PENGAMANAN FILE BERBASIS WEB DENGAN METODE AES-128 CTR
Fribyan Yusuf, Safrina Amini.....174-182

RANCANG BANGUN ALAT PENERING APEL MENGGUNAKAN WEBSOCKET
SERVER BERBASIS IOT
Yusron Ageng Pangestu, Utomo Budiyo183-191

PENERAPAN ALGORITMA APRIORI UNTUK MENGANALISA POLA PENJUALAN
PADA CIPTA ADIDAYA – STEAK
Hendryansyah Saputra, Sri Mulyati192-200

ARTIFICIAL INTELLIGENCE

IMPLEMENTASI CONTENT MANAGEMENT SYSTEM DALAM PEMBUATAN
SISTEM PENDAFTARAN ONLINE BIMBINGAN BELAJAR EAZY
Aghri Zahra, Nawindah.....201-210

ANALISIS MARKET BASKET DENGAN ALGORITMA APRIORI UNTUK
IDENTIFIKASI POLA PEMBELIAN DI NAFIE MOTOR
Fikri Ikhsan Al Yusufi, Dewi Kusumaningsih.....211-220

ANALISIS SENTIMEN 100 HARI KERJA PRESIDEN PRABOWO SUBIANTO
MENGGUNAKAN NAIVE BAYES DAN LOGISTIC REGRESSION
Aziz Mujahiddin Nugraha, Hari Soetanto.....221-230

KOMPARASI METODE C4.5 DAN RANDOM FOREST UNTUK PENENTUAN DEPRESI
PADA PELAJAR
Elni Salini Zebua, Gandung Triyono231-240

CLUSTERING DATA MOBIL BEKAS OLX MENGGUNAKAN ALGORITME K-MEANS
DAN GAUSSIAN MIXTURE MODEL
Raynaldi Dwi Cahyono, Gandung Triyono241-250

IMPLEMENTASI METODE NAIVE BAYES DAN SVM DALAM ANALISIS SENTIMEN
MASYARAKAT INDONESIA TERKAIT FENOMENA KABUR AJA DULU PADA
MEDIA SOSIAL X
Taufiq Rahman, Sejati Waluyo251-260

ANALISIS SENTIMEN PUBLIK TERHADAP KEBIJAKAN PENGIRIMAN SISWA KE
BARAK MILITER MENGGUNAKAN SUPPORT VECTOR MACHINE
Az Zahra Rabiul Tsani; Utomo Budiyo.....261-268

IMPLEMENTASI SISTEM VERIFIKASI E-KTP BERBASIS OCR DAN CNN UNTUK ADMINISTRASI	AKADEMIK
Mohammad Zaghy Zalayetha Sofjan, Hari Soetanto	269-278
ANALISA KOMPARATIF MULTINOMIAL NAÏVE BAYES DAN MULTINOMIAL LOGISTIC REGRESSION UNTUK KLASIFIKASI HOAX MULTI-KATEGORI PADA BERITA	NASIONAL
Erza Pranata Ramadhan	279-288
IMPLEMENTASI NAIVE BAYES DAN LOGISTIC REGRESSION UNTUK DIAGNOSIS DINI	PENYAKIT JANTUNG
M Ridhoni, Gandung Triyono.....	289-298
PENERAPAN DATA MINING APRIORI UNTUK ANALISIS PREFERENSI PRODUK TOKO	RITEL
Muhammad Baldy Imalian, Anita Diana, Grace Gata, Rizky Tahara Shita	299-307
ANALISIS SENTIMEN REVIEW PENGGUNA APLIKASI BLU BCA PADA PLAY STORE MENGGUNAKAN	ALGORITMA NAÏVE BAYES
Arzellin Anggraini Zein, Dewi Kusumaningsih	308-317
PREDIKSI KELULUSAN SISWA MENGGUNAKAN METODE PRINCIPAL COMPONENT ANALYSIS DAN KLASIFIKASI LOGISTIC REGRESSION	
Orbit Rasi Rayana Jati, Mardi Hardjianto	318-327
ANALISIS SENTIMEN KOMENTAR NETIZEN TENTANG RUU TNI DI APLIKASI X MENGGUNAKAN	METODE NAÏVE BAYES
Faris Haidar, Hari Soetanto.....	328-337
ANALISIS SENTIMEN DATA ULASAN APLIKASI PLN MOBILE DI GOOGLE PLAY STORE	DENGAN METODE NAÏVE BAYES
Rafael Calvin Fardinand, Safrina Amini.....	338-345
ANALISIS SENTIMEN PUBLIK TWITTER DENGAN TF-IDF DAN SUPPORT VECTOR MACHINE	
Fildzah Putri Zhafirah Awliya, Utomo Budiyanto	346-354
KLASIFIKASI SENTIMEN KEBIJAKAN EFISIENSI ANGGARAN 2025 DI TWITTER DENGAN	MULTINOMIAL NAÏVE BAYES
Leo Nardi Halawa, Mohammad Syafrullah	355-363
ANALISIS SENTIMEN KOMENTAR YOUTUBE TENTANG PINJAMAN ONLINE MENGGUNAKAN	SUPPORT VECTOR MACHINE
Zea Gratia Ismael, Imelda Imelda.....	364-372

ANALISIS SENTIMEN TRANSFORMASI DIGITAL BERBASIS AI DI MEDIA SOSIAL X DENGAN NAIVE BAYES Rizsyad Abiyandra Riadi, Yuliazmi	373-380
IMPLEMENTASI METODE APRIORI BERBASIS WEB UNTUK ANALISIS TRANSAKSI PENJUALAN DI PT. RODA MEDIKA MULYA Muhammad Zulfa, Arief Wibowo	381-388
PERBANDINGAN NAÏVE BAYES CLASSIFIER DAN SUPPORT VECTOR MACHINE PADA ANALISIS SENTIMEN NETIZEN X #KABURAJADULU Kharis Amazio, Windarto	389-397
KLASIFIKASI SENTIMEN PUBLIK TERHADAP PROGRAM MAKAN SIANG GRATIS DI MEDIA SOSIAL X DENGAN ALGORITMA KNN Qoriatul Adawiyah, Gunawan Pria Utama	398-407
ANALISIS SENTIMEN TWITTER TERHADAP KEBIJAKAN ANAK MASUK BARAK MILITER DENGAN NAÏVE BAYES Febryan Dwi Prastyo, Sri Mulyati	408-415
KLASTERISASI INTERAKSI KOMUNITAS BOOKTOK PADA MEDIA SOSIAL TIKTOK MENGUNAKAN ALGORITMA K-MEANS Annisa Camelia Syarif, Achmad Solichin	416-423
ANALISIS SENTIMEN PUBLIK TERHADAP PROGRAM BANTUAN SUBSIDI UPAH (BSU) DI TWITTER MENGGUNAKAN ALGORITMA SVM Rohmat Nur Muhamad, Utomo Budiyanto	424-431
ANALISIS PREDIKTIF RISIKO PENYAKIT JANTUNG DENGAN REGRESI LOGISTIK DAN K-NEAREST NEIGHBOR Fakhri Alifio, Prof. Ir. Wendi Usino, MM., M.Sc., Ph.D	432-440
ANALISIS SENTIMEN PADA X TERHADAP DEDI MULYADI DENGAN NAÏVE BAYES DAN SUPPORT VECTOR MACHINE Ichsanul Yazid Azhari, Mufti	441-448
PENERAPAN ALGORITMA NAÏVE BAYES UNTUK KLASIFIKASI BUKU POPULER BERBASIS WEB Rizki Akbar, Titin Fatimah	449-458
ANALISIS POLA PEMBELIAN KONSUMEN MENGGUNAKAN ALGORITMA APRIORI PADA COFFEE SHOP SS Muhamad Jordi Riawan, Joko Christian Chandra	459-467

IMPLEMENTASI DATA MINING UNTUK ANALISIS POLA PENJUALAN OBAT MENGUNAKAN ALGORITMA APRIORI	468-477
Deny Riyanto, Pipin Farida Ariyani.....	
PENERAPAN ALGORITMA NAIVE BAYES UNTUK ANALISIS SENTIMEN OPINI MASYARAKAT PADA DATA TWITTER	478-485
Al Hajju Arafah, Rizky Pradana	
IMPLEMENTASI DATA MINING BERBASIS WEBSITE MENGGUNAKAN ALGORITMA FP-GROWTH TERHADAP MARKET BASKET ANALYSIS PENJUALAN FASHION	486-494
Ghina Nabila Febrianti, Mardi Hardjianto.....	
PENERAPAN ALGORITMA RANDOM FOREST UNTUK MENDETEKSI SERANGAN SIBER	495-502
Fadhilla Muhammad, Safrina Amini	
KLASTERISASI KELOMPOK APT BERDASARKAN TEKNIK SERANGAN PADA MITRE ATT&CK FRAMEWORK MENGGUNAKAN ALGORITMA HIERARCHICAL AGGLOMERATIVE DAN K-MODES	503-512
Muchamad Angga Dwi Wahyu, Dian Anubhakti, Hendi Setiawan	
ANALISIS SENTIMEN KOMENTAR YOUTUBE TERHADAP ISU BISNIS GELAP DOKTER DAN PERUSAHAAN FARMASI MENGGUNAKAN ALGORITMA NAÏVE BAYES	513-522
Septian Farriz Hartono, Achmad Solichin, noni juliasari, purwanto purwanto ...	
KLASIFIKASI SENTIMEN NETIZEN TERHADAP PATRICK KLUIVERT DI PLATFORM X DENGAN METODE NAÏVE BAYES	523-530
Alif Al Fadhilla; Wahyu Pramusinto, Hadidtyo Wardani	
ANALISIS SENTIMEN PENGGUNA APLIKASI OLXMOBBI PADA SOSIAL MEDIA X MENGGUNAKAN ALGORITMA SUPPORT VECTOR MACHINE	531-538
Maesheilla Noordjaianti Diva Utama, Arief Wibowo.....	
PENERAPAN ALGORITMA APRIORI UNTUK REKOMENDASI PENATAAN OBAT DI APOTEK	539-546
Burhanul Arifin, Painem	
ANALISIS SENTIMEN KUALITAS PELAYANAN MIKROTRANS JAKLINGKO DENGAN ALGORITMA NAÏVE BAYES CLASSIFIER	547-555
Indira Arifin, Noni juliasari	

PROGRAMMING

SISTEM DETEKSI KEBAKARAN MENGGUNAKAN SENSOR FLAME DAN MQ-2 DENGAN METODE FUZZY MAMDANI PADA PAUD PELANGI NUSANTARA
Rizqa Pandu Maulana, Dewi Kusumaningsih.....556-565

SISTEM MONITORING DAN KEAMANAN DI RUANGAN SERVER MENGGUNAKAN KOMUNIKASI LORA BERBASIS INTERNET OF THINGS
Alfa Kautsar.....566-575

RANCANG BANGUN SISTEM SORTIR BARANG MENGGUNAKAN QR CODE BERBASIS ARDUINO MEGA
Muhammad Daffa, Irawan.....576-584

IMPLEMENTASI WEB SERVICE API PADA PEMESANAN PAKET MEMBER DI STILLFIT GYM DENGAN MENGGUNAKAN ALGORITMA JWT (JSON WEB TOKEN)
Mohammed Zaki Abira Kurniawan, Sejati Waluyo.....585-593

IMPLEMENTASI FINITE STATE MACHINE DAN FUZZY LOGIC DALAM GAME 2D UNTUK PENGUATAN LITERASI DIGITAL HOAKS
Deni Rizki Armando, Wahyu Pramusinto.....594-602

DESAIN ROBOT PEMILAH SAMPAH LINGKARAN MENGGUNAKAN VISI KOMPUTER DENGAN KENDALI PID
Rikza Khamami, Yani Prabowo, Jan Everhard Riwurohi, Irawan.....603-612

IMPLEMENTASI SISTEM CERDAS UNTUK MENDETEKSI KEBOCORAN GAS DAN KELEMBAPAN UDARA MENGGUNAKAN FUZZY LOGIC
Andrew Bayu Permana, Rizky Pradana.....613-622

SISTEM KEAMANAN PINTU DENGAN 2 LANGKAH AUTENTIKASI BERBASIS IOT
Ragil Prabawijaya, Jan Everhard Riwurohi, Irawan, Yani Prabowo623-631

PERBANDINGAN NAIVE BAYES DAN KNN UNTUK SENTIMEN KESADARAN LINGKUNGAN DI KONTEN PANDAWARA GROUP.
Gina Putri Rezi, imelda imelda.....632-640

IMPLEMENTASI METODE FINITE STATE MACHINE PADA GAME CINDUA MATO SEBAGAI MEDIA PEMBELAJARAN BUDAYA MINANGKABAU
Auliatul Wahyudi, Safrina Amini.....641-650

IMPLEMENTASI ALGORITMA A-STAR PADA PERMAINAN TIMUN MAS DAN RAKSASA
Muhammad Rendy, Windarto.....651-660

PROTOTIPE SISTEM PENDETEKSI BANJIR BERBASIS IOT TERINTEGRASI APLIKASI ANDROID Akbar Nur Wahyudin, Ferdiansyah; Ika Susanti.....	661-670
IMPLEMENTASI SISTEM PRESENSI MENGGUNAKAN PENGENALAN WAJAH (FACE RECOGNITION) PADA SMA ISLAM AL – LAYYINAH Ubaidillah Kamal Syauqi; Purwanto	671-680
SISTEM KONTROL LAMPU LALU LINTAS MENGGUNAKAN DEEP LEARNING PENGENALAN KENDARAAN Yoga Aprio Pratama, Rizky Pradana	681-690
IMPLEMENTASI ALGORITMA FISHER-YATES SHUFFLE PADA GAME JELAJAH RASA NUSANTARA BERBASIS WEB Fransiscus Wahyu Adi Saputro, Dolly Virgian Shaka Yudha Sakti.....	691-700
RANCANG BANGUN SISTEM MONITORING SUHU, KELEMBAPAN, DAN GAS PADA RUANG SERVER BERBASIS NODE MCU ESP8266 Riko Pratama, Sri Mulyati	701-709
SISTEM MONITORING SUHU, KELEMBAPAN DAN KEBAKARAN RAK SERVER BERBASIS IOT PADA ZENIT TECHNOLOGIES Akmal Yusuf Nursyahfikri, Mufti	710-719
IMPLEMENTASI ALGORITMA APRIORI UNTUK MENENTUKAN POLA LAYANAN PERBAIKAN PADA BENGKEL KARYA MOTOR Vincent Gunawan, Gunawan Pria Utama	720-728
ANALISIS SENTIMEN KOMENTAR PLATFORM X MENGENAI EKSPLOITASI RAJA AMPAT MENGGUNAKAN ALGORITMA SUPPORT VECTOR MACHINE Ahmad Arga, Gunawan Pria Utama	729-736
PREDIKSI LAGU TERPOPULER MENGGUNAKAN ALGORITMA GAUSSIAN NAÏVE BAYES BERBASIS WEB Azfa Widiyanto, Titin Fatimah	737-744
PENERAPAN SISTEM VALIDASI TANDA TANGAN DIGITAL DENGAN FUNGSI HASH MD5 PADA FAKULTAS TEKNOLOGI INFORMASI UNIVERSITAS BUDI LUHUR Erlangga, Achmad Solichin.....	755-764
IMPLEMENTASI SISTEM DETEKSI KEBAKARAN KANTIN BERBASIS ESP32 DENGAN TELEGRAM Calista Marshanda Putri, Windarto.....	765-773

PENERAPAN SISTEM ABSENSI KARYAWAN MENGGUNAKAN RFID DAN ESP32
CAM PADA CV. BERKAT ABADI
Denny Sugianto, Indra.....774-783

SISTEM MONITORING BANJIR MENGGUNAKAN SENSOR ULTRASONIK DAN
WATER LEVER SENSOR DENGAN NOTIFIKASI PESAN
Alberto Hasiholan, Indra.....784-792

IMPLEMENTASI WEB SERVICE RESTFUL API DENGAN KEAMANAN JWT UNTUK
DISTRIBUSI BAHAN BANGUNAN PT SUMBER BAROKAH
Faza Ghani Marcellino, Dolly Virgian Shaka Yudha Sakti.....793-800

INFORMATION SYSTEM

SISTEM PENUNJANG KEPUTUSAN PROFILE MATCHING UNTUK SELEKSI
KARYAWAN CAPTURE IT PHOTOBOOTH
Arya Kedaton, Dian Anubhakti, Retno Wulandari.....801-810

SISTEM INFORMASI PENJUALAN ONLINE MENGGUNAKAN CMS WORDPRESS
PADA NUNI COOKIEZ
Phuja Mahesa, Refaldy Hilmy Akram, Devit Setiono811-820

PERANCANGAN E-CRM BERBASIS WEB UNTUK DIGITALISASI DATA
PELANGGAN DAN LAYANAN PADA BENGKEL ADI MOTOR
Kresna Pangestu, Goenawan Brotosaputro.....821-829

PENERAPAN E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM (CMS)
WORDPRESS PADA TOKO SABLON UTSMAN ATHAR
Abi Salihin, Grace Gata.....830-839

IMPLEMENTASI PLATFORM E-COMMERCE MENGGUNAKAN WORDPRESS
UNTUK OPTIMALISASI PROMOSI DAN PENJUALAN TOKO TASARAH CLOTHING
Dwi Hardiansyah, Grace Gata.....840-849

PENERAPAN E-COMMERCE MENGGUNAKAN CONTENT MANAGEMENT SYSTEM
(CMS) PADA BARASA MOTOR UNTUK MENINGKATKAN PENJUALAN SPAREPART
Junica Kristin Ompusunggu, Lestari Margatama.....850-859

PENGEMBANGAN SISTEM E-CRM BERBASIS WEB METODE WATERFALL UNTUK
MENINGKATKAN KEPUASAN DAN LOYALITAS PELANGGAN
Rendy Lorenzo, Lauw Li Hin.....860-868

SISTEM PENUNJANG KEPUTUSAN PEMILIHAN PEGAWAI NON-ASN TERBAIK MENGGUNAKAN METODE SAW PADA KECAMATAN PONDOK AREN Muhammad Daifullah, Dian Anubhakti	869-878
IMPLEMENTASI CRM SEBAGAI STRATEGI PENINGKATAN LOYALITAS DAN PELAYANAN KONSUMEN PADA KINCLONG LAGI DENGAN WATERFALL Muhammad Syachru Rizky, Hendri Irawan	879-886
IMPLEMENTASI E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM (CMS) PADA TOKO SANDRINA COLLECTION UNTUK MENINGKATKAN PENJUALAN Anisa Dwi Utami, Lestari Margatama	887-896
PENERAPAN E-CRM BERBASIS WEB DENGAN METODE WATERFALL DI HAREFA LAUNDRY Muhammad Rizki Marten, Goenawan Brotosaputro	897-906
SISTEM PENUNJANG KEPUTUSAN STANDARISASI PEMILIHAN KARYAWAN TERBAIK DENGAN SAW PADA CV SINERGI PRIMA MAGNA Haekal Rida Putra, Dian Anubhakti	907-916
PENERAPAN SISTEM E-CRM BERBASIS WEB UNTUK MENINGKATKAN LAYANAN INFORMASI DI SDI AL MUHAJIRIN Muhammad Hilmi Athallah, Ita Novita	917-926
IMPLEMENTASI CONTENT MANAGEMENT SYSTEM (CMS) UNTUK MEMBANGUN MODEL E-COMMERCE PADA TOKO BAJU BASIC JAKARTA Tirto Utomo, Bima Cahya Putra	927-936
IMPLEMENTASI E-COMMERCE MENGGUNAKAN CONTENT MANAGEMENT SYSTEM (CMS) BERBASIS WORDPRESS PADA TOKO DAMAR BETTA Reyza Adriansyah, Grace Gata	937-946
IMPLEMENTASI E-COMMERCE BERBASIS CMS SEBAGAI MEDIA PROMOSI DAN MEMPERLUAS PEMASARAN PADA TOKO BILUES CRYSTAL Farhan Firdaus An Nazih, Joko Sutrisno	947-956
IMPLEMENTASI E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM (CMS) PADA TOKO MERCHANDISE HUMAN\$ UNTUK MENINGKATKAN PENJUALAN Danni Alief, Yudi Santoso	957-966
IMPLEMENTASI E-COMMERCE BERBASIS (CMS) UNTUK OPTIMALISASI PROMOSI DAN PEMASARAN PADA CAHAYA FRAME & MIRROR Muhamad Luthfan Ilyasa, Joko Sutrisno	967-976

IMPLEMENTASI CONTENT MANAGEMENT SYSTEM PADA E-COMMERCE SEBAGAI STRATEGI PEMASARAN DI TOKO BANGUNAN HARAPAN 1 Ahmad Damanhuri, Bima Cahya Putra	977-986
IMPLEMENTASI E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM WORDPRESS PADA PRODUSEN BATIK JARI KASIM Irgie Davariansyah, Lauw Li Hin.....	987-996
ANALISA DAN PERANCANGAN WEBSITE E-COMMERCE MENGGUNAKAN PYTHON PADA TOKO LOKAL PETSHOP Rizky Hasyim Nugraha, Bima Cahya Putra.....	997-1006
RANCANGAN E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM (CMS) PADA PRODUK RED SWAN PLAST Bilal Satya Ramadhan, Bruri Trya Sartana, Ririt Ririt Roeswidiah.....	1007-1016
ANALISIS DAN DESAIN WEBSITE E-COMMERCE PADA TOKO ANEKA BARU MENGGUNAKAN CONTENT MANAGEMENT SYSTEM (CMS) Raihan Nur Kharisman, Ita Novita	1017-1026
ANALISIS DAN PERANCANGAN SISTEM E-COMMERCE BERBASIS CMS WORDPRESS UNTUK MENINGKATKAN PEMASARAN PRODUK SORA INDONESIA Alreza Aziz Ainun Nadjib, Joko Sutrisno.....	1027-1035
PENERAPAN ELECTRONIC CUSTOMER RELATIONSHIP MANAGEMENT (E-CRM) PADA PARI SAKTI TRIATHLON CLUB UNTUK MENINGKATKAN PELAYANAN Ahmad Aslam Ramadhan, Humisar Hasugian	1036-1045
RANCANG BANGUN WEB E-COMMERCE UNTUK MENINGKATKAN PENJUALAN TOKO MY GOLDEN STAR MENGGUNAKAN FRAMEWORK LARAVEL Hilmy Lazuardi, Yudi Santoso.....	1046-1055
IMPLEMENTASI E-COMMERCE BERBASIS CONTENT MAGNAGEMENT SYSTEM (CMS) UNTUK MENINGKATKAN PENJUALAN BUKET TOKO VANTSA SHOP Senli Visela, Hendri Irawan; Nawindah, Agus Umar Hamdani.....	1056-1065
PENERAPAN E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM UNTUK MEMPERLUAS JANGKAUAN PEMASARAN PADA TOKO NUR COLLECTION Ahmad Tarmizi, Agnes Aryasanti	1066-1075
IMPLEMENTASI E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM (CMS) UNTUK MENINGKATKAN PENDAPATAN PADA TOKO C.S.ELECTRONIC Sherin Halim; Agus Hamdani	1076-1085

PENERAPAN DATA MINING PADA TOKO BUKU MENGGUNAKAN ALGORITMA APRIORI DALAM STRATEGI PENJUALAN BUNDLING PRODUK Dodi Prayoga, Joko Sutrisno	1086-1095
IMPLEMENTASI E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM UNTUK MENINGKATKAN PENJUALAN PADA MATAHARI FRAME Rangga Abdi Maulana, Grace Gata	1096-1105
PENERAPAN WEBSITE E-COMMERCE MENGGUNAKAN CONTENT MANAGEMENT SYSTEM (CMS) PADA TOKO FAIRY LOOK COLLECTION Kevin Endra Pratama, Humisar Hasugian	1106-1114
IMPLEMENTASI WEBSITE E-COMMERCE PADA PENJUALAN TOKO KURIMAS JAYA AQUARIUM MENGGUNAKAN CONTENT MANAGEMENT SYSTEM (CMS) Muhammad Nadhif Fadhal Kautsar, Ita Novita	1115-1124
PENERAPAN E-COMMERCE MENGGUNAKAN WORDPRESS UNTUK MENINGKATKAN DAYA SAING DAN EFISIENSI PENJUALAN PADA CAHAYA ABADI Yulita Maharani, Agnes Aryasanti	1125-1134
IMPLEMENTASI WEBSITE E-COMMERCE BERBASIS WORDPRESS UNTUK MEMPERLUAS JANGKAUAN PELANGGAN PADA HAFIZH SPORT Luthfia Maharani, Agnes Aryasanti	1135-1144
PENGELOMPOKAN JENIS SAMPAH MENGGUNAKAN ALGORITMA K-MEANS PADA BANK SAMPAH BUNGA RAYA Rizky Ramadhan, Anita Diana, yudi wiharto	1145-1152
PENERAPAN ALGORITMA K-MEANS UNTUK PENGELOMPOKAN KEKERASAN TERHADAP ANAK LAKI-LAKI DI PROVINSI JAWA BARAT Rehan Ramdani, Yudi Santoso	1153-1161
PENERAPAN METODE K-MEANS CLUSTERING UNTUK PENGELOMPOKAN RISIKO PASIEN PENYAKIT GINJAL KRONIK M Bintang Akram; Yudi Santoso	1162-1170
PENGEMBANGAN WEB CRM UNTUK RETENSI PELANGGAN PADA ALLE LAUNDRY PALAPA DENGAN SDLC Aferil Yudhatama, Lestari Margatama	1171-1179
SISTEM PENUNJANG KEPUTUSAN KELAYAKAN KREDIT BERBASIS SIMPLE ADDITIVE WEIGHING (SAW) PADA KOPERASI JASA PRATAMA Awaludin Novianto; Yudi Santoso; Nurwati	1180-1189

PENERAPAN METODE SAW UNTUK MENDUKUNG KEPUTUSAN PENERIMAAN KARYAWAN HOST LIVE PADA CV.DUNIA MAS COMPUTER Salma Hayati, Anita Diana	1190-1199
PENERAPAN E-BUSINESS PENYEWAAN MOBIL PADA BSU RENT CARS Fahri Ansyah, Dian Anubhakti, Retno Wulandari	1200-1207
PERANCANGAN WEBSITE E-COMMERCE MENGGUNAKAN CONTENT MANAGEMENT SYSTEM PADA TOKO ARSYAM FASHION STORE UNTUK MENINGKATKAN PENJUALAN Tegar Cahyo Erianto, Humisar Hasugian	1208-1217
PERANCANGAN SISTEM RESERVASI DAN PEMESANAN BERBASIS WEB PADA COFFEE SHOP ALLEY.JKT DENGAN INTEGRASI PAYMENT GATEWAY Virgi Aditya Putra, Yudi Santoso, Nurwati	1218-1227
PERANCANGAN E-COMMERCE PAKAIAN MUSLIM BERBASIS CONTENT MANAGEMENT SYSTEM WORDPRESS PADA TOKO AL-VIATHOR Novia Paraswati, Bruri Trya Sartana	1228-1237
IMPLEMENTASI WEBSITE E-COMMERCE BERBASIS CMS MENGGUNAKAN WORDPRESS: STUDI KASUS PADA TOKO KIRANASANI Fiqi Alvarizi Fahmi, Lauw Li Hin	1238-1247
PERANCANGAN E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM UNTUK MENINGKATKAN PENJUALAN PADA TOKO BOUQUET BY DITHA Wasilah Ulul Azmi, Atik Ariesta	1248-1257
PENERAPAN E-COMMERCE PENJUALAN KUKU PALSU BERBASIS CONTENT MANAGEMENT SYSTEM (CMS) UNTUK MENINGKATKAN PENJUALAN Ezza Putri, Lestari Margatama	1258-1267
IMPLEMENTASI PENUNJANG KEPUTUSAN LOKASI STRATEGIS ARTOLOUIS BERBASIS ANALYTICAL HIERARCHY PROCESS Amanda Aura Putri, Lis Suryadi	1268-1275
PERANCANGAN E-COMMERCE DENGAN CONTENT MANAGEMENT SYSTEM UNTUK MENDUKUNG PENJUALAN PRODUK TOKO MELT A DESSERT Renaldi Rachman, Agus Umar Hamdani	1276-1285
SISTEM PENUNJANG KEPUTUSAN PENILAIAN KINERJA KARYAWAN BERBASIS SAW: STUDI KASUS DI YAYASAN AS-SALAM JOGLO Rangga Prakoso, Dian Anubhakti	1286-1293

PERANCANGAN WEBSITE E-COMMERCE MENGGUNAKAN WORDPRESS PADA TOKO BUDHE SNACK Faqih Khaikal Al Amin, Ita Novita	1294-1302
CLUSTERING DAFTAR SAHAM BERDASARKAN LIKUIDITAS DAN KAPITALISASI PASAR MENGUNAKAN ALGORITMA GMM DAN BGM ANGEL Patrecia, Dian Anubhakti, Kukuh Harsanto.....	1303-1310
IMPLEMENTASI CONTENT MANAGEMENT SYSTEM PADA E-COMMERCE TOKO BERKAH JAYA Farrel Andhika Sulton, Yudi Santoso, Nurwati, Muhammad Anif	1311-1320
PENERAPAN CMS WORDPRESS PADA TOKO YOVIS SPORT DALAM MENINGKATKAN PENJUALAN ONLINE Fadlan Ramdhani, Humisar Hasugian.....	1321-1329
PERANCANGAN SISTEM E-COMMERCE LAYANAN PERCETAKAN BERBASIS ODOO MENGGUNAKAN METODE SDLC PADA PT XEROGRAPHY INDONESIA Muhammad Ridhowan Annas, Lis Suryadi, Grace Gata, Lauw Li Hin.....	1330-1339
PENERAPAN SISTEM PENUNJANG KEPUTUSAN UNTUK PEMILIHAN SUPPLIER AYAM PADA AYAM BAKAR JOGLO CAK MOYO MENGGUNAKAN METODE SIMPLE ADDITIVE WEIGHTING Rifai Abdul Azis, Humisar Hasugian	1340-1347
RANCANGAN SISTEM E-COMMERCE PADA TOKO BATIK TRIWARNI UNTUK MEMPERLUAS JANGKAUAN PASAR Rafi Ichsan Madani, Lis Suryadi.....	1348-1357
ANALISIS DAN PERANCANGAN WEB E-COMMERCE MENGGUNAKAN CONTENT MANAGEMENT SYSTEM WORDPRESS PADA TOKO SINAR BERLIAN Farrel Yusuf, Ita Novita.....	1358-1367
IMPLEMENTASI E-COMMERCE MENGGUNAKAN CMS WORDPRESS UNTUK MENGOPTIMALKAN PENJUALAN DI TOKO LEGOSO PARFUM Ahmad Rizky Utomo, Agnes Aryasanti	1368-1376
IMPLEMENTASI E-COMMERCE UNTUK MENDUKUNG PENJUALAN PADA TOKO ZAFANKA MENGGUNAKAN CMS (CONTENT MANAGEMENT SYSTEM) WORDPRESS Siti Ayu Nurzanah, Bima Cahya Putra, Hari Prapcoyo.....	1377-1385
RANCANGAN SISTEM PEMESANAN PAKAIAN BERBASIS WOOCOMMERCE PADA RUMAH JAHIT QUEENNARA Dhoni Khairi, Wiwin Windihastuty	1386-1395

IMPLEMENTASI SISTEM PENJUALAN ONLINE BERBASIS CMS PADA TOKO BUTIK NAOMI

Salsabila Vasya, Bima Cahya Putra, Novita Mariana 1396-1405

SISTEM PENDUKUNG KEPUTUSAN PENILAIAN KARYAWAN TERBAIK PADA PT. DIGIVO KREATIF INDONESIA MENGGUNAKAN PROFILE MATCHING

Afnan Firdaus Febriansyah, Atik Ariesta..... 1406-1415

IMPLEMENTASI E-COMMERCE MENGGUNAKAN PLATFORM CONTENT MANAGEMENT SYSTEM (CMS) UNTUK MENINGKATKAN PENJUALAN PADA PT OLAIF

Histori Buulolo, Agus Umar Hamdani..... 1416-1425

SISTEM PENENTUAN SKEMA PENAWARAN PROYEK IT YANG OPTIMAL BERBASIS AHP DAN WP

Marsha Nurtya Rachma, Bima Cahya Putra, Mujito 1426-1435

SISTEM PENUNJANG KEPUTUSAN PEMILIHAN SUPPLIER DENGAN METODE ANALYTICAL HIERARCHY PROCESS DAN SIMPLE ADDITIVE WEIGHTING

Andry, samsinar 1436-1445

MEMBANGUN E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM (CMS) WORDPRESS PADA TOKO KARYA DARA UNTUK MEMPERLUAS JANGKAUAN PASAR

Lilis Sri Lestari, Bima Cahya Putra 1446-1455

STRATEGI PENERAPAN CRM BERBASIS WEB PADA SISTEM RESERVASI SERVICE KENDARAAN DIBENKEL MOTOR GONGGO

Muhamad Alfian Sandhikara, Lestari Margatama 1456-1465

PERANCANGAN DAN IMPLEMENTASI SISTEM E-COMMERCE PADA TOKO SAKINAH UNTUK PENJUALAN PRODUK FASHION BERBASIS WEB

Meriani Wulandari, Lis Suryadi..... 1466-1474

PERANCANGAN, IMPLEMENTASI WEBSITE E-COMMERCE PT MAP DENGAN ANALISIS BMC DAN FISHBONE DIAGRAM BERBASIS WORDPRESS

Muhammad Farhan Akbar, Lis Suryadi 1475-1483

PENERAPAN E-COMMERCE BERBASIS CONTENT MANAGEMENT SYSTEM (CMS) PADA TOKO SRC DIDI

Ghafira Ramdhania Putri Hami, Muhammad Ainur Rony 1484-1493

IMPLEMENTASI *HYBRID ENCRYPTION* ECC-AES UNTUK PENGAMANAN KOMUNIKASI DAN BERBAGI FILE BERBASIS WEB

Risqi Rahman Pratama^{1*}, Dolly Virgianshaka Yudha Sakti²

^{1,2} Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: ^{1*}2111510596@student.budiluhur.ac.id, ²dolly.virgianshaka@budiluhur.ac.id

(* : corresponding author)

Abstrak—Perkembangan komunikasi digital menuntut mekanisme pengamanan yang efektif untuk pesan dan pertukaran *file*, terutama pada aplikasi web. Penelitian ini bertujuan mengimplementasikan skema *hybrid encryption* berbasis *Advanced Encryption Standard* (AES) 256-bit dalam mode *Galois/Counter Mode* (GCM) dan *Elliptic Curve Cryptography* (ECC) X25519 untuk menjamin kerahasiaan serta integritas data. Metode penelitian mencakup penerapan kombinasi algoritma tersebut, validasi fungsi enkripsi dan dekripsi menggunakan *test vector* standar internasional, serta uji coba pada modul *chatting* dan berbagi *file* berukuran 4–41 MB. Hasil validasi menunjukkan bahwa algoritma AES-256-GCM menghasilkan data terenkripsi sesuai spesifikasi, sementara ECC X25519 mampu mendistribusikan kunci dengan aman dan efisien. Uji performa sistem memperlihatkan bahwa pesan teks dapat dienkripsi dan didekripsi secara *real-time* dengan latensi rata-rata sekitar 45 milidetik, sedangkan *file* berukuran menengah hingga besar berhasil dienkripsi dengan durasi 38–332 detik, dan proses dekripsi tetap reliabel melalui mekanisme pemrosesan *file* per bagian (*chunking*) meskipun terbatas oleh waktu eksekusi *server*. Integritas data terjaga, karena setiap perubahan pada *ciphertext* terdeteksi melalui mekanisme autentikasi. Kesimpulannya, implementasi *hybrid* AES-256-GCM dan ECC X25519 berhasil diterapkan pada aplikasi web nyata, menyediakan pengamanan yang efektif untuk komunikasi pesan dan pertukaran *file*, serta relevan untuk diterapkan pada sistem *real-time*. Penelitian ini juga memberikan kontribusi praktis sebagai bukti bahwa *hybrid encryption* dapat langsung digunakan pada aplikasi berbasis web, sementara optimalisasi performa untuk *file* berukuran sangat besar dan pengujian *multi-user* menjadi arah pengembangan selanjutnya.

Kata Kunci: Hybrid encryption, AES-256-GCM, ECC X25519, keamanan komunikasi, enkripsi file.

IMPLEMENTATION OF ECC-AES HYBRID ENCRYPTION FOR SECURING WEB-BASED COMMUNICATION AND FILE SHARING

Abstract—The advancement of digital communication demands effective security mechanisms for messages and file exchanges, particularly in web-based applications. This study aims to implement a hybrid encryption scheme combining *Advanced Encryption Standard* (AES) 256-bit in *Galois/Counter Mode* (GCM) and *Elliptic Curve Cryptography* (ECC) X25519 to ensure data confidentiality and integrity. The research method involves applying this algorithm combination, validating encryption and decryption functions using international standard test vectors, and testing on web-based chat modules and file-sharing systems with file sizes ranging from 4 to 41 MB. Validation results indicate that AES-256-GCM produces encrypted data according to specifications, while ECC X25519 securely and efficiently handles key distribution. Performance tests show that text messages can be encrypted and decrypted in *real-time* with an average latency of approximately 45 milliseconds, whereas medium to large files are successfully encrypted within 38–332 seconds. Decryption remains reliable through chunked file processing, despite server execution time limitations. Data integrity is maintained, as any modifications to ciphertext are detected via the authentication mechanism. In conclusion, the hybrid AES-256-GCM and ECC X25519 implementation is successfully applied in a real web application, providing effective security for message communication and file sharing, and is suitable for *real-time* systems. This study also offers practical evidence that hybrid encryption can be directly deployed in web applications, while further optimization for very large files and *multi-user* scenarios remains a direction for future development.

Keywords: Hybrid encryption, AES-256-GCM, ECC X25519, secure communication, file encryption.

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah memudahkan komunikasi digital dan pertukaran data secara *real-time*. Aplikasi *chatting* dan berbagi *file* menjadi salah satu sarana utama dalam menunjang kolaborasi, baik di sektor profesional maupun personal. Namun, kemudahan ini membawa konsekuensi serius terhadap aspek keamanan informasi. Risiko seperti penyadapan, manipulasi pesan, dan pencurian *file* sensitif semakin meningkat, terutama jika komunikasi dilakukan tanpa mekanisme enkripsi yang memadai [1], [2].

Salah satu pendekatan yang banyak digunakan untuk mengatasi permasalahan ini adalah penerapan kriptografi modern. Algoritma *Advanced Encryption Standard* (AES) dalam mode *Galois/Counter Mode* (GCM)

dengan panjang kunci 256 bit banyak diadopsi karena mampu memberikan kecepatan enkripsi sekaligus memastikan autentikasi data melalui *authentication tag* [3], [4]. Sedangkan *Elliptic Curve Cryptography* (ECC) menjadi pilihan populer untuk kriptografi asimetris karena tingkat keamanan tinggi dengan ukuran kunci yang relatif kecil. Varian *Curve25519* dengan algoritma pertukaran kunci X25519 direkomendasikan oleh standar internasional [5] dan telah terbukti efisien pada sistem berbasis web maupun perangkat *Internet of Things* [6].

Sebagian penelitian terdahulu hanya menggunakan algoritma tunggal, seperti AES untuk pengamanan data medis [4] atau ECC untuk sistem berbasis web [7]. Ada pula yang mengusulkan kombinasi hybrid AES–ECC [8], [9] tetapi masih terbatas pada simulasi atau diarahkan ke konteks lain seperti penyimpanan awan (*cloud storage*). Belum ditemukan penelitian yang secara khusus menerapkan *hybrid encryption* AES-256-GCM dan ECC X25519 pada aplikasi *chatting* dan berbagi *file* berbasis web secara nyata.

Tujuan penelitian ini adalah mengimplementasikan *hybrid encryption* berbasis AES-256-GCM dan ECC X25519 pada aplikasi komunikasi berbasis web, memvalidasi kebenaran implementasi algoritma menggunakan *test vector* resmi (RFC 7748 Section 6.1 untuk ECC X25519 [10] dan NIST SP 800-38D Test Case 14 untuk AES-256-GCM [11]), serta menilai efektivitas penerapannya dalam skenario komunikasi *real-time* dan berbagi *file*.

2. METODE PENELITIAN

Penelitian ini termasuk kategori penelitian terapan, karena berfokus pada penerapan algoritma kriptografi modern dalam sebuah sistem komunikasi berbasis web. Model enkripsi yang digunakan adalah *hybrid encryption*, yaitu kombinasi antara algoritma simetris AES-256-GCM dan algoritma asimetris ECC X25519.

2.1 Hybrid Encryption

Model enkripsi yang digunakan dalam penelitian ini adalah *hybrid encryption*, yaitu penggabungan algoritma simetris AES-256-GCM dengan algoritma asimetris ECC X25519.

AES-256-GCM merupakan algoritma simetris berbasis blok cipher dengan panjang kunci 256 bit. Mode GCM (*Galois/Counter Mode*) bekerja menggunakan counter untuk proses enkripsi dan dekripsi. Mekanisme ini membuat proses enkripsi dan dekripsi berjalan dengan cara yang mirip, hanya berbeda pada input yang digunakan: enkripsi dilakukan dengan plaintext sebagai masukan, sedangkan dekripsi menggunakan *ciphertext*. Selain menghasilkan *ciphertext*, GCM juga memproduksi *authentication tag* yang berfungsi sebagai verifikasi integritas data [4].

Sementara itu, ECC X25519 digunakan untuk pertukaran kunci. Algoritma ini beroperasi melalui proses *clamping* pada kunci privat untuk memastikan nilai yang valid, lalu dilanjutkan dengan *scalar multiplication* terhadap kunci publik lawan. Hasilnya adalah *shared secret* yang identik di kedua pihak, yang kemudian dimanfaatkan untuk mengamankan kunci AES [7], [12].

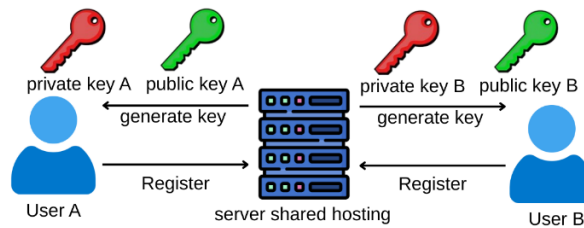
Dengan pendekatan ini, data pesan maupun *file* diamankan oleh AES-256-GCM, sementara distribusi kunci AES dilindungi melalui mekanisme ECC X25519. Skema kombinasi ini memungkinkan sistem berfungsi secara efisien sekaligus memberikan jaminan keamanan sesuai praktik terbaik kriptografi modern [8], [9].

2.2 Tahapan Implementasi

Implementasi *hybrid encryption* pada penelitian ini dilakukan melalui beberapa tahapan berurutan, mulai dari pembangkitan kunci, pembentukan *shared secret*, hingga proses enkripsi dan dekripsi pesan maupun *file*. Tahapan tersebut dijelaskan secara rinci berikut ini:

a. Inisialisasi Kunci ECC

Pada tahap registrasi, setiap pengguna menghasilkan pasangan kunci privat dan publik menggunakan algoritma X25519. Proses dimulai dengan pembangkitan nilai acak sepanjang 32 byte, kemudian dilakukan proses *clamping* agar sesuai dengan spesifikasi keamanan X25519 menurut RFC 7748 [10]. Hasil *clamping* menjadi kunci privat, sedangkan kunci publik diperoleh melalui operasi *scalar multiplication* antara kunci privat dengan titik dasar (*base point*) kurva elliptic ($u = 9$ pada *Curve25519*). Alur proses pembangkitan dan penyimpanan kunci ini ditunjukkan pada Gambar 1.



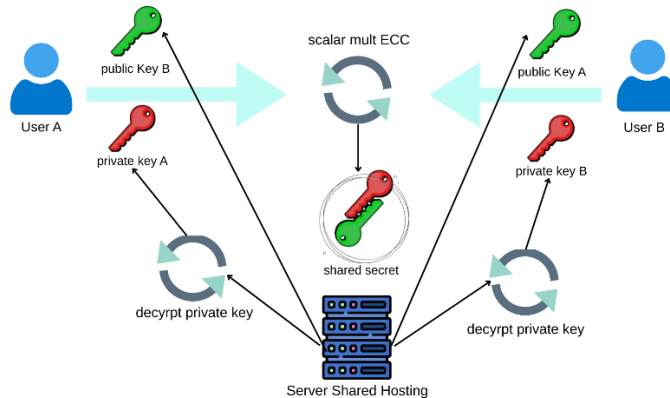
Gambar 1. Proses inialisasi kunci privat dan publik ECC X25519 pada tahap registrasi pengguna

Kunci publik disimpan dan dapat dipertukarkan antar pengguna untuk keperluan pertukaran kunci, sementara kunci privat tetap dirahasiakan dengan cara disimpan dalam basis data dalam bentuk terenkripsi menggunakan AES-256-GCM pada sisi server.

b. Pembentukan *Shared Secret*

Pada tahap pertukaran kunci, ketika pengguna A ingin mengirim pesan kepada pengguna B, maka pengguna A menggunakan kunci privat miliknya dan kunci publik milik B untuk melakukan *scalar multiplication* sesuai algoritma X25519. Sebaliknya, pengguna B dapat melakukan proses yang sama dengan menggunakan kunci privat miliknya dan kunci publik milik A.

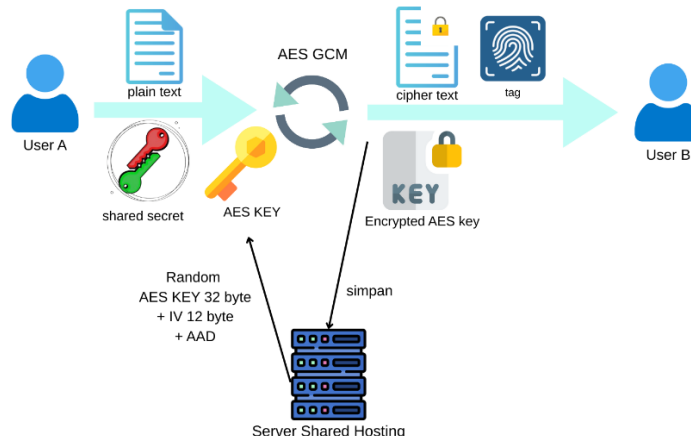
Kedua perhitungan tersebut menghasilkan nilai yang identik, yaitu *shared secret*, meskipun dilakukan secara independen di sisi masing-masing pengguna. *Shared secret* ini kemudian digunakan sebagai untuk enkripsi kunci AES. Alur pertukaran kunci dan pembentukan *shared secret* ditunjukkan pada Gambar 2.



Gambar 2. Pembentukan shared secret melalui pertukaran kunci publik dan privat antar pengguna

c. Proses Enkripsi Pesan/*File*

Setelah *shared secret* terbentuk, langkah berikutnya adalah melakukan enkripsi terhadap data aktual (pesan atau *file*) menggunakan algoritma AES-256-GCM. Proses enkripsi pesan/*file* ditunjukkan pada Gambar 3.



Gambar 3. Proses Enkripsi *Plaintext* dan Kunci AES

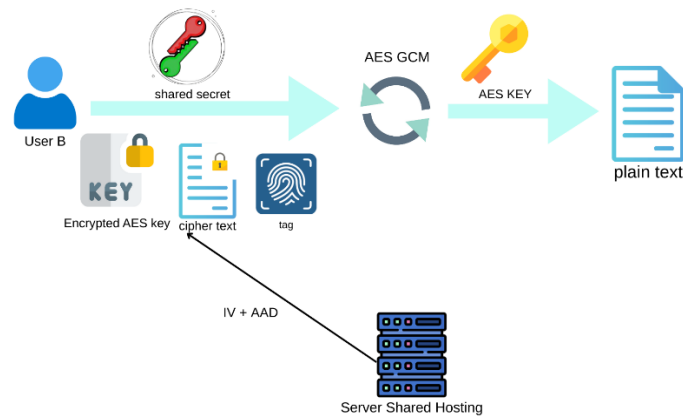
Proses ini berjalan sebagai berikut:

1. Input *plaintext* (pesan/*file*), kunci AES-256 (dibangkitkan secara acak 32 byte), IV (*nonce* 12 byte), serta data tambahan opsional AAD (*Additional Authenticated Data*).
2. Algoritma AES-256-GCM melakukan enkripsi dengan mode *counter* (CTR) yang menghasilkan *ciphertext* sekaligus membangkitkan *authentication tag* yang berfungsi sebagai kode autentikasi yang diverifikasi di sisi penerima untuk menjamin integritas dan keaslian data, sehingga apabila terjadi modifikasi sekecil apa pun pada *ciphertext*, dekripsi akan gagal.
3. Distribusi kunci AES-256 yang digunakan tidak dikirim secara langsung. Kunci tersebut terlebih dahulu dienkripsi menggunakan *shared secret* dengan AES-256-GCM, menghasilkan *encrypted AES key*. *Encrypted key* ini dikirim bersamaan dengan *ciphertext* dan *authentication tag*.

Dengan cara ini, penerima yang memiliki *shared secret* yang sama dapat mendekripsi *encrypted AES key*, mendapatkan kembali kunci AES-256, lalu menggunakan kunci tersebut untuk membuka *ciphertext* menjadi *plaintext*.

d. Proses Dekripsi Pesan/*File*

Selanjutnya di sisi penerima proses dekripsi ditunjukkan pada Gambar 4.



Gambar 4. Proses dekripsi *ciphertext*

Proses dekripsi dilakukan secara kebalikan dari enkripsi:

1. Penerima memperoleh *ciphertext*, *encrypted AES key*, *authentication tag*, serta parameter IV dan AAD dari pengirim.
2. *Encrypted AES key* didekripsi menggunakan *shared secret* hasil pertukaran kunci ECC X25519, sehingga diperoleh kembali kunci AES-256.
3. *Ciphertext* didekripsi menggunakan kunci AES-256 tersebut dengan algoritma AES-256-GCM.
4. *Authentication tag* diverifikasi. Jika tag valid, *plaintext* asli berhasil dipulihkan; jika tidak valid, pesan dianggap rusak atau telah dimanipulasi.

Dengan demikian, penerima hanya dapat membuka pesan apabila memiliki *shared secret* yang benar dan *authentication tag* valid, sehingga kerahasiaan serta integritas data tetap terjaga.

e. Ringkasan Proses

Secara keseluruhan, tahapan implementasi *hybrid encryption* dalam sistem ini dapat diringkas yaitu:

1. Inisialisasi kunci terjadi pada saat registrasi, setiap pengguna membangkitkan pasangan kunci privat dan publik ECC X25519. Kunci privat disimpan dalam database dalam bentuk terenkripsi AES-256-GCM, dan saat login kunci privat didekripsi ke dalam session pengguna.
2. Pertukaran kunci publik antar pengguna melalui *server*.
3. Pembentukan *shared secret* melalui operasi *scalar multiplication* antara kunci privat milik sendiri dan kunci publik milik lawan komunikasi.
4. Enkripsi pesan/*file* menggunakan kunci AES-256-GCM yang dibangkitkan secara acak (32 byte AES key + 12 byte IV + AAD).
5. Kunci AES-256 kemudian dienkripsi menggunakan *shared secret* dengan AES-GCM.
6. Pengiriman *ciphertext*, *authentication tag*, serta *encrypted AES key* ke penerima.

7. Penerima mendekripsi *encrypted* AES key menggunakan *shared secret*, sehingga mendapatkan kembali kunci AES-256.
8. *Ciphertext* didekripsi dengan kunci AES-256-GCM, dan *plaintext* asli berhasil dipulihkan jika *authentication tag* valid.

2.3 Pengujian dan Validasi

Pada bagian ini dijelaskan pendekatan pengujian yang digunakan untuk memastikan sistem *hybrid encryption* bekerja sesuai standar kriptografi modern. Pengujian dilakukan dengan dua pendekatan utama, yaitu validasi algoritma dan uji program.

a. Validasi Algoritma

1. ECC X25519 divalidasi menggunakan *test vector* resmi dari RFC 7748.
2. AES-256-GCM divalidasi menggunakan *test vector* dari NIST SP 800-38D.

Kesesuaian hasil enkripsi/dekripsi dengan nilai acuan menjadi indikator bahwa fungsi kriptografi dasar telah diimplementasikan dengan benar.

b. Uji Program

Pengujian program dilakukan pada modul *chatting* dan penyimpanan *file* dalam sistem *hybrid encryption* pada web:

1. Jenis pesan: teks pendek (≤ 100 karakter) dan teks panjang (≥ 1.000 karakter).
2. *File*: kecil (≤ 5 MB) dan (10–40 MB).

Parameter yang dicatat:

1. Durasi proses (enkripsi dan dekripsi per pesan maupun per *file*).
2. Kesesuaian *ciphertext* (apakah *file*/pesan berhasil dipulihkan 100% menjadi *plaintext* asli).
3. Keutuhan data (apakah *authentication tag* valid atau gagal diverifikasi).
4. Kinerja sistem (latensi *chatting real-time*, kecepatan unduhan *file* terenkripsi dengan *chunk*).

Kriteria keberhasilan:

1. Pesan dan *file* berhasil dipulihkan dengan *plaintext* asli tanpa error.
2. *Authentication tag* valid, menandakan integritas data terjaga.
3. Sistem tetap dapat beroperasi meskipun terdapat keterbatasan infrastruktur (misalnya limit eksekusi 120 detik pada *shared hosting*).

3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi analisis, hasil implementasi ataupun pengujian serta pembahasan dari topik penelitian, yang bisa dibuat terlebih dahulu metodologi penelitian. Bagian ini juga merepresentasikan penjelasan yang berupa penjelasan, gambar, tabel dan lainnya.

3.1 Data Pengujian

Pengujian dilakukan menggunakan data simulasi yang menyerupai pesan teks dan *file* dokumen sebagaimana aktivitas komunikasi internal perusahaan. Jenis data dan tujuannya dirangkum pada Tabel 1. Pengujian awal dilakukan untuk memastikan implementasi kriptografi sesuai dengan standar internasional.

Tabel 1. Data Pengujian

No	Nama File	Jenis File	Ukuran	Fungsi Pengujian
1	Pesan Chat Simulasi	Plaintext, JPG, XLSX, DOCX	-	Uji komunikasi <i>real-time</i> dan enkripsi pesan
2	Data Kupon A	XLSX	11 MB	Uji enkripsi file kecil
3	Data Kupon B	XLSX	25 MB	Uji performa enkripsi file sedang
4	Data Kupon C	XLSX	41 MB	Uji integritas data dengan AES-GCM
5	<i>Test Vector</i> AES-GCM	Hexadecimal	-	Validasi enkripsi AES-GCM (NIST)
6	<i>Test Vector</i> X25519	Hexadecimal	-	Validasi <i>scalar multiplication</i> (RFC 7748)

3.2 Validasi Algoritma

Pengujian Pengujian awal dilakukan untuk memastikan bahwa implementasi kriptografi pada sistem sesuai dengan acuan standar internasional. Dua algoritma yang divalidasi adalah *Elliptic Curve Diffie-Hellman X25519* dan AES-256-GCM.

a. Validasi ECC X25519

Validasi algoritma dilakukan menggunakan *test vector* resmi dari RFC 7748 *Section 6.1*. Pada uji coba ini, digunakan kunci privat milik Alice dan kunci publik milik Bob, yang terlebih dahulu dikonversi dari heksadesimal ke biner, kemudian diubah ke format Base64 agar sesuai dengan fungsi helper dalam sistem. Proses *scalar multiplication* menghasilkan *shared secret* outputnya :

```
4a5d9d5ba4ce2de1728e3bf480350f25e07e21c947d19e3376f09b3c1e161742
```

Nilai tersebut identik dengan hasil yang tercantum dalam dokumen RFC 7748. Hal ini menunjukkan bahwa implementasi X25519 pada sistem telah memenuhi kriteria berikut:

1. Proses *clamping* terhadap kunci privat berjalan sesuai aturan.
2. *Decoding little-endian* dilaksanakan dengan benar.
3. *Shared secret* yang dihasilkan bersifat simetris pada kedua belah pihak.

Dengan demikian, mekanisme pertukaran kunci dapat dinyatakan valid dan aman untuk digunakan dalam skema enkripsi. Hasil pengujian divisualisasikan pada Gambar 5.

```
[u593200165@id-dci-web1416 laravel]$ php artisan tinker
Psy Shell v0.12.8 (PHP 8.3.19 - cli) by Justin Hileman
> $privatekey = base64_encode(hex2bin("77076d0a7318a57d3c16c17251b26645df4c2f87e
bc0992ab177fba51db92c2a"));
= "dwdtCnMYpX08FsFyUbJmRd9ML4frwJkqsXf7pR25LCo="
> $publickey = base64_encode(hex2bin("de9edb7d7b7dc1b4d35b61c2ece435373f8343c85b
78674dadfc7e146f882b4f"));
= "3p7bfXt9wbTTW2HC7OQ1Nz+DQ8hbeGdNr fx+FG+IK08="
> use App\Helpers\ECC\ECCHelper;
> $sharedKey = ECCHelper::sharedSecret($privatekey, $publickey);
= "S12dW6TOLeFyjjv0gDUPJeB+Ic1H0Z4zdVcbPB4WF0I="
> base64_decode($sharedKey);
= b"J]0[ř†-8zÄ;9Ç5\x0F%0~!FGD×3v-ø<\x1E\x16\x17B"
> bin2hex(base64_decode($sharedKey));
= "4a5d9d5ba4ce2de1728e3bf480350f25e07e21c947d19e3376f09b3c1e161742"
```

Gambar 5. Hasil validasi algoritma ECC X25519 menggunakan *test vector* RFC 7748 pada terminal Laravel Tinker

b. Validasi AES-256-GCM

Validasi AES-256-GCM dilakukan menggunakan *test vector* dari NIST GCM Specification, *Test Case 14* (SP 800-38D). Parameter yang dipakai berupa kunci 256-bit bernilai nol, IV bernilai nol, dan plaintext sepanjang 16 byte nol. Proses enkripsi melalui fungsi *aesGcmEncrypt()* menghasilkan *ciphertext* berikut: cea7403d4d606b6e074ec5d3baf39d18 dan *authentication tag*: 036f9a92e192638daebb4061a3db57e7 hasil validasi AES-256-GCM dapat dilihat pada Gambar 6.

Pada Gambar 7, terlihat bahwa setiap pesan menampilkan informasi durasi proses enkripsi dan dekripsi dalam satuan detik. Nilai yang ditampilkan relatif sangat kecil (misalnya 0,045 detik), menunjukkan bahwa proses kriptografi terjadi secara *real-time* tanpa menimbulkan latensi berarti. Dengan demikian, dapat disimpulkan bahwa penerapan *hybrid encryption* (AES-GCM + ECC X25519) dapat digunakan dalam komunikasi aktif tanpa mengurangi kenyamanan pengguna.

b. Pengujian Enkripsi dan Dekripsi *File*

Selain pengujian pada pesan teks, modul penyimpanan *file* juga diuji untuk mengukur kinerja enkripsi dan dekripsi pada data berukuran besar. Transparansi sistem diperkuat dengan penampilan waktu proses langsung pada antarmuka aplikasi, sehingga pengguna dapat mengetahui durasi enkripsi maupun dekripsi setiap *file*. Pada Gambar 8 ditunjukkan tabel penyimpanan *file* yang berisi informasi ukuran *file*, durasi enkripsi, dan durasi dekripsi.

Penyimpanan Saya

Nama File	Ukuran	Dibuat	Durasi Enkripsi	Durasi Dekripsi	Kode Share	Key	Aksi
epn_januari_februari_Mar.xlsx	41,592.86 KB	33 menit yang lalu	332.834 detik	121.104 detik	-	-	Unduh Bagikan Hapus
EPN Data Raw Jan-Mar 2024 v0.1.21102024.xlsx	25,958.74 KB	44 menit yang lalu	209.402 detik	121.110 detik	-	-	Unduh Bagikan Hapus
data.xlsx	12,799.41 KB	46 menit yang lalu	136.590 detik	121.103 detik	-	-	Unduh Bagikan Hapus
DCM_Jobdesc_DBA.pptx	4,847.40 KB	1 jam yang lalu	38.682 detik	68.850 detik	-	-	Unduh Bagikan Hapus

Gambar 8. Pengujian penyimpanan file dan durasi proses di aplikasi web

Hasil uji menunjukkan bahwa:

1. *File* berukuran 41 MB membutuhkan waktu enkripsi 332 detik dan dekripsi berhenti 121 detik.
2. *File* berukuran 25 MB membutuhkan waktu enkripsi 209 detik dan dekripsi berhenti 121 detik.
3. *File* berukuran 12 MB membutuhkan waktu enkripsi 136 detik dan dekripsi berhenti 121 detik.
4. *File* berukuran kecil (sekitar 4 MB) hanya membutuhkan enkripsi 38 detik dan dekripsi 68 detik.
5. Durasi enkripsi meningkat sebanding dengan ukuran *file*, sedangkan proses dekripsi lebih lambat karena membuat tag dan membandingkan dengan tag di *database* untuk verifikasi tag.

Selain itu, hasil pengujian memperlihatkan peran penting mekanisme *chunking* dan *streaming*. Setiap *file* dipecah menjadi potongan (*chunk*) berukuran 512 KB agar dapat diproses secara bertahap. Hal ini dilakukan untuk mengatasi batasan eksekusi pada *shared hosting* (misalnya limit waktu PHP), serta memungkinkan pemrosesan *file* besar tanpa perlu memori besar sekaligus. Setiap *chunk* disimpan dalam database bersama parameter kriptografi yang diperlukan, yaitu *initialization vector* (IV) dan *authentication tag*. Contoh penyimpanan hasil enkripsi ditunjukkan pada Gambar 9, di mana terlihat bahwa:

id	message_id	chunk_index	chunk_data	iv	tag	created_at	updated_at
9	11	0	n/bUbbtmr3uL66hQUyKF8BAyDdFyQJvMf8FHnuwBNy1wkT...	ui36gGQ4xwv7ZUs	qrDDWbc3JcXtSEakf4F3g==	2025-07-08 10:05:11	2025-07-08 10:05:11
10	12	0	Hl09SlKCN4DZ7WAK9M3M0FznaiWOJ35C9H9QFlaaWCnffxvC...	apIYpIUjRYV+GwGe	cv2kFLuxXz4qhoCymJoTYA==	2025-07-08 10:08:11	2025-07-08 10:08:11
11	13	0	NEXfwTq5HJl0FavUNs1xddRwFmLc1JuEDt9sp5n2lQrMhvRIJM...	UPbnm3mBghhh5Q80	IE9EzATwC2fLM+U4hftbg==	2025-07-08 10:09:15	2025-07-08 10:09:15
12	13	1	4lBwb0u2TD3ase1hdLYOcrwHNP8pURFJ555w0GF+WQQIGCpdD...	/MGN2k96u8m3AQfS	WHvzCfauxulatwixPHYEew==	2025-07-08 10:09:16	2025-07-08 10:09:16
13	13	2	RCJ49eY9OB4QRn7Ri7a2Cbq7Vc+PHSuoqkyjKZlSivgpNH...	yvQg0pQiel87/3JO	g1855+E1tgoJgfJQw8CZxg==	2025-07-08 10:09:16	2025-07-08 10:09:16
14	13	4	8FpI0+mzq8K9HvUGfhpOnZgwp16+Orcl3g+PROVnbwS49CR...	uqQRaNaqx8QXU7pP0	rvcMlqbmBJ26jnFrHEmY6g==	2025-07-08 10:09:27	2025-07-08 10:09:27
15	13	3	Qsft7hVad1t7ST3Djryl9z77SITh85qMfwwBDO5ic2wuucts...	I5xYx8kscEB4ybSW	dUuPn00QNdMm0qHfeU+J1A==	2025-07-08 10:09:27	2025-07-08 10:09:27
16	13	5	HWR81RqUc9Uizl0CthP7xClxyjop9lUj0Y52vP/tcvsaA8fr...	JGH5Vih0EenusYfpz	0KWYoiHMHJbHSLQoOxzsq==	2025-07-08 10:09:28	2025-07-08 10:09:28
17	13	8	kieRHQwBsG3A7OFI8hvCasUQVvXUA3djHGrighpRpg1F3JtUg...	bqer7B2CaoRlCIZD	y02DFV0AJXlGWZpQUbqAiw==	2025-07-08 10:09:37	2025-07-08 10:09:37
18	13	6	EJCMc2nSralbJgYF9Kli109eKwBfUz1A1MYrPm+afZmLH2Cz...	088bSRaIBKzOZ1T	ST3t9KJoE9FaV0dLporw==	2025-07-08 10:09:39	2025-07-08 10:09:39
19	13	7	aQvPOMVj09x9wBPorQsPyrGvNIK2SlpMGskPINRUMGJ161tw...	af+zJWD7IY5T5K12	NVdW0ufXBcTRgDbHZUaoOQ==	2025-07-08 10:09:39	2025-07-08 10:09:39

Gambar 9. Hasil penyimpanan *ciphertext* pada *file* dengan *chunk* di database

1. Kolom *chunk_data* berisi *ciphertext* hasil enkripsi AES-256-GCM.
2. Kolom *iv* menyimpan nonce unik untuk setiap chunk, yang dibutuhkan untuk proses dekripsi.
3. Kolom *tag* berisi *authentication tag* yang digunakan untuk menjamin integritas data.

4. Penyimpanan data dalam bentuk terenkripsi memastikan bahwa meskipun *database* berhasil diakses pihak tidak berwenang, isi *file* tetap tidak dapat dibaca tanpa kunci dekripsi yang sah.

Mekanisme dekripsi juga dioptimalkan dengan dukungan HTTP *Range Request* (status *206 Partial Content*). Server hanya mendekripsi *chunk* sesuai rentang byte yang diminta oleh client, kemudian mengirimkannya secara bertahap melalui koneksi TCP yang tetap terbuka. Dengan pendekatan ini:

1. Dekripsi berjalan *on-the-fly* (langsung saat data diminta), bukan setelah seluruh *file* selesai diproses.
2. Client dapat melanjutkan unduhan (*resume download*) jika koneksi terputus, cukup meminta sisa *chunk* yang belum diterima.
3. Durasi dekripsi relatif stabil karena dilakukan per *chunk*, bukan sekali proses penuh.

Namun, perlu dicatat bahwa pada pengujian di *shared hosting*, proses dekripsi terhenti pada batas waktu eksekusi *server* (sekitar 120 detik). Hal ini menjelaskan mengapa hasil pengukuran dekripsi selalu berhenti di angka ± 121 detik, meskipun ukuran *file* berbeda. Artinya, keterbatasan ini bukan berasal dari algoritma, melainkan dari konfigurasi *server*. Dengan infrastruktur yang lebih fleksibel (misalnya VPS dengan *execution time* tanpa batas atau pengaturan *chunk size* yang lebih kecil melalui *JavaScript*), durasi dekripsi dapat menyesuaikan ukuran file dan tidak terhenti di angka tetap.

Secara keseluruhan, hasil ini menunjukkan bahwa sistem mampu menangani *file* berukuran menengah hingga besar dengan reliabilitas yang baik. Walaupun waktu enkripsi relatif tinggi, penggunaan *chunking* dan *streaming* dekripsi memastikan sistem tetap efisien, aman, serta ramah bagi pengguna pada kondisi jaringan yang tidak selalu stabil.

c. Rincian Hasil Pengujian

Hasil pengujian dapat dirangkum dalam **Tabel 2**, yang memperlihatkan kinerja modul *chatting*, enkripsi *file*, serta validasi data.

Tabel 2. Hasil Pengujian

Modul	Parameter Utama	Hasil	Catatan Teknis
<i>Chatting</i>	Latensi enkripsi/dekripsi	$\sim 0,045$ detik per pesan (<i>real-time</i>)	Layak dipakai komunikasi aktif
Enkripsi File	4–41 MB	Enkripsi 38–332 s, Dekripsi berhenti 121 s	Dekripsi terhenti karena limit PHP 120 detik
Validasi Data	<i>Authentication tag</i>	Perubahan data terdeteksi	Integrity check berhasil

3.4 Analisis

Hasil pengujian memperlihatkan bahwa implementasi hybrid encryption berbasis AES-GCM dan ECC X25519 berjalan dengan benar, namun terdapat beberapa temuan penting yang perlu dianalisis lebih lanjut:

- a. Kinerja Enkripsi vs Dekripsi
 1. Waktu enkripsi meningkat sebanding dengan ukuran *file* (hingga 332 detik untuk 41 MB).
 2. Dekripsi relatif lebih cepat (sekitar 121 detik) karena hanya melakukan verifikasi *authentication tag*.
 3. Namun, pada *file* berukuran besar dekripsi terhenti di sekitar 121 detik akibat batas eksekusi PHP pada *shared hosting*, bukan karena keterbatasan algoritma.
- b. Keterbatasan Infrastruktur
 1. Lingkungan *shared hosting* membatasi eksekusi script maksimal ± 120 detik, sehingga *file* besar tidak dapat diproses penuh dalam satu permintaan.
 2. Hal ini menunjukkan bahwa performa sistem tidak hanya ditentukan oleh algoritma kriptografi, tetapi juga oleh infrastruktur server yang digunakan.
- c. Solusi Teknis
 1. Pembagian *file* menjadi *chunk* 512 KB sudah efektif mencegah limit memori.
 2. Untuk mengatasi limit waktu, mekanisme *resume download* dengan HTTP *Range Request* dapat dipadukan dengan *JavaScript client-side* agar proses dekripsi tetap berlanjut meski koneksi terputus atau *server timeout*.
 3. Alternatif lain adalah penggunaan *job queue* atau *worker* terpisah di server yang lebih fleksibel dibanding *shared hosting*.
- d. Implikasi Keamanan
 1. *Authentication tag* AES-GCM terbukti efektif dalam mendeteksi perubahan data, menjamin integritas *file*.

2. ECC X25519 menghasilkan *shared secret* yang aman dengan *overhead* komputasi rendah, sehingga cocok untuk aplikasi *real-time*

4. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

- a. *Hybrid encryption* berbasis AES-256-GCM dan ECC X25519 berhasil diimplementasikan pada aplikasi komunikasi berbasis web. AES-256-GCM menjaga kerahasiaan sekaligus integritas data melalui *authentication tag*, sedangkan ECC X25519 menjamin distribusi kunci secara aman dan efisien.
- b. Implementasi kriptografi sesuai dengan standar resmi (RFC 7748 untuk X25519 dan NIST SP 800-38D untuk AES-GCM). Hal ini membuktikan bahwa fungsi dasar enkripsi dan dekripsi berjalan benar serta dapat diandalkan.
- c. Sistem terbukti berjalan *real-time* pada modul *chatting* dengan latensi sangat rendah, serta mampu mengenkripsi dan mendekripsi file ukuran menengah hingga besar dengan mekanisme *chunking*, meskipun durasi enkripsi meningkat seiring ukuran file.
- d. Penelitian ini menunjukkan bahwa kombinasi AES-256-GCM dan ECC X25519 dapat diterapkan secara nyata pada aplikasi *chatting* dan *file sharing* berbasis web, bukan hanya simulasi, sehingga menjadi kontribusi praktis dalam penerapan *hybrid encryption*.
- e. Proses enkripsi file berukuran besar masih relatif lambat, dan pengujian di lingkungan *shared hosting* terhenti pada batas waktu eksekusi ± 120 detik, sehingga dekripsi tidak sepenuhnya optimal untuk file besar.
- f. Optimalisasi performa enkripsi file besar dapat dilakukan dengan metode paralelisasi, pemanfaatan GPU, atau *job queue* di server. Selain itu, pengujian pada skenario jaringan kompleks (*multi-user dan real-time*) dapat memperluas validitas sistem.

DAFTAR PUSTAKA

- [1] Z. Arif and A. Nurokhman, "Analisis perbandingan algoritma kriptografi simetris dan asimetris dalam meningkatkan keamanan sistem informasi," *Jurnal Teknologi dan Sistem Informasi (JTSI)*, vol. 4, no. 2, pp. 394–405, Sep. 2023, doi: 10.35957/jtsi.v4i2.6077.
- [2] A. R. Harahap and T. A. Salim, "Sistem kriptografi pada pengamanan autentikasi dokumen elektronik: Systematic literature review," *Jurnal Pengembangan Kearsipan*, vol. 16, no. 2, pp. 203–220, Oct. 2023, doi: 10.22146/khazanah.81893.
- [3] J. Daemen and V. Rijmen, "Advanced encryption standard (AES)," *NIST FIPS PUB 197*, Nov. 2001, updated May 2023, doi: 10.6028/NIST.FIPS.197-upd1.
- [4] R. M. H. Hernandi and J. C. Chandra, "Implementasi algoritme AES-256 dan AES-GCM untuk mengamankan dokumen pada sistem data rekam medis klinik mulya," *KRESNA: Jurnal Riset dan Pengabdian Masyarakat*, vol. 4, no. 1, pp. 12–22, May 2024, doi: 10.36080/kresna.v4i1.131.
- [5] L. Chen, D. Moody, A. Regenscheid, A. Robinson, and K. Randall, "Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters," *NIST Special Publication 800-186*, Feb. 2023, doi: 10.6028/NIST.SP.800-186.
- [6] V. Tanksale, "Efficient elliptic curve Diffie–Hellman key exchange for resource-constrained IoT devices," *Electronics (Switzerland)*, vol. 13, no. 18, pp. 1–13, Sep. 2024, doi: 10.3390/electronics13183631.
- [7] P. Iqlima et al., "Implementasi sistem keamanan data menggunakan algoritma kriptografi asimetris elliptic curve cryptography (ECC) berbasis website," *Jurnal Ilmu Komputer (JIKUM)*, vol. 1, no. 1, pp. 10–18, 2025, doi: 10.62671/jikum.v1i1.37.
- [8] P. Selvi and S. Sakthivel, "A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection," *Scientific Reports*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-01315-5.
- [9] Y. M. A. Abualkas and D. L. Bhaskari, "Hybrid approach to cloud storage security using ECC-AES encryption and key management techniques," *International Journal of Engineering Trends and Technology*, vol. 72, no. 4, pp. 92–100, Apr. 2024, doi: 10.14445/22315381/IJETT-V72I4P110.
- [10] A. Langley, M. Hamburg, and S. Turner, "Elliptic curves for security," RFC 7748, Internet Engineering Task Force (IETF), Jan. 2016. [Online]. Available: <https://www.rfc-editor.org/info/rfc7748>.
- [11] D. A. McGrew and J. Viega, "The Galois/counter mode of operation (GCM)," National Institute of Standards and Technology (NIST), 2004. [Online]. Available: <https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/gcm/gcm-spec.pdf>.
- [12] A. Widarma, "Kombinasi algoritma simetri dan ECC untuk meningkatkan keamanan pesan," *Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 8, no. 1, pp. 1–5, 2023, doi: 10.30743/infotekjar.v8i1.9642.