



Implementasi Hybrid Algoritma RSA dan Vernam Cipher Menggunakan Model DevSecOps untuk Keamanan Data Pegawai pada BPKPAD Kabupaten Balangan

Muhammad Rifky¹, Deanna Durbin Hutagalung²

Program Studi Teknik Informatika, Universitas Pamulang^{1,2}

Jl. Raya Puspitek No.46, Kel.Buaran, Kec.Serpong, Kota Tangerang Selatan, Indonesia^{1,2}

muhirifky03@gmail.com*¹, dosen01677@unpam.ac.id²

Kata Kunci:

Keamanan Data
Pegawai; RSA;
Vernam Cipher;
Hybrid
Cryptography;
DevSecOps.

ABSTRAK

Keamanan data pegawai merupakan aspek penting dalam menjaga kerahasiaan informasi pada instansi pemerintah. Pengelolaan data secara digital tanpa mekanisme pengamanan yang memadai berpotensi menimbulkan akses tidak sah, kebocoran data, serta penyalahgunaan informasi. Penelitian ini bertujuan mengimplementasikan hybrid algoritma RSA dan Vernam Cipher menggunakan model DevSecOps untuk meningkatkan keamanan data pegawai pada Badan Pengelolaan Keuangan, Pendapatan, dan Aset Daerah (BPKPAD) Kabupaten Balangan. Metode penelitian meliputi identifikasi kebutuhan sistem, perancangan aplikasi berbasis web menggunakan framework Laravel 11, implementasi algoritma hybrid untuk proses enkripsi dan dekripsi file, penerapan prinsip DevSecOps melalui mekanisme logging aktivitas, serta pengujian sistem menggunakan Black Box Testing, White Box Testing, pengujian waktu proses, dan evaluasi keamanan sistem. Hasil penelitian menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi file secara konsisten sehingga dokumen yang telah dienkripsi tidak dapat diakses tanpa mekanisme autentikasi dan kunci yang sesuai. Implementasi DevSecOps juga mendukung proses pemantauan aktivitas pengguna melalui pencatatan log sehingga meningkatkan kemampuan audit dan pengawasan keamanan sistem. Dengan demikian, penerapan hybrid algoritma RSA dan Vernam Cipher yang dipadukan dengan model DevSecOps mampu meningkatkan perlindungan data pegawai secara lebih aman, terintegrasi, dan terkelola pada lingkungan BPKPAD Kabupaten Balangan.

Keywords

Employee Data
Security; RSA;
Vernam Cipher;
Hybrid
Cryptography;
DevSecOps.

ABSTRACT

Employee data security is a crucial aspect of protecting confidential information within government institutions. Managing digital data without adequate security mechanisms may lead to unauthorized access, data breaches, and information misuse. This study aims to implement a hybrid RSA and Vernam Cipher algorithm integrated with the DevSecOps model to enhance employee data security at the Regional Financial, Revenue, and Asset Management Agency (BPKPAD) of Balangan Regency. The research methodology includes system requirements analysis, web-based application development using the Laravel 11 framework, implementation of the hybrid encryption and decryption algorithm, integration of DevSecOps principles through activity logging, and system evaluation using Black Box Testing, White Box Testing, processing time analysis, and security testing. The results demonstrate that the developed system performs encryption and decryption processes consistently, ensuring that encrypted files cannot be accessed without proper authentication and valid cryptographic keys. Furthermore, the implementation of DevSecOps supports continuous monitoring through activity logging, thereby improving system auditing and security supervision. Therefore, the integration of the hybrid RSA and Vernam Cipher algorithm



with the DevSecOps model provides a more secure, integrated, and manageable solution for protecting employee data within BPKPAD Balangan Regency.

---Jurnal JISTI @2026---

PENDAHULUAN

Kerahasiaan data sangat penting jika ada informasi yang tidak boleh diketahui oleh publik. Upaya pembobolan data biasanya terjadi saat pengiriman data. Seringkali, data disimpan dalam bentuk file dokumen, PDF, atau sebagai bagian dari gambar atau video. Keamanan dan kerahasiaan data sangat penting baik untuk organisasi maupun individu. Selain itu, dalam kasus di mana data tersebut berada dalam jaringan komputer yang terhubung ke jaringan lain. Tidak diragukan lagi, hal ini akan menimbulkan bahaya jika orang yang tidak berhak mendapatkan informasi sensitif dan penting tersebut. Jika hal itu terjadi, sangat mungkin akan merugikan atau bahkan membahayakan orang yang mengirim atau menerima pesan serta organisasinya. Data yang dibajak juga dapat berubah, yang dapat menyebabkan penerima pesan salah memahaminya. Selain itu, data yang dibajak mungkin rusak atau bahkan hilang, yang dapat menyebabkan kerugian material yang signifikan (Togar Timoteus Gultom, 2021).

Dalam pengiriman pesan, keamanan data sangat penting, terutama untuk pesan rahasia. Dalam aktivitas sehari-hari kita, seperti menggunakan internet untuk membeli sesuatu, mengirimkan e-mail, menggunakan sosial media, dan sebagainya, kita dapat mengetahui hal ini. Karena keamanan data yang dioperasikan pada jaringan publik rentan terhadap serangan, kode diperlukan untuk memastikan bahwa pesan tersebut tetap rahasia dan aman. Mekanisme keamanan data digunakan untuk membuat layanan yang aman (Purnama dkk., 2022).

Fenomena tersebut tercermin dari berbagai insiden kebocoran data yang terjadi dalam beberapa tahun terakhir. Pada tahun 2023 dilaporkan dugaan kebocoran jutaan data paspor dari Direktorat Jenderal Imigrasi yang memuat informasi penting, seperti nama, tanggal lahir, nomor paspor, dan kewarganegaraan. Selanjutnya, pada tahun 2024 diduga terjadi kebocoran sekitar 204 juta data kependudukan yang dikelola oleh Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil). Memasuki tahun 2025, dugaan kebocoran data juga terjadi pada sejumlah layanan kesehatan berbasis digital yang berpotensi mengungkapkan informasi medis masyarakat. Rangkaian kasus tersebut menunjukkan bahwa sektor publik masih menghadapi tantangan dalam membangun sistem keamanan informasi yang kuat dan terintegrasi sehingga diperlukan upaya peningkatan perlindungan data secara berkelanjutan (Mulyadi dkk., 2026).

Badan Pengelolaan Keuangan, Pendapatan, dan Aset Daerah (BPKPAD) Kabupaten Balangan merupakan salah satu instansi yang mengelola data pegawai, data administrasi, serta dokumen penting dalam pelaksanaan tugasnya. Pengelolaan data dilakukan melalui sistem informasi berbasis komputer yang terhubung pada jaringan internal. Namun, berdasarkan hasil identifikasi pada objek penelitian, pengamanan data yang diterapkan masih memiliki beberapa keterbatasan, di antaranya belum optimalnya penerapan teknologi enkripsi, belum terintegrasinya aspek keamanan ke dalam seluruh siklus pengembangan sistem, serta masih adanya potensi akses tidak sah akibat kelemahan dalam pengelolaan hak akses maupun penyalahgunaan kredensial pengguna. Kondisi tersebut menunjukkan perlunya mekanisme keamanan yang mampu melindungi data sekaligus mendukung pengelolaan sistem secara lebih aman.

Salah satu pendekatan yang dapat diterapkan untuk meningkatkan keamanan data adalah kriptografi. Pada penelitian ini digunakan kombinasi algoritma RSA dan Vernam Cipher dalam skema



hybrid cryptography. Algoritma RSA dimanfaatkan sebagai algoritma kriptografi asimetris untuk mendukung pengelolaan dan distribusi kunci secara aman, sedangkan Vernam Cipher digunakan sebagai algoritma simetris yang memiliki proses enkripsi dan dekripsi relatif sederhana. Kombinasi kedua algoritma tersebut diharapkan mampu memanfaatkan keunggulan masing-masing algoritma sehingga dapat menghasilkan mekanisme pengamanan data yang lebih efektif dibandingkan penggunaan satu algoritma secara terpisah (Liana dkk., 2023).

Selain penerapan algoritma kriptografi, penelitian ini mengintegrasikan model DevSecOps sebagai pendekatan keamanan dalam proses pengembangan sistem. DevSecOps menempatkan aspek keamanan sebagai bagian yang terintegrasi pada setiap tahapan pengembangan aplikasi sehingga proses perlindungan data tidak hanya berfokus pada mekanisme enkripsi, tetapi juga mencakup autentikasi pengguna, pencatatan aktivitas (logging), serta pengawasan keamanan sistem secara berkelanjutan. Berdasarkan kondisi tersebut, penelitian ini bertujuan mengimplementasikan hybrid algoritma RSA dan Vernam Cipher menggunakan model DevSecOps untuk meningkatkan keamanan data pegawai pada BPKPAD Kabupaten Balangan sehingga mampu memberikan perlindungan data yang lebih aman, terintegrasi, dan mudah diawasi (Gultom, 2021).

METODE PENELITIAN

1. Metode Pengembangan Sistem

Dalam penelitian ini, pendekatan DevSecOps digunakan sebagai pendekatan pengembangan sistem. Dalam pengembangan perangkat lunak, DevSecOps adalah pendekatan yang mengintegrasikan proses pengembangan, keamanan, dan operasional secara berkelanjutan.

Dalam penelitian ini, empat tahap utama implementasi DevSecOps difokuskan, yaitu:

- a. Plan
Pada BPKPAD Kabupaten Balangan, tahap rencana dilakukan dengan menganalisis kebutuhan sistem, menemukan masalah keamanan data pegawai, dan menentukan kebutuhan sistem yang berfungsi dan tidak berfungsi.
- b. Code
Mengimplementasikan algoritma Hybrid RSA dan Vernam Cipher menggunakan framework Laravel 11 dan menerapkan fitur keamanan sistem berbasis DevSecOps adalah langkah-langkah yang digunakan untuk menjalankan kode.
- c. Build
Membangun prototipe aplikasi web yang mencakup fitur login, enkripsi dan dekripsi file, pengelolaan data pegawai, dan pemantauan aktivitas log keamanan merupakan tahap build.
- d. Test
Sistem yang telah dikembangkan diuji dalam beberapa tahap. Ini termasuk pengujian fungsi sistem, pengujian keamanan akses, pengujian proses enkripsi dan dekripsi, dan pengujian fitur logging DevSecOps.

Dalam penelitian ini, prinsip DevSecOps juga diterapkan melalui fitur log keamanan otomatis dan halaman Log Aktivitas DevSecOps sebagai bentuk pemantauan keamanan sistem.

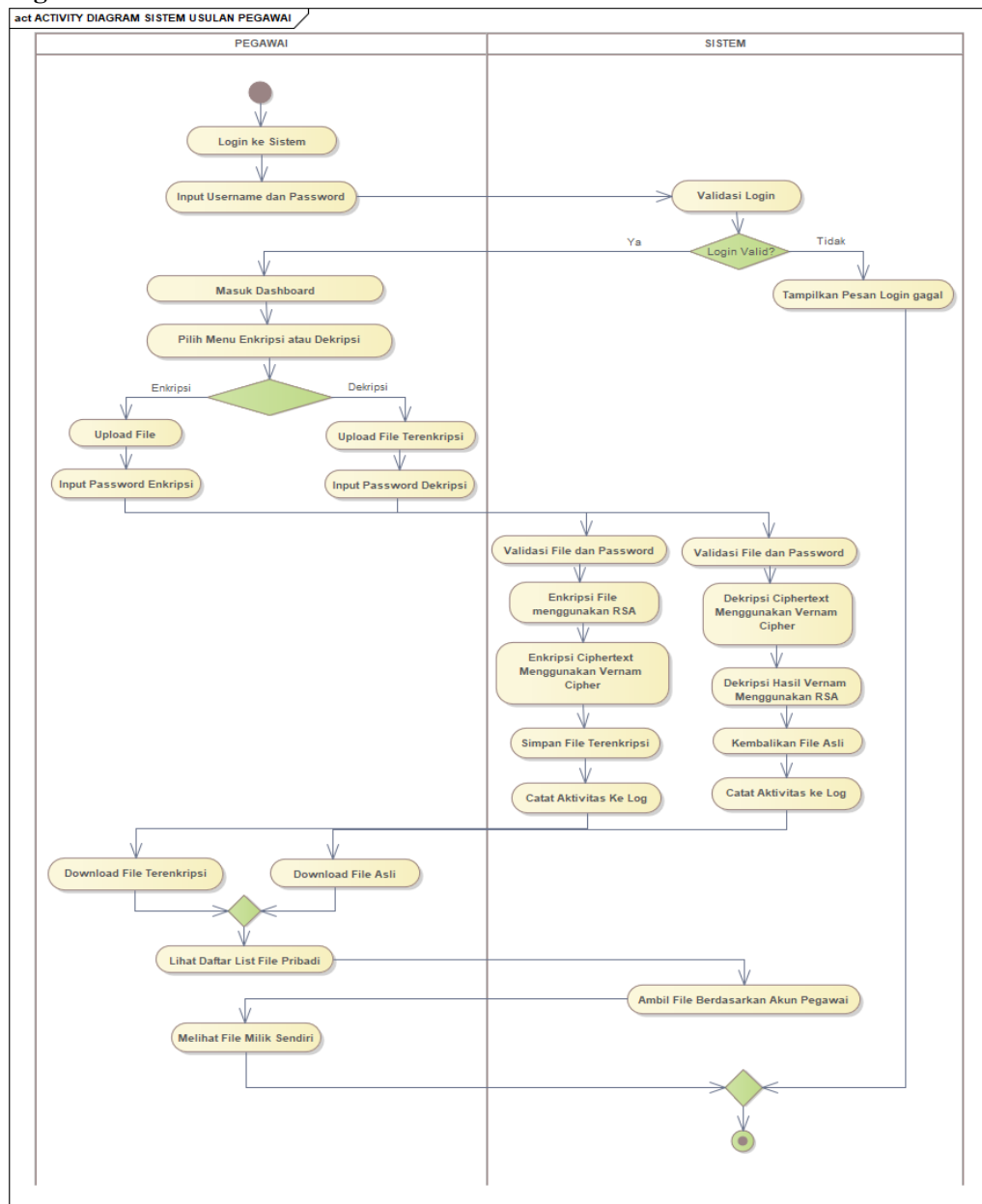
2. Metode Pengumpulan Data

Berikut ini adalah beberapa metode pengumpulan data yang digunakan untuk mendapatkan informasi yang diperlukan untuk proses analisis dan perancangan sistem yaitu Studi Literatur Untuk melakukan penelitian ini, kami melihat buku, artikel, jurnal, dan sumber referensi lainnya yang berkaitan dengan algoritma RSA, Vernam Cipher, Hybrid Cryptography, keamanan data, dan gagasan DevSecOps. Observasi Secara langsung, observasi dilakukan pada BPKPAD Kabupaten Balangan



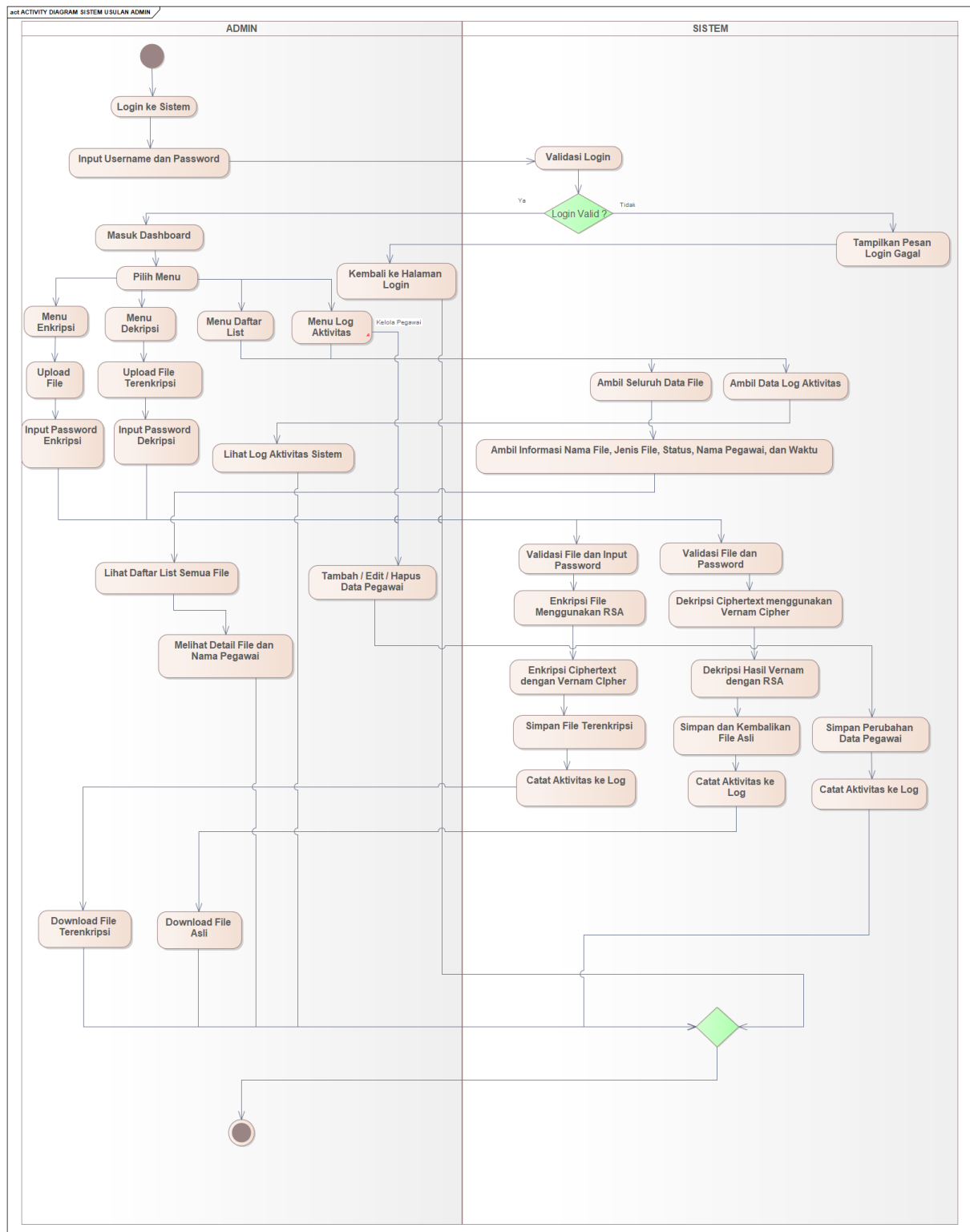
untuk memperoleh pemahaman tentang prosedur pengelolaan data pegawai, metode penyimpanan file, dan masalah keamanan data yang muncul pada sistem yang sedang beroperasi. Wawancara dilakukan dengan pihak-pihak yang relevan mengenai kebutuhan sistem, prosedur pengelolaan data pegawai, dan masalah keamanan data. Dan dokumentasi Untuk melakukan dokumentasi, contoh data pegawai dan informasi tentang sistem pengelolaan data yang digunakan dikumpulkan. Data dummy digunakan untuk menjaga kerahasiaan data asli penelitian.

3. Perancangan Sistem



Gambar 4. Activity Diagram Sistem Usulan Pegawai

Alur proses yang digunakan oleh pegawai untuk melindungi data mereka menggunakan algoritma hybrid RSA dan Vernam Cipher yang dibangun oleh DevSecOps digambarkan dalam aktivitas diagram sistem usulan. Sistem usulan dimaksudkan untuk meningkatkan keamanan data pegawai melalui proses enkripsi dan dekripsi, pengelolaan file pribadi, dan pengawasan aktivitas pengguna.



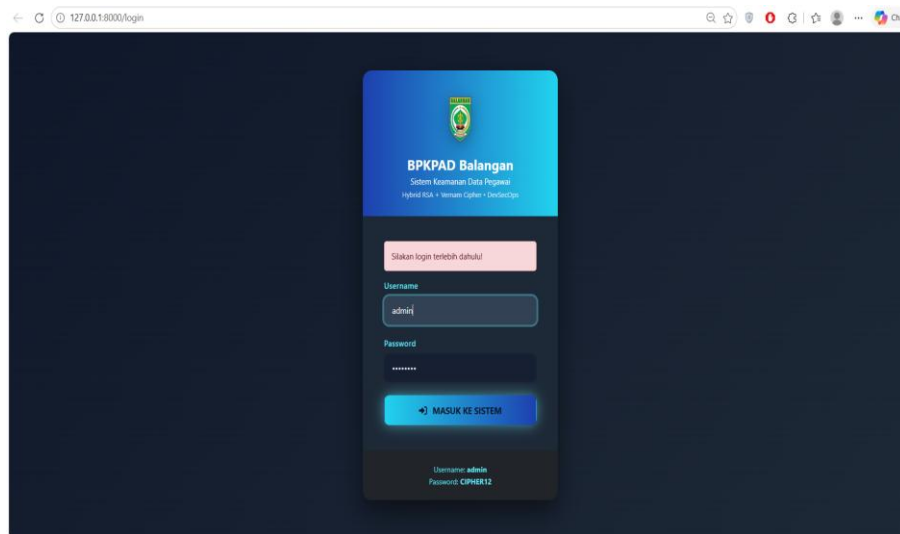
Gambar 5. Activity Diagram Sistem Usulan Admin

Dengan menggunakan algoritma hybrid RSA dan Vernam Cipher berbasis DevSecOps, aktivitas diagram sistem usulan admin menunjukkan proses manajemen keamanan data pegawai. Diagram ini menunjukkan alur login, proses enkripsi dan dekripsi file, pengelolaan data pegawai, pengawasan log aktivitas, dan pengelolaan file sistem.



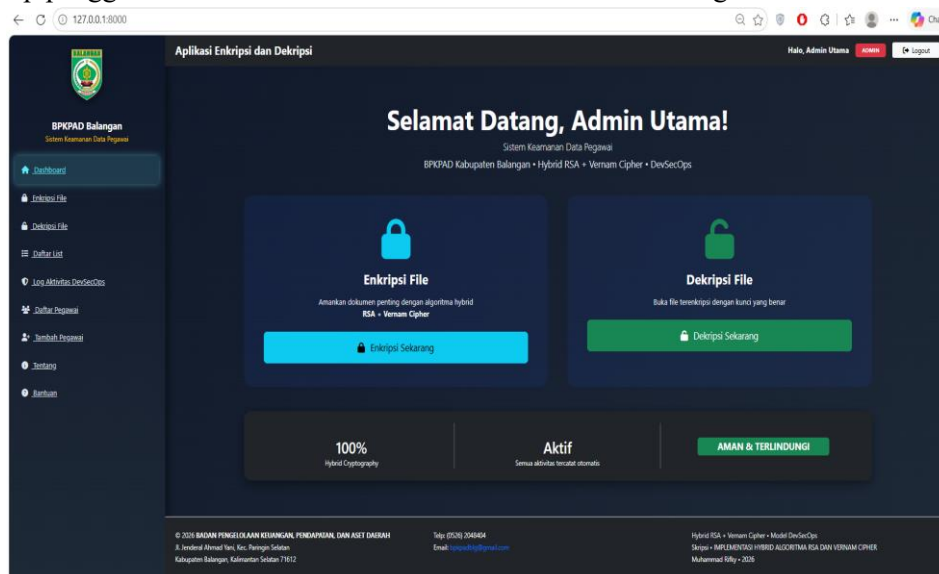
HASIL DAN PEMBAHASAN

1. Implementasi Sistem



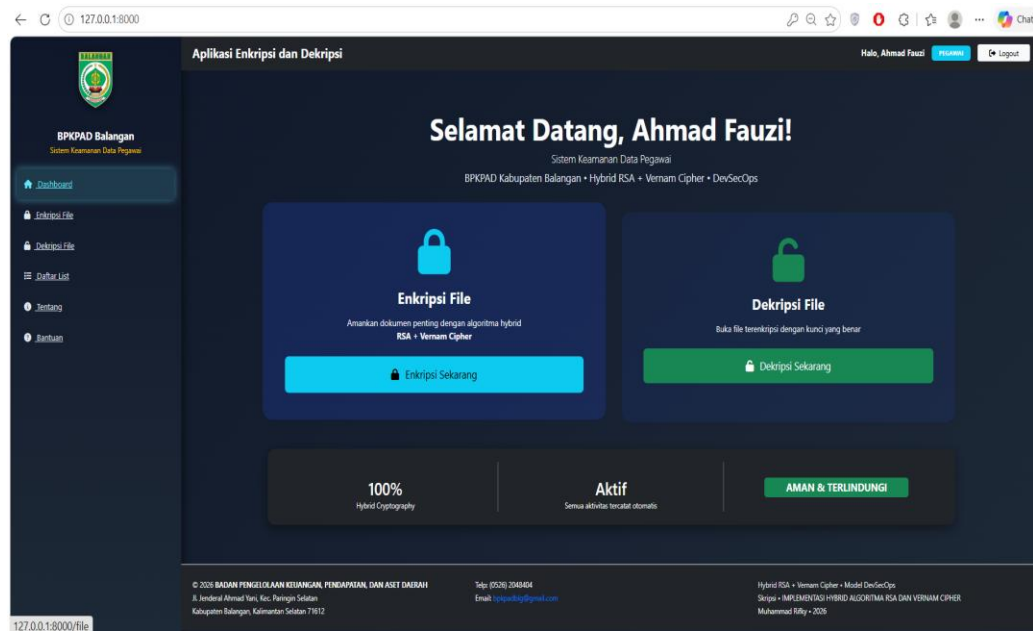
Gambar 6. Halaman Login Admin dan Pegawai

Halaman login adalah tampilan awal sistem di mana administrator dan pegawai dapat mengakses aplikasi keamanan data pegawai. Untuk melakukan proses autentikasi, pengguna harus memasukkan username dan password mereka sebelum dapat mengakses sistem. Halaman ini tidak hanya menampilkan formulir login, tetapi juga informasi singkat tentang implementasi hybrid RSA, Vernam Cipher, dan DevSecOps yang digunakan dalam sistem keamanan data pegawai. Setelah proses login selesai, setiap pengguna akan dibawa ke halaman dashboard sesuai dengan hak akses mereka.



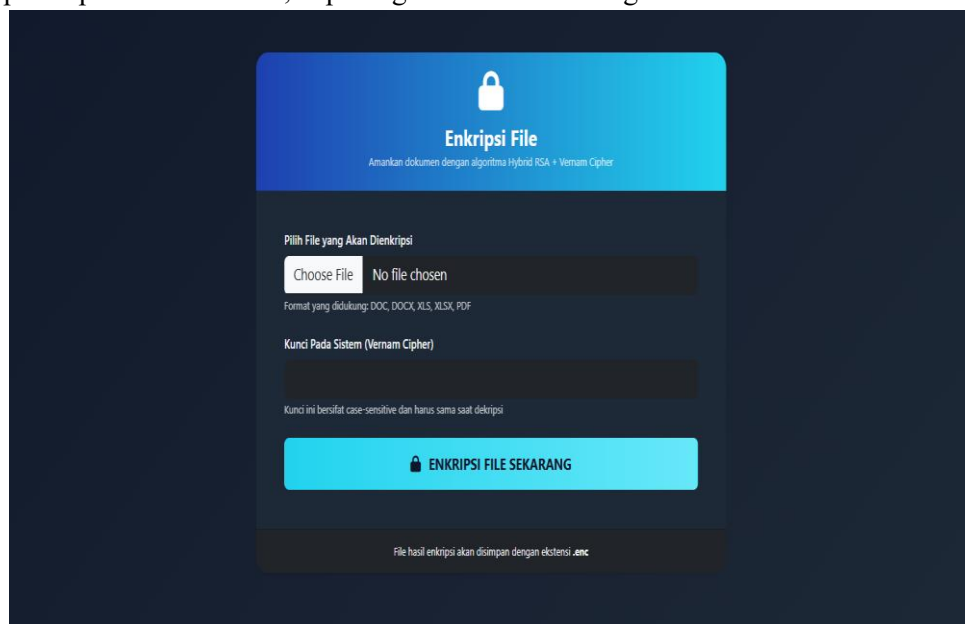
Gambar 7. Halaman Awal dan Dashboard Admin

Setelah admin berhasil login ke sistem, halaman dashboard admin adalah halaman utama di mana admin dapat mengakses fitur penting sistem seperti enkripsi dan dekripsi file, daftar file, log aktivitas DevSecOps, dan pengelolaan data pegawai. Selain itu, dashboard menampilkan informasi singkat tentang status keamanan sistem, implementasi hybrid RSA, Vernam Cipher, dan DevSecOps, yang membantu dalam proses pengamanan data pegawai di aplikasi.



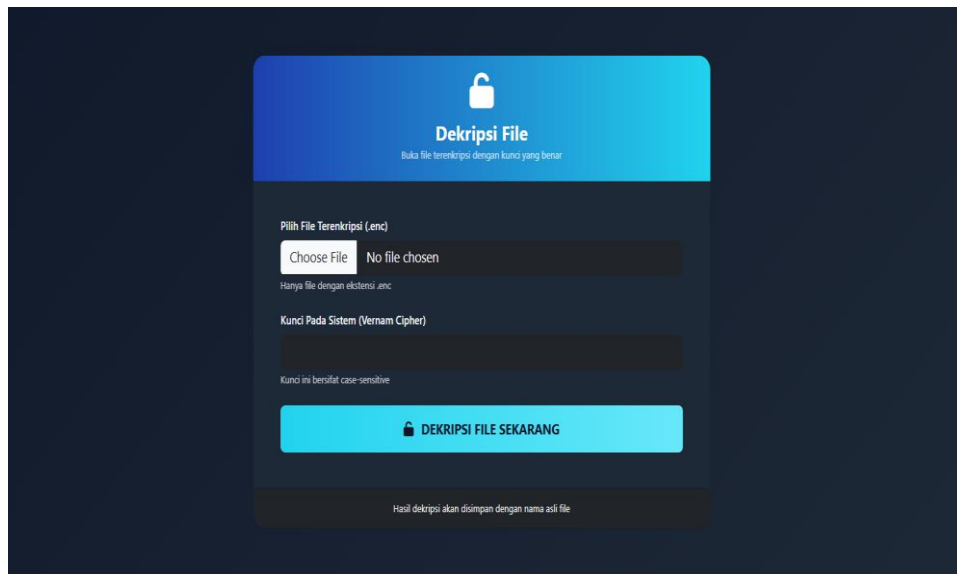
Gambar 8. Halaman Awal dan Dashboard Pegawai

Halaman utama yang ditampilkan setelah pegawai memasuki sistem disebut halaman dashboard pegawai. Pegawai yang memiliki hak akses pengguna dapat melihat fitur enkripsi dan dekripsi file, daftar file, dan informasi aplikasi pada halaman ini. Halaman dashboard menampilkan informasi tentang implementasi hybrid RSA, Vernam Cipher, dan DevSecOps, yang membantu proses keamanan data pegawai pada aplikasi. Selain itu, dapat digunakan untuk mengakses fitur utama sistem.



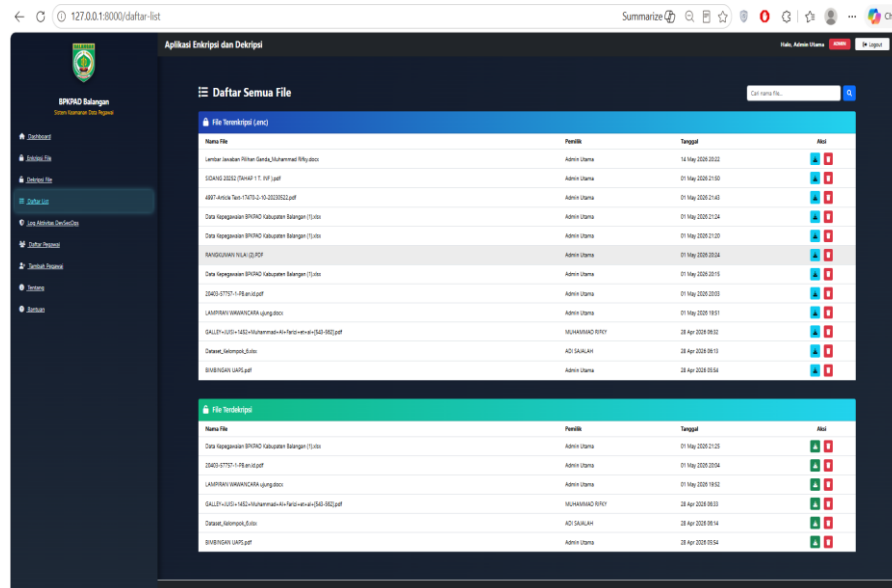
Gambar 9. Halaman Enkripsi File Admin dan Pegawai

Halaman enkripsi file digunakan oleh manajer dan staf untuk melindungi file data mereka dengan menggunakan hybrid RSA dan Vernam Cipher. Pengguna dapat memilih file mana yang akan dienkripsi dan memasukkan kata sandi sebagai kunci Vernam Cipher sebelum sistem memulai proses enkripsi. Selain itu, halaman ini menampilkan informasi dalam format file yang didukung oleh sistem, seperti DOC, DOCX, XLS, dan PDF. File yang telah dienkripsi akan disimpan dengan ekstensi .enc di sistem setelah proses enkripsi selesai.



Gambar 10. Halaman Dekripsi File Admin dan Pegawai

Halaman dekripsi file digunakan oleh admin dan pegawai untuk mengembalikan file terenkripsi ke bentuk file asli. Di halaman ini, pengguna dapat memilih file berekstensi .enc dan memasukkan kata sandi yang sesuai sebelum sistem menjalankan proses dekripsi file menggunakan hybrid RSA dan Vernam Cipher. Halaman ini juga menunjukkan bahwa sistem hanya dapat menangani file dengan ekstensi .enc. File yang dihasilkan dari proses dekripsi akan disimpan kembali dengan nama file asli setelah proses tersebut selesai.

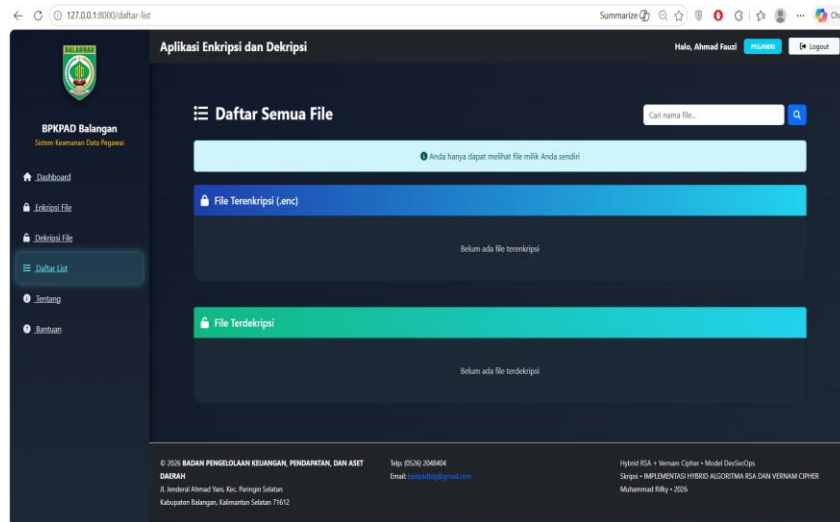


Gambar 11. Halaman Daftar List File Admin

Untuk melihat semua file yang telah dienkripsi dan didekripsi pada sistem, halaman daftar list file admin menampilkan informasi seperti nama, pemilik, dan tanggal file. Administrator juga dapat melakukan apa pun yang diperlukan untuk mengelola data, seperti mendownload dan menghapus file. Selain itu, halaman ini memisahkan daftar file terenkripsi dan file terdekripsi, sehingga administrator dapat melakukan pengawasan dan pengelolaan file pada sistem keamanan data pegawai. Sebagai bagian

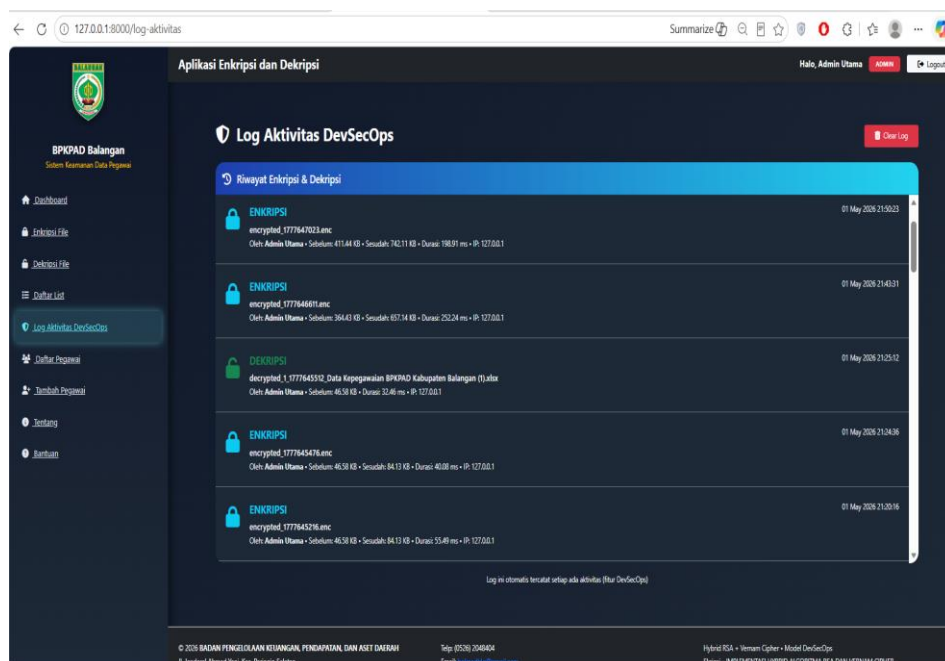


dari proses pengelolaan dan pengawasan keamanan sistem, administrator memiliki akses penuh ke semua file yang tersimpan pada aplikasi.



Gambar 12. Halaman Daftar List File Pegawai

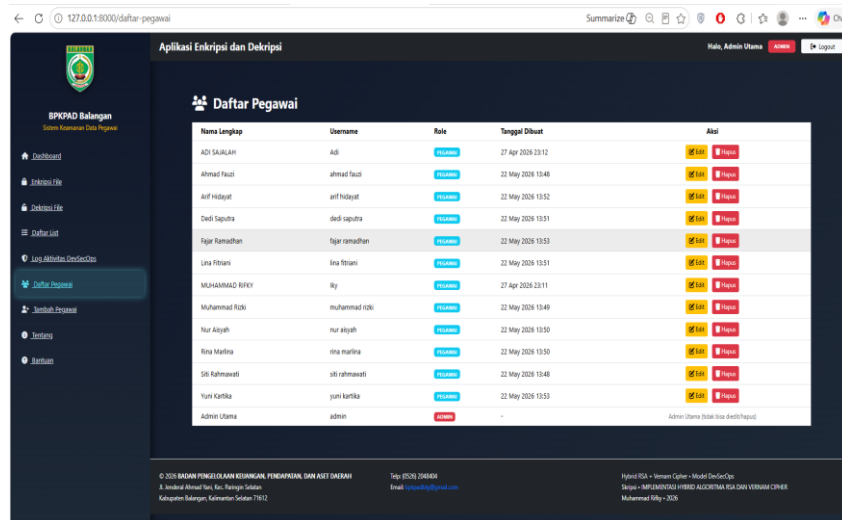
Halaman daftar list file digunakan untuk menampilkan file hasil enkripsi dan dekripsi pengguna. Pegawai dapat melakukan pencarian file sesuai kebutuhan pengguna dan melihat daftar file yang tersimpan pada sistem. Selain itu, sebagai bagian dari implementasi keamanan data pada aplikasi, sistem membatasi hak akses pengguna sehingga pengguna hanya dapat melihat file mereka sendiri. Mereka juga dapat melakukan proses download dan penghapusan file sesuai dengan hak akses yang diberikan oleh sistem.



Gambar 13. Halaman Log Aktivitas Admin

Seluruh riwayat aktivitas pengguna pada sistem keamanan data pegawai ditampilkan pada halaman log aktivitas admin. Administrator dapat melacak tindakan enkripsi dan dekripsi file yang dilakukan oleh pengguna secara otomatis sebagai bagian dari implementasi DevSecOps pada sistem. Selain itu, halaman log aktivitas menampilkan informasi seperti nama file, ukuran file sebelum dan sesudah

enkripsi, durasi proses, alamat IP pengguna, dan waktu aktivitas dilakukan. Dengan fitur ini, administrator dapat melakukan monitoring dan audit keamanan sistem secara lebih efisien.



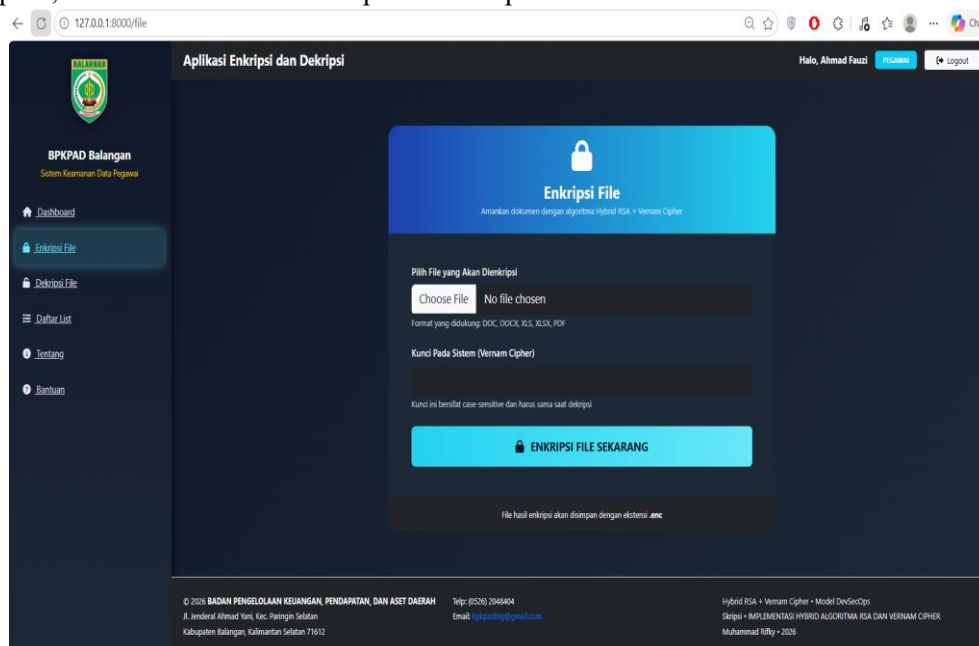
Gambar 14. Halaman Daftar Pegawai Admin

Halaman daftar pegawai admin menampilkan semua informasi pengguna, termasuk nama lengkap, username, peran, dan tanggal pembuatan akun. Selain itu, administrator dapat mengelola data pengguna seperti menambah, mengedit, dan menghapus data pegawai sesuai kebutuhan sistem. Fitur ini membantu administrator mengatur hak akses pengguna pada aplikasi keamanan data pegawai.

2. Implementasi Hybrid Algoritma RSA dan Vernam Cipher

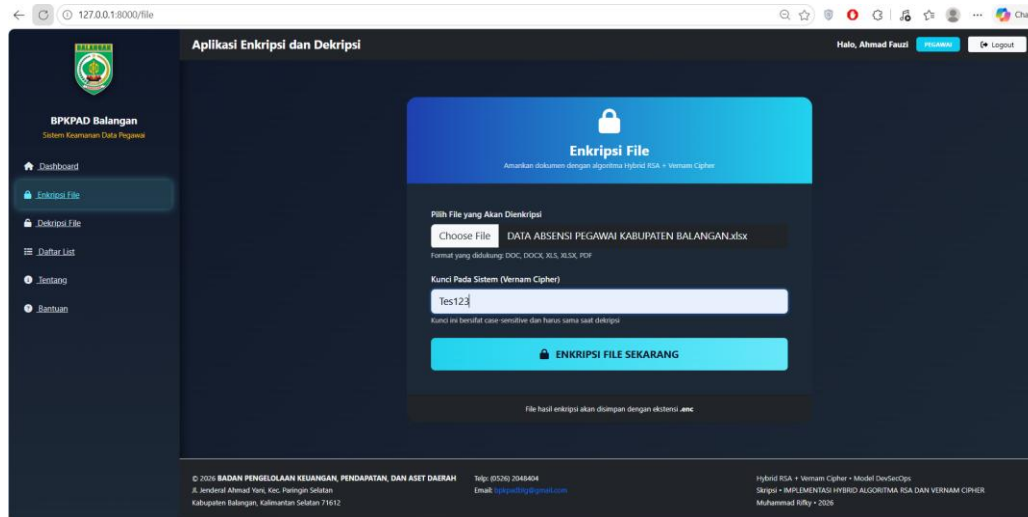
Implementasi Proses Enkripsi File

Sistem keamanan data pegawai menggunakan implementasi hybrid RSA dan Vernam Cipher untuk enkripsi file. Pengguna memilih file untuk dienkripsi, kemudian memasukkan kata sandi sebagai kunci Vernam Cipher, sebelum sistem memulai proses enkripsi.



Gambar 15. Halaman Enkripsi File

Pada tahap awal proses enkripsi, pengguna dapat mengakses halaman enkripsi file di sistem keamanan data pegawai. Di halaman ini, mereka dapat memilih file yang akan dienkripsi dengan hybrid RSA dan Vernam Cipher.



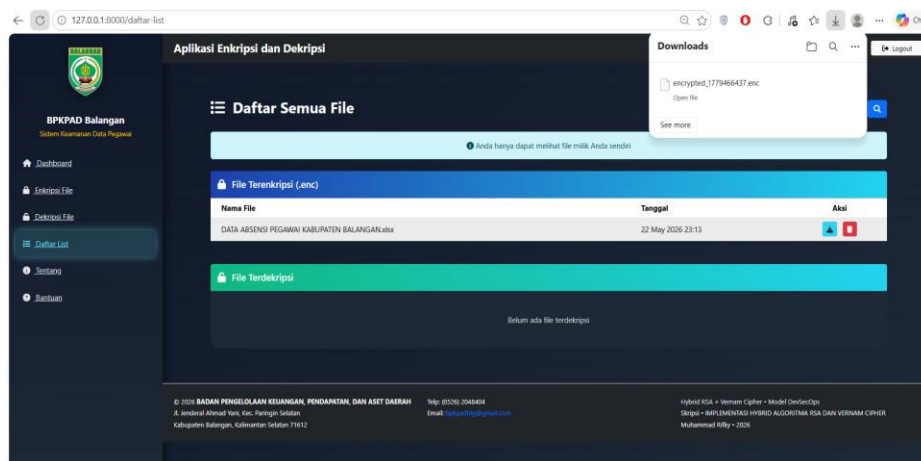
Gambar 16. Pemilihan File dan Input Password Vernam Cipher

Pada langkah ini, pengguna memilih file yang akan dienkripsi dan memasukkan kata sandi sebagai kunci Vernam Cipher. Kata sandi ini digunakan oleh sistem dalam proses pembentukan kunci XOR untuk membantu mengamankan ciphertext yang dihasilkan dari implementasi RSA.



Gambar 17. Proses Enkripsi Berhasil

Setelah enkripsi selesai, notifikasi akan ditampilkan oleh sistem. Selain itu, sistem secara otomatis membuat file dengan ekstensi .enc dan menyimpannya di folder penyimpanan sistem.



Gambar 18. File Hasil Enkripsi Pada Daftar List



Halaman daftar list file akan menampilkan file yang telah dienkripsi dengan sukses. Pada halaman ini, pengguna dapat melihat file yang tersimpan pada sistem dan melakukan proses download file sesuai kebutuhan.

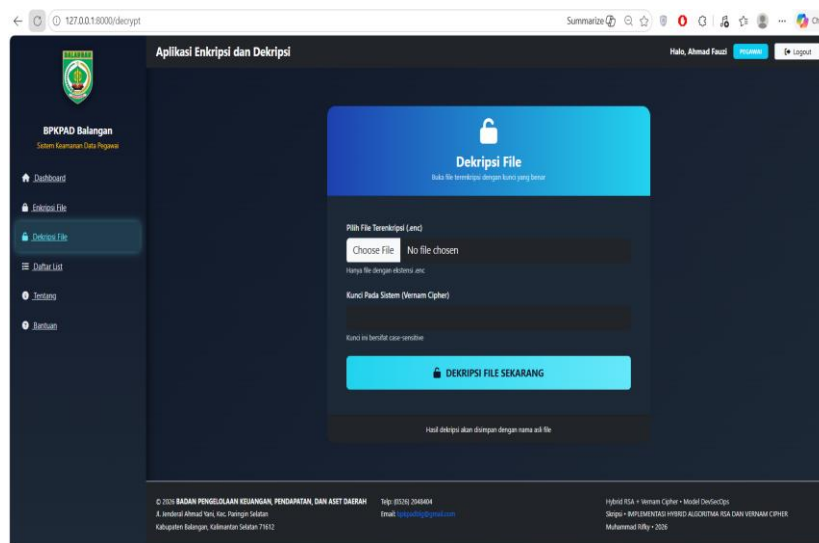
Name	Date modified	Type	Size
✓ Today			
 encrypted_1779466437.enc	22/05/2026 23:14	ENC File	21 KB

Gambar 19. File Ciphertext Berekstensi .enc

File ciphertext dengan ekstensi.enc yang dihasilkan oleh proses enkripsi adalah hasil dari implementasi kombinasi Cipher Vernam dan RSA, sehingga isi file tidak dapat dibaca secara langsung kecuali proses dekripsi menggunakan password yang tepat.

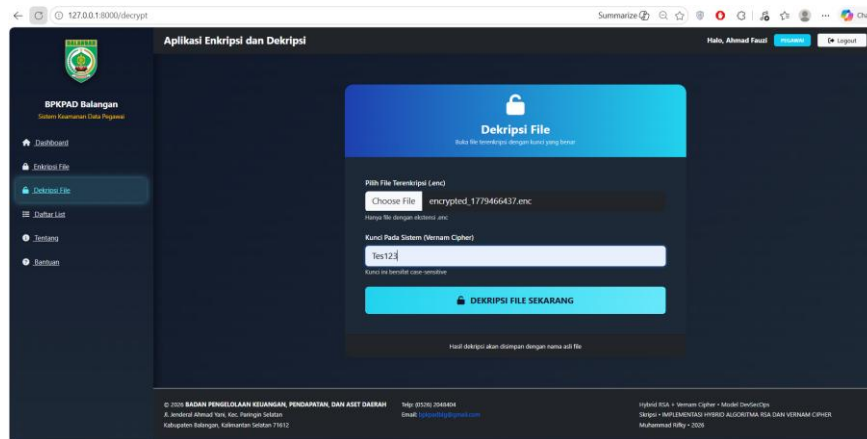
Implementasi Proses Dekripsi File

Dengan menggunakan implementasi hybrid RSA dan Vernam Cipher, proses dekripsi file mengembalikan file ciphertext ke bentuk file asli. Untuk melakukannya, pengguna memilih file dengan ekstensi.enc dan memasukkan kata sandi yang sama yang digunakan saat proses enkripsi.



Gambar 20. Halaman Dekripsi File

Pada awal proses dekripsi, pengguna dapat mengakses halaman dekripsi file dari sistem keamanan data pegawai. Di halaman ini, mereka dapat memilih file ciphertext yang akan dikembalikan ke bentuk file asli.



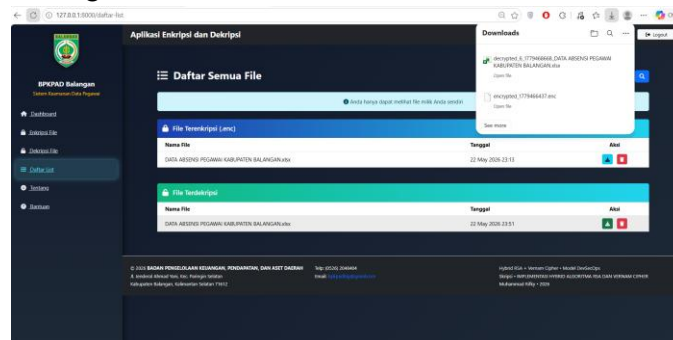
Gambar 21. Pemilihan File Ciphertext dan Input Password Vernam Cipher

Pada langkah ini, pengguna memilih file dengan ekstensi .enc dan kemudian memasukkan kata sandi Vernam Cipher yang digunakan saat proses enkripsi file. Kata sandi ini digunakan oleh sistem untuk membuka kembali ciphertext yang dihasilkan dari penggunaan hybrid RSA dan Vernam Cipher.



Gambar 22. Proses Dekripsi Berhasil

Setelah proses dekripsi selesai, pesan akan ditampilkan yang menunjukkan bahwa file telah dikembalikan ke bentuk asli. Selain itu, sistem secara otomatis menyimpan file hasil dekripsi pada folder penyimpanan sistem dengan nama file asli.



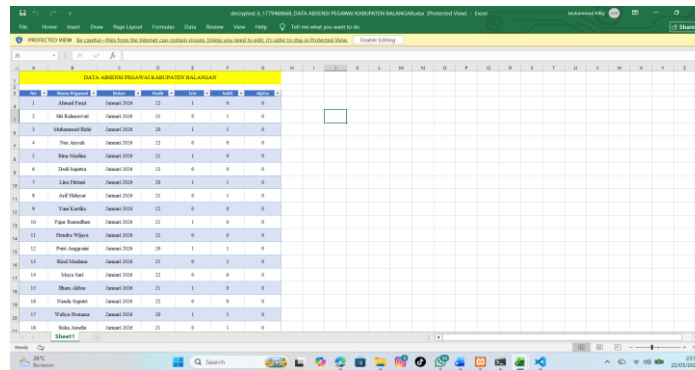
Gambar 23. File Hasil Dekripsi pada Daftar List

Halaman daftar list file akan menampilkan file hasil dekripsi yang berhasil diproses. Pada halaman ini, pengguna dapat melihat file hasil dekripsi dan melakukan proses download file sesuai kebutuhan mereka.

Name	Date modified	Type	Size
decrypted_6_1779470398_DATA SURAT TUGAS ...	23/05/2026 00:20	Microsoft Excel Work...	12 KB

Gambar 24. File Hasil Dekripsi

Hasil dari proses dekripsi adalah file asli yang dikembalikan dari file ciphertext yang berhasil diproses dengan hybrid RSA dan Vernam Cipher. Akibatnya, isi file dapat dibaca kembali dan digunakan oleh pengguna.



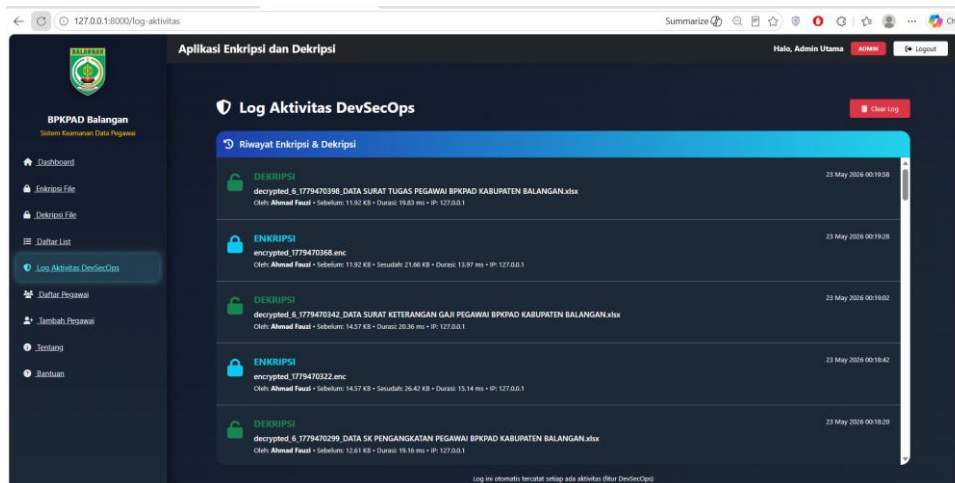
No	Nama Pegawai	Jenis Dokumen	Tanggal	Status	Kategori	Aksi
1	Alfred Faust	Surat Tugas	2026	1	0	0
2	Wibisono	Surat Tugas	2026	0	1	0
3	Muhammad Rizki	Surat Tugas	2026	0	1	0
4	Yusuf Alim	Surat Tugas	2026	0	0	0
5	Rita Nurhikmah	Surat Tugas	2026	0	1	0
6	Dedi Supriatna	Surat Tugas	2026	0	0	0
7	Indah Nurhikmah	Surat Tugas	2026	0	1	0
8	Andi Nurhikmah	Surat Tugas	2026	0	1	0
9	Yusuf Alim	Surat Tugas	2026	0	0	0
10	Pegawai Baru	Surat Tugas	2026	0	1	0
11	Yusuf Alim	Surat Tugas	2026	0	0	0
12	Pegawai Baru	Surat Tugas	2026	0	1	0
13	Yusuf Alim	Surat Tugas	2026	0	1	0
14	Yusuf Alim	Surat Tugas	2026	0	0	0
15	Yusuf Alim	Surat Tugas	2026	0	1	0
16	Yusuf Alim	Surat Tugas	2026	0	0	0
17	Wibisono	Surat Tugas	2026	0	1	0
18	Wibisono	Surat Tugas	2026	0	1	0

Gambar 25. Hasil File Setelah Dibuka

Dengan menggunakan aplikasi Microsoft Excel, file hasil dekripsi dapat dibuka kembali dengan sukses, menunjukkan bahwa proses dekripsi sistem berhasil mengembalikan file ciphertext ke bentuk data asli. Setelah menerima kata sandi dan ciphertext dari file, sistem secara otomatis menjalankan proses dekripsi hybrid Vernam Cipher dan RSA hingga file berhasil dikembalikan ke bentuk semula. Selama implementasi sistem, dekripsi dilakukan dengan membuka lapisan Vernam Cipher dengan kata sandi pengguna. Kemudian, hasil dekripsi Vernam diproses kembali menggunakan algoritma RSA, yang memungkinkan pemulihan file asli.

3. Implementasi DevSecOps

DevSecOps menerapkan sistem keamanan data pegawai melalui fitur pencatatan log aktivitas pengguna. Fitur ini mencatat semua aktivitas penting pengguna, seperti login dan logout, proses enkripsi dan dekripsi, upload file, dan pengelolaan file dalam aplikasi. Fitur log aktivitas memungkinkan administrator untuk memantau keamanan sistem dan audit aktivitas pengguna pada aplikasi keamanan data pegawai.



Riwayat Enkripsi & Dekripsi	Status	Tanggal	Aksi
DEKRIPSI decrypted_6_1779470398_DATA SURAT TUGAS PEGAWAI BPKPAD KABUPATEN BALANGKALAH User: Alfred Faust - Sebelum: 11.52 KB - Durasi: 19.83 ms - IP: 127.0.0.1	Selesai	23 May 2026 00:19:58	
ENKRIPSI encrypted_1779470398.enc User: Alfred Faust - Sebelum: 11.52 KB - Setelah: 21.66 KB - Durasi: 13.97 ms - IP: 127.0.0.1	Selesai	23 May 2026 00:19:58	
DEKRIPSI decrypted_6_1779470312_DATA SURAT KETERANGAN GAI PEGAWAI BPKPAD KABUPATEN BALANGKALAH User: Alfred Faust - Sebelum: 14.57 KB - Durasi: 30.35 ms - IP: 127.0.0.1	Selesai	23 May 2026 00:19:02	
ENKRIPSI encrypted_1779470312.enc User: Alfred Faust - Sebelum: 14.57 KB - Setelah: 26.42 KB - Durasi: 15.14 ms - IP: 127.0.0.1	Selesai	23 May 2026 00:18:42	
DEKRIPSI decrypted_6_1779470299_DATA SK PENGANGKATAN PEGAWAI BPKPAD KABUPATEN BALANGKALAH User: Alfred Faust - Sebelum: 10.41 KB - Durasi: 19.18 ms - IP: 127.0.0.1	Selesai	23 May 2026 00:18:29	

Gambar 26. Tampilan Halaman Log Aktivitas Admin

Pada halaman log aktivitas, semua aktivitas pengguna yang tercatat pada sistem ditampilkan. Jenis aktivitas, nama file, ukuran file, waktu proses, durasi proses, dan alamat IP pengguna ditampilkan. Ini adalah bagian dari implementasi monitoring keamanan berbasis DevSecOps.

4. Pengujian Enkripsi dan Dekripsi



Tabel 1. Pengujian Waktu Enkripsi dan Dekripsi

No	Kode File	Ukuran File Sebelum	Ukuran File Sesudah	Waktu Proses (ms)	Jenis Proses
1	F1	11.92 KB	21.66 KB	13.97	Enkripsi
2	F1	11.92 KB	11.92 KB	19.83	Dekripsi
3	F2	14.57 KB	26.42 KB	15.14	Enkripsi
4	F2	14.57 KB	14.57 KB	20.36	Dekripsi
5	F3	12.61 KB	22.89 KB	26.80	Enkripsi
6	F3	12.61 KB	12.61 KB	19.16	Dekripsi
7	F4	11.47 KB	20.83 KB	16.71	Enkripsi
8	F4	11.48 KB	11.48 KB	16.04	Dekripsi
9	F5	11.09 KB	20.15 KB	745.26	Enkripsi
10	F5	11.09 KB	11.09 KB	23.73	Dekripsi

Keterangan:

F1 = Data Surat Tugas Pegawai Bpkpad Kabupaten Balangan.Xlsx

F2 = Data Surat Keterangan Gaji Pegawai Bpkpad Kabupaten Balangan.Xlsx

F3 = Data Sk Pengangkatan Pegawai Bpkpad Kabupaten Balangan.Xlsx

F4 = Data Riwayat Pegawai Bpkpad Kabupaten Balangan.Xlsx

F5 = Data Absensi Pegawai Kabupaten Balangan.Xlsx

5. Pengujian Keamanan Sistem

Tabel 2. Pengujian Keamanan Sistem

No	Pengujian	Hasil Yang Diharapkan	Hasil
1	Membuka file ciphertext secara langsung	File tidak dapat dibaca	Berhasil
2	Dekripsi dengan password salah	File gagal didekripsi	Berhasil
3	Dekripsi dengan password benar	File berhasil dikembalikan	Berhasil
4	Akses file oleh pengguna lain	Sistem menolak akses	Berhasil
5	Monitoring aktivitas pengguna	Aktivitas tercatat di log	Berhasil

Hasil pengujian keamanan sistem menunjukkan bahwa file yang telah dienkripsi tidak dapat dibaca secara langsung kecuali password yang tepat digunakan untuk mendekripsinya. Selain itu, sistem memiliki kemampuan untuk membatasi akses pengguna dan mencatat aktivitas mereka melalui fitur log aktivitas.

6. Pengujian DevSecOps

Pengujian DevSecOps dilakukan untuk mengetahui bagaimana menjalankan sistem keamanan data pegawai untuk memantau dan melacak aktivitas pengguna.

Tabel 3. Pengujian DevSecOps

No	Aktivitas	Hasil Yang Diharapkan	Hasil
1	Login pengguna	Aktivitas login tercatat	Berhasil



2	Login pengguna	Aktivitas logout tercatat	Berhasil
3	Enkripsi file	Aktivitas enkripsi tercatat	Berhasil
4	Dekripsi file	Aktivitas dekripsi tercatat	Berhasil
5	Upload file	Aktivitas upload tercatat	Berhasil

SIMPULAN DAN SARAN

Penelitian ini berhasil mengimplementasikan sistem keamanan data pegawai berbasis web menggunakan hybrid algoritma RSA dan Vernam Cipher yang diintegrasikan dengan model DevSecOps pada BPKPAD Kabupaten Balangan. Sistem yang dikembangkan mampu mendukung proses pengamanan data melalui fitur autentikasi pengguna, pengelolaan file, proses enkripsi dan dekripsi, serta pencatatan aktivitas pengguna. Hasil implementasi menunjukkan bahwa kombinasi algoritma RSA dan Vernam Cipher dapat meningkatkan kerahasiaan data, di mana file yang telah dienkripsi tidak dapat dibaca secara langsung dan hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan mekanisme autentikasi yang sesuai. Selain itu, penerapan model DevSecOps berhasil mendukung aspek keamanan sistem melalui fitur *logging* dan *monitoring* aktivitas pengguna, sehingga administrator dapat melakukan pengawasan serta audit terhadap aktivitas sistem secara lebih efektif. Berdasarkan hasil implementasi dan pengujian, sistem yang dikembangkan mampu mendukung pengamanan data pegawai secara lebih aman, terintegrasi, dan sesuai dengan kebutuhan BPKPAD Kabupaten Balangan.

Pengembangan penelitian selanjutnya dapat dilakukan dengan menambahkan dukungan terhadap lebih banyak format dokumen sehingga sistem dapat digunakan pada berbagai jenis file. Selain itu, implementasi algoritma kriptografi lain dapat dipertimbangkan untuk membandingkan tingkat keamanan maupun efisiensi waktu proses enkripsi dan dekripsi. Dari sisi DevSecOps, sistem juga dapat dikembangkan dengan menambahkan fitur pemantauan keamanan secara *real-time*, notifikasi otomatis terhadap aktivitas mencurigakan, serta integrasi dengan mekanisme analisis log yang lebih komprehensif guna meningkatkan efektivitas pengawasan dan keamanan sistem secara berkelanjutan.

DAFTAR PUSTAKA

- Abi Assyarif, R., Eka Yulastuti, G., & Nurina Prabiantissa Institut Teknologi Adi Tama Surabaya, C. (2023). *Implementasi Kombinasi Algoritma Rot13 dan Vernam Cipher untuk Keamanan Data Teks*.
- Afiifah, K. ', Fira Azzahra, Z., & Anggoro, A. D. (2022). Universitas Negeri Jakarta; Jl. Rawamangun Muka Raya No.11 RW.14 Rawamangun. *JURNAL INTECH*, 3(2), 18–22.
- Al Farizi, M., & Voutama, A. (2026). Implementasi UML Dalam Sistem Penjualan Sepatu MAF Clobber Berbasis Website. *Jurnal Ilmiah Sistem Informasi*, 5(1), 543–562. <https://doi.org/10.51903/gqfza719>
- Andara, H., & Damayanti, F. (2022). *Implementasi Kriptografi Hybrida Algoritma RSA dan Vernam Cipher Dalam Pengamanan File Text*.
- Dharma Putra, E., Hafiz Zachary, E., Thariq Izaz, M., & Arif Fadilah, N. (2024). Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya. *Journal of Information and Information Security (JIFORTY)*, 5(2), 88955882. <http://ejurnal.ubharajaya.ac.id/index.php/jiforty>



- Diba Tanzilla, F., Hanita, M., & Widiawan, B. (2023). *Keamanan Siber di Indonesia Pasca Pembentukan Personal Hukum Perlindungan Data*. 40(2), 164–170. www.onlinedoctranslator.com
- Gultom, J. M. (t.t.). Indra Gunawan 2) , Ika Okta Kirana 3) , Poningsih 4) , Irawan 5) 1,2,3) STIKOM Tunas Bangsa Jl. Jend. Sudirman Blok A, 11(2), 21127.
- Gultom, J. M. (2021). Indra Gunawan 2) , Ika Okta Kirana 3) , Poningsih 4) , Irawan 5) 1,2,3) STIKOM Tunas Bangsa Jl. Jend. Sudirman Blok A, 11(2), 21127.
- Jinan, A., Siregar, M. P., Suryani, D. F., Muis, A., & Gunung, T. M. R. (2025). Optimasi Implementasi Kriptografi Kunci Publik dalam Meningkatkan Keamanan dan Otentikasi Data pada Sistem Informasi Kampus. *Digital Transformation Technology*, 5(2), 1–9. <https://doi.org/10.47709/digitech.v5i2.6425>
- Khudzaifah, M., Ma'rifah, S. H., & Fahmi, H. (2023). *Implementation of Rubik's Cube Algorithm and Rivest-Shamir-Adleman (RSA) Algorithm on Iris Digital Image Security* (hlm. 312–323). https://doi.org/10.2991/978-94-6463-148-7_31
- Kshetri, N., Rahman, M. M., Osama, O. F., & Hutson, J. (t.t.). *algoTRIC: Symmetric and asymmetric encryption algorithms for Cryptography-A comparative analysis in AI era*.
- Liana, L., Zarlis, M., & Tulus, T. (2023). Hybrid Cryptosystem Analysis RSA Algorithm And Triple DES Algorithm. *Sinkron*, 8(3), 1461–1473. <https://doi.org/10.33395/sinkron.v8i3.12467>
- Listia, H., Enkripsi, A., Deskripsi, D., Menggunakan, T., Chiper, V., Web, B., Wardaniah, S., & Indra, Z. (t.t.). *JETBUS Journal of Education Transportation and Business*.
- Mahandis Shama, A., & Chandra, D. W. (t.t.). *Abriza Mahandis Shama Implementasi Static Application Security Implementasi Static Application Security Testing Menggunakan Jenkins CI/CD Berbasis Docker Container Pada PT. Emporia Digital Raya*.
- Mohammed, K. I., Shanmugam, B., & El-Den, J. (2025). Evolution of DevSecOps and Its Influence on Application Security: A Systematic Literature Review. Dalam *Technologies* (Vol. 13, Nomor 12). Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/technologies13120548>
- Muhamad Sabilal Karim, R., Khudzaifah, M., & Rozi, F. (2025). Studi Komparatif Algoritma RSA dan AES pada Enkripsi dan Dekripsi Citra Digital. *Jurnal Riset Mahasiswa Matematika*, 4(2), 74–81. <https://doi.org/10.18860/jrmm.v4i2.31191>
- Mulyadi, D., Mulyana, A., Carmenita, A., Utami, H. L., Almira Aulia, K., Putri, M., & Rahma Alia, N. (2026). Implementasi Kebijakan Pemerintah terhadap Pencegahan Kebocoran Data Pribadi dalam Pelayanan Publik Berbasis Digital. *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora*, 6(1), 15. <https://doi.org/10.53697/iso.v6i1.3473>
- Nesterenko, M., & Posta, S. (2025). *Qusicryslals in Vernam cipher*. <http://arxiv.org/abs/2502.10468>
- Pemesanan Bibit Ternak pada BPSI UAT, A., Nanda Rahmat Herlambang, D., & Pravitasari, N. (2024). Penerapan Kriptografi AES untuk Keamanan Data. *Remik: Riset dan E-Jurnal Manajemen Informatika Komputer*, 8(1). <https://doi.org/10.33395/remik.v8i1.13157>
- Pengaman, A., Digital, D., Algoritma, M., Hybrid, K., Kompresi, A., Febri Dwinata, H., #1, Y., Nasution, H., & Priyanto, H. (2021). *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*.
- Perkasa, P. R., & Mailoa, E. (2023). Adopsi Devsecops Untuk Mendukung Metode Agile Menggunakan Trivy Sebagai Security Scanner Docker Image Dan Dockerfile. *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, 4(3), 856–863. <https://doi.org/10.35870/jimik.v4i3.291>
- Persetujuan Bersama, D. (t.t.). *Fresiden Republik Indonesia 2-Dewan Perwakilan Rakyat Republik Indonesia Dan Presiden Republik Indonesia*.



- Purnama, L., Iskandar Mulyana, D., Maulana, Y., Okta, E., & Sulaiman, P. (2022). Implementasi Algoritma One Time Menggunakan Algoritma Cipher Transposition Sebagai Pengamanan Rahasia Pesan. *Jurnal Informatika dan Teknologi Komputer*, 03(1), 40–48. <https://ejurnalunsam.id/index.php/jicom/>
- Rahman, R., & Chaerul Ghazali, M. (2024). Merancang dan Menerapkan Sistem Keamanan Jaringan untuk Jaringan Nirkabel. *Jurnal Ilmiah Multidisiplin*, 2(7), 677–682. <https://doi.org/10.5281/zenodo.12952735>
- Riaunaldy Hisyam, F., & Kartika Dini, S. (2023). Persepsi Aparatur Sipil Negara (ASN) Kabupaten Sleman Terhadap Keamanan Data Pribadi dengan Metode Statistika Deskriptif. *Emerging Statistics and Data Science Journal*, 1(3).
- Siregar, M. N. H., & Mardiah. (2025). Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001. *Jurnal Ilmu Komputer dan Teknik Informatika*, 1(2), 58–64. <https://doi.org/10.64803/juikti.v1i2.52>
- Suseno, A., & Sulistiyowati, N. (2021). *STRING (Satuan Tulisan Riset dan Inovasi Teknologi) Analisis Peningkatan Hybrid Cryptosystem Untuk Enkripsi Dan Dekripsi Menggunakan Vigenere Cipher Dan Rsa Pada Text*.
- Togar Timoteus Gultom. (2021). Penerapan Algoritma Hybrid Affine Cipher dan RSA Terhadap Sistem Keamanan. *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, 1(1), 1–6. <https://doi.org/10.54259/satesi.v1i1.1>
- Undang-Undang Nomor 27 Tahun 2022. (2022). *Presiden Republik Indonesia 2-Dewan Perwakilan Rakyat Republik Indonesia Dan Presiden Republik Indonesia*.
- Wenhua, Z., Kamrul Hasan, M., Ismail, A. F., Yanke, Z., Razzaque, M. A., Islam, S., & Anil kumar, B. (2023). Data security in smart devices: Advancement, constraints and future recommendations. Dalam *IET Networks* (Vol. 12, Nomor 6, hlm. 269–281). John Wiley and Sons Inc. <https://doi.org/10.1049/ntw2.12091>