Jurnal Komputasi Terdistribusi

Vol. 9 No.6, Juni 2026
ISSN: 27224707

EKSPLORASI *CLIENT-SIDE* ENCRYPTION MENGGUNAKAN *EXTENDED VIGENERE CIPHER* DAN KUNCI DINAMIS PADA SISTEM MANAJEMEN ARSIP PEMERINTAH BERBASIS *GOOGLE CLOUD ECOSYSTEM*

Juni Agung Prasetiyo[1], Margiyono[2], Ahsanul Fikri[3], Eka Ardhianto[4], Aji Supriyanto[5]
Program Studi Teknologi Informsi, Fakultas Teknologi Informasi Dan Industri, Universitas Stikubank, Semarang, Indonesia
E-mail: juniagung0033@mhs.unisbank.ac.id[1], margiyono0031@mhs.unisbank.ac.id[2], ahsanulfikri7012@mhs.unisbank.ac.id[3], ekaardhianto@edu.unisbank.ac.id[4], ajisup@edu.unisbank.ac.id[5]

ABSTRAK

Kemajuan teknologi mendorong instansi pemerintah beralih ke pengelolaan arsip elektronik berbasis public cloud seperti Google Spreadsheet. Namun, penyimpanan konvensional ini umumnya masih berbasis teks biasa (plaintext), sehingga rentan terhadap intersepsi jaringan, akses ilegal, maupun ancaman internal (insider threat) dari penyedia layanan. Penelitian ini bertujuan untuk merancang skema keamanan Client-Side Encryption (CSE) guna melindungi dokumen dinas berkategori tertutup pada Sistem Manajemen Arsip Pemerintah. Metode yang diusulkan mengombinasikan algoritma Extended Vigenere Cipher berbasis Modulo 75 (Mod 75) dengan skema Kunci Dinamis (Dynamic Key) yang mengintegrasikan Master Key dan salt kontekstual berupa Kode Klasifikasi Berkas. Proses kriptografi diimplementasikan penuh di sisi browser pengguna (client-side) menggunakan Google Apps Script dan JavaScript sebelum data ditransmisikan ke database. Hasil pengujian empiris menunjukkan bahwa sistem berhasil melakukan enkripsi kondisional secara otomatis dan menghancurkan pola periodisitas kunci statis pada Vigenere klasik. Perluasan ruang karakter menjadi Modulo 75 sukses memfasilitasi penyandian karakter campuran khas dokumen kedinasan sekaligus meningkatkan kompleksitas ruang kunci (keyspace) hingga 7521 pada panjang kunci efektif 21 karakter. Penelitian ini berhasil mewujudkan model Zero-Knowledge Architecture secara mutlak, memosisikan Google Spreadsheet murni sebagai Blind Storage, serta menjamin perlindungan forward secrecy yang aman secara komputasi (computationally infeasible) dari serangan Brute Force maupun analisis frekuensi.

Kata Kunci : Blind Storage, Client-Side Encryption, Kunci Dinamis, Extended Vigenere Cipher, Zero-Knowledge Architecture.

ABSTRACT

Advances in technology have driven government agencies to shift toward electronic archive management based on public clouds like Google Sheets. However, this conventional cloud storage typically stores data in plaintext, making it vulnerable to network interception, unauthorized access, and insider threats from cloud providers. This study aims to design a Client-Side Encryption (CSE) security framework to protect restricted government documents within an Archive Management System. The proposed method combines a Modulo 75 (Mod75) Extended Vigenere Cipher with a Dynamic Key generation scheme that concatenates a Master Key and a contextual salt derived from the Archive Classification Code. The cryptographic process is executed entirely on the user's browser (client-side) using Google Apps Script and JavaScript

before the data is transmitted to the database. Empirical testing results demonstrate that the system successfully performs automatic conditional encryption and shatters the key periodicity patterns inherent in the classical Vigenere cipher. Expanding the character space to Modulo 75 accommodates the complex character mix of official government documents while exponentially increasing the keyspace complexity to 7521 for an effective 21-character key length. This research successfully achieves a complete Zero-Knowledge Architecture, shifting Google Sheets purely into a Blind Storage medium and ensuring computationally infeasible forward secrecy against both Brute Force attacks and frequency analysis.
Keywords: *Blind Storage, Client-Side Encryption, Kunci Dinamis, Extended Vigenere Cipher, Zero-Knowledge Architecture.*

PENDAHULUAN

Arsip adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa, dan bernegara. Kemajuan teknologi informasi telah mengubah paradigma pengelolaan arsip di instansi pemerintahan. Tuntutan akan pelayanan publik yang cepat, transparan, dan akuntabel membuat sistem kearsipan berbasis kertas semakin tidak relevan karena prosesnya lambat, membutuhkan ruang besar, dan berisiko menimbulkan kehilangan data. Arsip memiliki peran penting tidak hanya sebagai dokumen administratif, tetapi juga sebagai dasar bukti legal dan pengambilan keputusan [1]. Dalam Pengelolaan Arsip Elektronik, Pemerintah dianjurkan untuk menerapkan Metode Keamanan yang telah diatur oleh Arsip Nasional RI memanfaatkan perkembangan teknologi informasi khususnya di bidang Keamanan Siber salah satunya dengan menerapkan Public key infrastructure yaitu teknologi untuk enkripsi arsip Elektronik yang menjamin keamanan transmisi arsip ke pihak lain[2].

Di bidang Keamanan Siber, dikenal sebuah istilah yaitu kriptografi. Kriptografi adalah teknik mengamankan informasi dengan cara menghilangkan makna pesan membiarkan data terenkripsi terlihat melalui proses enkripsi-deskripsi menggunakan kunci[3]. Kriptografi berperan penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data di era digital yang ditandai oleh pertukaran informasi besar-besaran melalui jaringan dan layanan cloud. Berbagai sektor seperti pemerintahan, kesehatan, hingga layanan desa bergantung pada mekanisme keamanan yang andal untuk mencegah penyadapan, manipulasi, dan akses tidak sah terhadap data sensitif[4]. Dalam konteks Cloud Computing, kekhawatiran utama adalah perpindahan data ke infrastruktur pihak ketiga yang berpotensi menimbulkan kebocoran data dan hilangnya kendali pengguna terhadap informasi yang disimpan[5].

Cloud computing menyediakan kemudahan akses dan skala penyimpanan, namun membuka tantangan serius terkait serangan peretasan, akses tidak sah, serta kelemahan pada kebijakan enkripsi dan kontrol akses[6]. Untuk mengurangi risiko tersebut, pendekatan client-side encryption yakni enkripsi data di sisi pengguna sebelum dikirim ke server dipandang mampu menambah lapisan perlindungan karena penyedia layanan tidak pernah melihat plaintext dan tidak memegang kunci dekripsi[7]. Google Cloud Ecosystem membentuk sebuah ekosistem layanan terintegrasi untuk menyimpan, memproses, mengamankan, dan menganalisis data sepenuhnya di dalam infrastruktur Google, tanpa harus keluar dari cloud. Google Cloud Ecosystem mengenkripsi semua data client dengan AES-256/128 dalam mode CBC, GCM, atau CTR data dipecah menjadi chunk, tiap chunk punya kunci dan tag unik, disebar ke banyak lokasi untuk mengurangi risiko kompromi tunggal. Google Cloud Ecosystem menyediakan kontrol akses, enkripsi, dan perlindungan

malware untuk arsip digital, sekaligus fitur kolaborasi dan pencarian cerdas[10].

Di sisi lain, algoritma klasik seperti Vigenere cipher masih banyak dikaji sebagai dasar skema enkripsi teks, basis data, maupun citra digital, namun kelemahannya terhadap analisis frekuensi dan penggunaan kunci berulang mendorong berbagai modifikasi[8]. Beragam penelitian mengusulkan perluasan himpunan karakter (tabel 95×95 atau extended ASCII), kombinasi dengan algoritma lain (Caesar, SHA-256, ElGamal), serta pembangkit kunci acak/dinamis menggunakan CSPRNG, Blum Blum Shub, RSA, grup simetri, hingga LCG untuk meningkatkan kerandoman kunci dan menyulitkan kriptanalisis[9].

Perkembangan tersebut menunjukkan kecenderungan menuju skema Vigenere termodifikasi dengan kunci dinamis sebagai bagian dari sistem Hybrid Cryptography yang diterapkan pada berbagai konteks penyimpanan dan pengelolaan data, termasuk basis data kependudukan, informasi desa, citra digital, hingga dokumen dokumen PDF/DOCX/XLSX. Dalam ekosistem cloud, menggabungkan enkripsi sisi klien dengan algoritma Vigenere yang diperluas dan pembangkit kunci dinamis berpotensi memberikan solusi yang seimbang antara keamanan, fleksibilitas karakter, dan kemudahan implementasi pada sistem manajemen arsip berbasis layanan cloud.

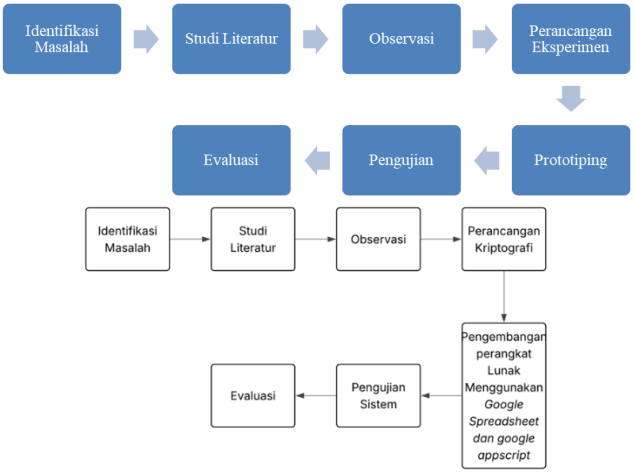
Penelitan ini bertujuan untuk merancang Client-Side Encryption mengunakan Extended Vigenere Cipher dan Kunci Dinamis pada Sistem Manajemen Arsip Pemerintah dengan memanfaatkan Google Spreadsheet dan ekstensi Google Appscript yang termasuk dalam Google Cloud Ecosystem. Harapannya dengan Extended Vigenere Cipher dan Kunci Dinamis, arsip yang sifatnya tertutup menurut Peraturan Arsip Nasional RI tentang Pengelolaan Arsip Digital tidak disalahgunakan oleh pihak ketiga yang tidak bertanggung jawab.

METODE PENELITIAN

Metodologi penelitian ini dirancang untuk memberikan alur yang sistematis dalam memodifikasi algoritma, merancang arsitektur sistem, hingga menguji tingkat keamanan data pada pada penelitian ini.

Alur Penelitian

Penelitian ini mengadopsi model Waterfall yang dimodifikasi untuk pengembangan perangkat lunak keamanan, meliputi tahapan sebagai berikut:



Gambar. Alur Penelitian

Penelitian ini diawali dengan identifikasi masalah dilapangan dan mengidentifikasi regulasi kearsipan terkait dokumen tertutup dan memetakan struktur Daftar Arsip pada Instansi Pemerintah, mengidentifikasi celah keamanan ada penyimpanan cloud berbasis

Google Spreadsheet yang sedang trend digunakan instansi pemerintah dimana data masih tersimpan dalam bentuk teks biasa sehingga rentan terhadap akses ilegal atau kebocoran data. Dilanjutkan dengan Studi Literatur penelitian-penelitian sebelumnya yang membahas tentang Client-Side Encryption, Extended Vigenere Cipher, Kunci Dinamis, dan Google Cloud Ecosystem. Langkah berikutnya dilakukan observasi ke Perangkat Daerah Pemerintah yang menangani urusan kearsipan.

HASIL DAN PEMBAHASAN

Hasil Implementasi Arsitektur Client-Side Encryption (Cse)

Arsitektur Client-Side Encryption (CSE) adalah mekanisme di mana proses enkripsi dan dekripsi data dilakukan sepenuhnya di sisi pengguna (client), bukan di server. Hal ini memastikan bahwa penyedia layanan cloud tidak memiliki akses ke kunci enkripsi maupun isi data, sehingga privasi pengguna lebih terjaga.

Penelitian ini berhasil mengimplementasikan prototipe sistem manajemen arsip dengan model arsitektur Client-Side Encryption (CSE) yang terintegrasi pada Google Cloud Ecosystem (Google Apps Script dan Google Sheets).

Perbedaan mendasar antara sistem konvensional dengan arsitektur Client-Side Encryption (CSE) yang dibangun terletak pada lokasi proses kriptografi dijalankan. Pada sistem manajemen arsip dinas umumnya, data dikirim dalam bentuk teks biasa (plaintext) melalui jaringan menuju cloud server, baru kemudian dienkripsi oleh penyedia layanan (Google). Hal tersebut menyisakan celah keamanan berupa insider threat (admin cloud) atau intersepsi di tengah jalan.

Pada sistem yang diusulkan, mesin enkripsi berbasis JavaScript dieksekusi langsung pada browser pengguna (client side). Sebelum data meninggalkan komputer pengguna untuk disimpan ke Google Sheets melalui Google Apps Script, teks dokumen telah berubah menjadi ciphertext.

Hasil Pengujian Kondisional Akses Arsip

Sistem yang dibangun dari hasil penelitian ini diuji menggunakan skenario memisahkan antara data Arsip Terbuka dan Arsip Tertutup Hasil Pencatatan Data ditunjukkan pada Tabel 1.

Tabel 1. Log Record Penyimpanan Google Spreadsheet

Kode Arsip	Judul Arsip	Status	Isi Arsip Terenkripsi
200.1.2.3	Bela Negara	Terbuka	Apel besar HUT Kab. Semarang ke -504 Tahun 2025
200.1.2.1	Ketahanan Ideologi Negara	Tertutup	V9(& 9C1A29DOPVQQJKs5-* %
400.1.2.2	Fasilitasi Kesehatan PengembanganSumber Daya	Tertutup	o*#FJi*1EEH0NBX2ZGx9& CA%1A4KEcFRCdCy
400.7.3.6	Pelayanan pasien jaminan kesehatan	Tertutup	a9!&Q9C1A4PAcPOQ.Pl^9E*_p,&WEHKaKQ
400.8	Agama dan Kepercayaan	Terbuka	Kegiatan silaturahmi Ulama - Umaro ke 309 BAZNAS tingkat Kab. Semarang
500.12.6.4	Aplikasi Layanan Kepemerintahan	Tertutup	09&DA_I1#S01 .2^-A%5Yf
500.14	Data Statistik	Terbuka	ekspose dan publikasi buku-buku statistik sektoral
500.14.3.3	Pelaksanaan Lapangan, Antara lain: Pelaksanaan listing, Pemilihan sampel,	Tertutup	09@*A_%1A5REUPQOQND3@a)*_p@&YADKUE.VdD4 @*KA*

Kode Arsip	Judul Arsip	Status	Isi Arsip Terenkripsi
400.14.8	Pengumpulan data, Pemeriksaan, Pengawasan Lapangan, Monitoring kualitas Penerbitan Majalah, buletin, koran dan jurnal	Terbuka	Surat pengantar majalah gema serasi edisi I Tahun 2025
400.14.5.4	Hubungan dengan Perguruan Tinggi/ sekolah, termasuk magang, Pendidikan Sistem Ganda (PSG) / Praktek Kerja Lapang (PKL)	Tertutup	09#-*_I1E4PRKLXSP.Wt++&s12lnAIDiB4 WKNlevE=9G1A

Pada Tabel 1. menunjukkan bahwa sistem berhasil melakukan enkripsi kondisional. Pada Baris 1, data tetap berwujud plaintext karena berstatus "Terbuka". Hal ini menjaga performa sistem agar tidak membuang daya komputasi untuk data publik. Pada Data Arsip yang sifatnya Tertutup, dilakukan pengujian menggunakan kunci yang sama (“Kearsipan”) namun kode arsip berbeda. Berdasarkan hasil akhir, kolom Isi Arsip Terenkripsi string acak yang berbeda. Hal ini membuktikan fungsi penggabungan kunci dinamis dengan kode klasifikasi arsip berhasil mematahkan analisis frekuensi di tingkat Google Cloud Ecosystem.

Proses enkripsi Extended Vigenere Cipher dan Kunci Dinamis diuji dari data Tabel 1 Baris ke 10, dijelaskan sebagai berikut :

$$K_{dynamic} = K_{master} \,||\, K_{salt}$$

$$K_{dynamic} = Kearsipan \,||\, 400.14.5.4$$

$$K_{dynamic} = Kearsipan400.14.5.4$$

Melalui skema ini, panjang kunci efektif meningkat dari 9 karakter menjadi 21 karakter. Kunci dinamis inilah yang akan diulang (looping) secara berkala sepanjang ukuran teks asli (plaintext) untuk mematahkan metode kriptanalisis analisis frekuensi (Kasiski Examination).

Proses enkripsi dilakukan dengan memetakan setiap karakter plaintext (Pi) dan karakter kunci dinamis (Ki) ke dalam indeks integer berdasarkan himpunan karakter terurut (CHARSET) dengan ukuran Modulus 75 yang ditanam pada sistem sebagai berikut :

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789.,!@#$%^&*()_+-="

Untuk membuktikan keabsahan algoritma, berikut adalah simulasi perhitungan matematis terhadap kata ”Pengantar(spasi)” dari data Tabel 1 Baris ke 10 menggunakan rumus Extended Vigenere Cipher, dijelaskan pada Tabel 2.

Tabel 2. Perhitungan Extended Vigenere Cipher dan Kunci Dinamis

P_i	Indeks P_i	K_i	Indeks K_i	Indeks Hasil (C_i)	C_i
P	42	K	11	53	0
E	31	a	27	58	9
n	40	r	44	9	#
g	33	s	45	3	-
a	27	i	35	62	*
n	40	p	42	7	-

t	46	a	27	73	I
a	47	n	40	67	1
r	44	4	52	21	E
(spasi)	0	0	48	48	4

Analisis Ketahanan Algoritma Extended Vigenere Cipher Dan Kunci Dinamis

Untuk memvalidasi peningkatan performa keamanan dari Algoritma Extended Vigenere Cipher dan Kunci Dinamis, dilakukan studi komparatif terhadap beberapa penelitian-penelitian sebelumnya yang mengkaji optimasi Vigenere Cipher.

Penggunaan kunci statis membuat sistem rentan apabila panjang dokumen sangat besar, karena perulangan kunci akan membentuk pola simetris[13]. Sementara itu, penelitian lain menggunakan metode Autokey dimana potongan plaintext digunakan sebagai kunci berikutnya. Kelemahan Autokey adalah jika peretas berhasil menebak satu kata di awal, maka seluruh sisa dokumen akan runtuh secara berantai (cascade effect)[15]. Penelitian yang menggunakan M = 26 terbukti gagal di lingkungan administrasi karena tidak mampu mengamankan data-data yang vital. Kemudian penelitian lain memperbarui menggunakan M = 95 dimana karakter-karakter kontrol seperti Enter, Tab atau Null dimasukkan, namun hal ini justru seringkali menyebabkan error rendering data atau corrupt saat teks disimpan ke dalam database cloud berbasis web. Mayoritas penelitian Vigenere terdahulu berbasis offline atau server-side. Pada arsitektur server-side, data dikirim dalam bentuk teks asli ke server terlebih dahulu baru dienkripsi. Hal ini tidak aman untuk implementasi cloud public karena data dapat diintersep di jaringan atau diintip oleh admin penyedia cloud.

Pada penelitian ini mekanisme kunci menggunakan salt kontekstual memanfaatkan kode klasifikasi. Karena salt berubah di setiap baris data, periodisitas kunci hancur total tanpa perlu bergantung pada isi teks asli. Penggunaan M = 75 yang bersifat selektif hanya memuat karakter yang valid digunakan dalam dokumen administrasi pemerintah (Huruf, Angka, Spasi, dan 12 Simbol Inti). Pendekatan ini menjamin data 100% aman terenkripsi namun tetap kompatibel, ringan, dan stabil saat ditransmisikan ke dalam Google Cloud Ecosystem. Penerapan Client-Side Encryption dengan Google Appscript membuktikan peningkatan level privasi di mana Google Spreadsheet bertindak murni sebagai Blind Storage, sebuah konsep yang belum dieksplorasi pada tiga penelitian Vigenere cipher sebelumnya.

Untuk menguji ketahanan algoritma pada penelitian ini, digunakan perhitungan total variasi kombinasi pada Keyspace yang ditentukan oleh rumus berikut :

Keyspace = ML

Maka untuk membuktikan ketahanan algoritma pada penelitian dilakukan analisis komparatif dengan penelitian sebelumnya menggunakan sampel data nyata pada Tabel 1 Baris Ke-10 dimana Kunci Dinamis yang digunakan adalah ”Kearsipan” (9 Karakter) dijelaskan pada Tabel 3 berikut ini.

Tabel 3. Analisis Komparatif menggunakan Rumus Keyspace

	M = 26	M = 75
Keyspace	26^9	75^9
Hasil *Keyspace*	5.429.503.678.976 kombinasi ($5{,}42 \times 10^{12}$)	$2.463.151.789 \times 10^{30} \times 10^9$ kombinasi ($2{,}46 \times 10^{39}$)

Dilihat dari Tabel 3 berikut ini maka dapat dianalisa secara lebih komprehensif estimasi waktu eksekusi brute force attack untuk membongkar algoritma pada penelitian ini berdasarkan level kecepatan komputasi hardware saat ini, dijelaskan pada Tabel 4.

Tabel 4. Estimasi Waktu Brute Force Attack

Tipe Perangkat	Kecepatan Uji	Estimasi Waktu	Status Keamanan

Personal Computer	10^9 *(1 giga-keys/secs)*	2,46 x 10^{30} detik	Sangat Aman
Super Computer	10^{15} *(1 peta-keys/secs)*	2,46 x 10^{24} detik	Sangat Aman
Modern Cryptanalysis Cluster	10^{18} *(1 exa-keys/secs)*	2,46 x 10^{13} detik	Aman

Pembahasan Aspek Zero-Knowledge Architecture Pada Google Cloud Ecosystem

Penerapan Client-Side Encryption dengan kombinasi Extended Vigenere Cipher dan Kunci Dinamis dalam penelitian ini berhasil mewujudkan model keamanan Zero-Knowledge Architecture. Secara definisi, Zero-Knowledge Architecture adalah arsitektur keamanan dimana penyedia layanan penyimpanan (cloud provider) memiliki nol pengetahuan terhadap struktur data asli yang disimpan oleh pengguna. Dalam konteks Google Cloud Ecosystem (Google Spreadsheet dan Google Apps Script), aspek Zero-Knowledge Architecture dalam penelitian ini dianalisis melalui tiga parameter utama dijelaskan pada Tabel 5.

Tabel 5. Analisis Implementasi Aspek Zero-Knowledge Architecture

No	Parameter	*Server-Side*	Kondisi Pada Penelitian *(Client-Side Encryption)*	Pembuktian Keamanan dan Kriptografi
1	Key Management Location	Kunci enkripsi dikelola dan disimpan oleh *Google (Google-managed keys)* di sisi server.	*Master Key* disimpan 100% secara lokal oleh pengguna dan tidak pernah dikirim ke jaringan.	*Server Google* tidak memiliki salinan kunci matematika untuk membalikkan nilai *ciphertext*.
2	Storage Characteristic	Penyedia cloud dapat membaca isi data (plaintext) sebelum enkripsi otomatis server berjalan.	*Google Spreadsheet* bertindak murni sebagai *Blind Storage* (penyimpanan buta) berisi karakter acak	Teknisi *cloud* atau peretas akun hanya melihat simbol acak
3	Decryption Computation	Proses dekripsi membutuhkan komputasi server, teks asli sempat terbentuk di memori cloud.	Proses dekripsi bersifat *Efemeral* (sementara), dieksekusi oleh CPU lokal pada *browser* pengguna.	Teks asli hasil dekripsi hanya dirender pada *browser clien*. Tidak ada jejak *plaintext* di *log history Google Cloud*.

KESIMPULAN

Penelitian ini berhasil mengimplementasikan arsitektur Client-Side Encryption menggunakan Extended Vigenere Cipher dan Kunci Dinamis pada Sistem Manajemen Arsip Pemerintah berbasis Google Cloud Ecosystem. Pengujian empiris membuktikan model Client-Side Encryption mampu mewujudkan Zero-Knowledge Architecture secara mutlak, di mana substansi data telah bertransformasi menjadi ciphertext di sisi browser pengguna sebelum ditransmisikan, sehingga memposisikan Google Spreadsheet murni sebagai Blind Storage. Integrasi Kode Klasifikasi Berkas sebagai salt terbukti efektif menghancurkan periodisitas kunci statis, memitigasi serangan Kasiski Examination, serta menjamin perlindungan forward secrecy per baris data. Selain itu, perluasan ruang karakter melalui Modulo 75 (Mod 75) sukses memfasilitasi penyandian karakter campuran dokumen kedinasan sekaligus meningkatkan kompleksitas keyspace hingga 7521, yang membuat Brute Force Attack tidak layak secara komputasi (computationally infeasible).

Meskipun dari hasil pengujian terbukti kuat dari aspek privasi, keterbatasan sistem ini membuka peluang bagi penelitian selanjutnya. Risiko kehilangan data permanen akibat isolasi kunci memicu kebutuhan integrasi skema Secret Sharing sebagai metode pemulihan kunci mandiri di sisi klien. Selain itu, ketidakmampuan database cloud mengenali konten terenkripsi memicu urgensi penerapan metode Searchable Encryption guna mendukung fungsionalitas pencarian global tanpa mendekripsi data. Terakhir, beban komputasi peramban yang berpotensi menurunkan performa perangkat berspesifikasi rendah saat menangani data masif menjadi ruang eksplorasi lanjutan bagi implementasi Lightweight Cryptography atau optimasi berbasis WebAssembly.

DAFTAR PUSTAKA

Muhsin, Abid., & Nugraha. (2025). Implementasi Algoritma Levenshtein Distance dan SHA-256 Pada Sistem Pengelolaan Arsip Dengan Evaluasi TAM. Jurnal Algoritma Institut Teknologi Garut.

Arsip Nasional Republik Indonesia. (2021). Peraturan Arsip Nasional Republik Indonesia Nomor 6 Tahun 2021 tentang Pengelolaan Arsip Elektronik. Jakarta: Arsip Nasional Republik Indonesia.

Arifa, R., Husaini, H., & Rudi, F. (2024). Implementasi Aplikasi Enkripsi Dekripsi File Dokumen Menggunakan Algoritma Aes Pada Cloud Computing (Studi Kasus Prodi Teknologi Rekayasa Komputer Jaringan). Journal of Artificial Intelligence and Software Engineering (J-AISE).

Oktafiani, R., Ujianto, E., & Rianto, R. (2023). Kombinasi Algoritma Kriptografi Vigenere Cipher dan SHA256 untuk Keamanan Basis Data. Jurnal Sistem Komputer dan Informatika (JSON);

Dwina, N., Khairani, N., Nasir, M., & Indrawati, I. (2023). Penerapan Metode Advanced Encryption Standard pada Sistem Penyimpanan Data Menggunakan Cloud Computing Sebagai Software-as-a-Service. Journal of Artificial Intelligence and Software Engineering (J-AISE).

Akma, M., & Wardhani, D. (2025). Keamanan Data Dalam Cloud Computing untuk Institusi Kesehatan. Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI).

Musa, A., & Mahmood, A. (2021). Client-side Cryptography Based Security for Cloud Computing System. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 594-600.

Sianturi, M., & Zebua, T. (2023). Modifikasi Pembangkit Kunci Algoritma Vigenere Cipher Berdasarkan Pembangkit Bilangan Acak CSPRNG Untuk Mengamankan Citra Digital. Jurnal Sains dan Teknologi Informasi. https://doi.org/10.47065/jussi.v2i4.4792.

Informatika, J., Informasi, D., Studi, P., Informatika, T., Teknik, F., Firmansyah, F., Winarno, W., Nasiri, A., Editorial, D., Berlanjut, E., Ziaurrahman, M., Utami, E., Wibowo, F., Nurcahyo, A., & Raharjo, S. (2019). MODIFIKASI KRIPTOGRAFI KLASIK VIGENERE CIPHER MENGGUNAKAN ONE TIME PAD DENGAN ENKRIPSI BERLANJUT. 63-68.

Manthiramoorthy, C., Khan, K., & A, N. (2023). Comparing Several Encrypted Cloud Storage Platforms. International Journal of Mathematics, Statistics, and Computer Science.

Septianto, Yudi, et al. "Implementasi Multi Algoritma pada Aplikasi Enkripsi dalam Mengamankan File IMPLEMENTATION OF MULTIPLE ALGORITHMS ON ENCRYPTION APPLICATIONS IN SECURING FILES." 2022.

Riadi, I., et al. "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher." JISKA (Jurnal Informatika Sunan Kalijaga), 2022.

Sari, R. P., & Wardoyo, S. (2021). Optimasi Keamanan Teks Dokumen Menggunakan Algoritma Vigenere Cipher Klasik. Jurnal Teknik Informatika dan Sistem Informasi, 8(2), 345–354.

Pratama, A. B., Sukarno, P., & Nugroho, M. A. (2023). Penerapan Extended Vigenere Cipher Menggunakan Karakter ASCII 95 untuk Pengamanan Berkas Digital. Jurnal Cyber

Security dan Forensik Digital, 6(1), 12–21.
Setiawan, H. (2024). Analisis Ketahanan Autokey Vigenere Cipher Terhadap Serangan Known-Plaintext Attack pada Aplikasi Berbasis Web. Jurnal Sains dan Teknologi Informasi, 13(3), 115–123.