



Analisis Penerapan Metode Enkripsi AES dan Kompresi LZMA untuk Keamanan Dokumen Medis Elektronik

Toto Raharjo

23917010

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2025

Lembar Pengesahan Pembimbing

Analisis Penerapan Metode Enkripsi AES dan Kompresi LZMA untuk Keamanan Dokumen Medis Elektronik

Toto Raharjo

23917010



Yogyakarta, Mei 2025

Pembimbing

Dr. Yudi Prayudi, S.Si., M. Kom.

Lembar Pengesahan Penguji

Analisis Penerapan Metode Enkripsi AES dan Kompresi LZMA untuk Keamanan Dokumen Medis Elektronik

Toto Raharjo

23917010

Yogyakarta, Juli, 2025

Tim Penguji,

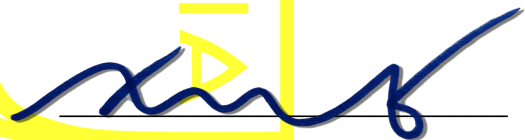
Dr. Yudi Prayudi, S.Si., M. Kom.

Ketua



Dr. Ahmad Luthfi, S.Kom., M.Kom.

Anggota I



Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Anggota II



Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia



Ir. Irving Vitra Paputungan, ST., M.Sc., Ph.D

Analisis Penerapan Metode Enkripsi AES dan Kompresi LZMA untuk Keamanan Dokumen Medis Elektronik

Seiring dengan meningkatnya ancaman keamanan di dunia maya, menjaga integritas data medis elektronik menjadi semakin krusial. Penelitian ini berfokus pada pengembangan metode yang menggabungkan enkripsi menggunakan Advanced Encryption Standard (AES) dan kompresi dengan algoritma Lempel-Ziv-Markov (LZMA) untuk melindungi file DICOM yang berisi informasi sensitif. Metode ini dirancang untuk mengatasi dua tantangan utama: peningkatan ukuran file setelah enkripsi dan efisiensi penyimpanan data. Dalam penelitian ini menggunakan desain eksperimental dengan teknik random sampling, menguji 542 file DICOM dari perpustakaan terbuka dengan ukuran berkisar antara 513,06 KB hingga 513,39 KB. Tujuannya adalah untuk mengevaluasi efektivitas metode ini dalam mengurangi ukuran file, waktu enkripsi dan menjaga integritas data. Hasil penelitian menunjukkan bahwa metode ini berhasil mengurangi ukuran file sebesar 40-50%, dengan waktu enkripsi rata-rata sekitar 0,2-0,3 detik per file. Selain itu data tetap utuh sebelum dan sesudah proses enkripsi, menandakan bahwa integritas data terjaga dengan baik. Analisis lebih lanjut mengungkapkan bahwa penggunaan CPU selama proses enkripsi mencapai 94,05%, sementara penggunaan memori tercatat sebesar 92,95 KB. Sebaliknya selama proses dekripsi penggunaan CPU menurun menjadi 78,16% dengan konsumsi memori yang jauh lebih rendah yaitu 31,07 KB. Temuan ini memiliki implikasi signifikan bagi sistem informasi medis, memungkinkan pengembang untuk dengan mudah mengimplementasikan metode ini melalui API. Penelitian ini diharapkan dapat menjadi acuan bagi studi-studi mendatang yang berfokus pada keamanan data dalam sistem informasi kesehatan, serta memberikan wawasan baru mengenai kombinasi enkripsi dan kompresi dalam konteks data medis.

Kata kunci

Enkripsi AES, Kompresi LZMA, Data Medis Elektronik, File DICOM, Keamanan Data

Analysis of the Implementation of AES Encryption and LZMA Compression Methods for the Security of Electronic Medical Documents

As cyber threats continue to rise, maintaining the integrity of electronic medical data has become increasingly crucial. This research focuses on developing a method that integrates encryption using the Advanced Encryption Standard (AES) and compression with the Lempel-Ziv-Markov Algorithm (LZMA) to protect DICOM files containing sensitive information. This method is designed to address two main challenges: the increase in file size after encryption and the efficiency of data storage. In this study, we applied an experimental design with random sampling, testing 542 DICOM files from an open library with sizes ranging from 513.06 KB to 513.39 KB. The aim was to evaluate the effectiveness of this method in reducing file size, encryption time, and maintaining data integrity. The results indicate that this method successfully reduced file size by 40-50%, with an average encryption time of approximately 0.2-0.3 seconds per file. Furthermore, the data remained intact before and after the encryption process, indicating that data integrity was well preserved. Further analysis revealed that CPU usage during the encryption process reached 94.05%, while memory usage was recorded at 92.95 KB. Conversely, during the decryption process, CPU usage decreased to 78.16% with significantly lower memory consumption of 31.07 KB. These findings have significant implications for medical information systems, allowing developers to easily implement this method through an API. This research is expected to serve as a reference for future studies focusing on data security in health information systems and to provide new insights into the combination of encryption and compression in the context of medical data.

Keywords

AES Encryption, LZMA Compression, Electronic Medical Data, DICOM Files, Data Security

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Mei 2025


Toto Raharjo.



Daftar Publikasi

Publikasi yang dihasilkan:

T. Raharjo and Yudi Prayudi, “Securing Electronic Medical Documents Using AES and LZMA”, J. RESTI (Rekayasa Sist. Teknol. Inf.), vol. 9, no. 2, pp. 374 -384, Apr. 2025.

Kontributor	Jenis Kontribusi
Toto Raharjo	Mendesain eksperimen (60%) Menulis <i>paper</i> (70%)
Dr. Yudi Prayudi, S.Si., M. Kom.	Mendesain eksperimen (40%) Menulis dan mengedit <i>paper</i> (30%)

Halaman Kontribusi

Penelitian ini melibatkan kontribusi dari berbagai pihak sebagai berikut:

1. Moh Ali Romli, S.Kom, M.Kom Melakukan review kritis terhadap hasil interpretasi data penelitian.
2. An'anqinudin Lahitama, S.Kom Melakukan pengujian dan validasi hasil interpretasi penelitian.
3. PT Gama Integra Informatika Berperan sebagai mitra objek pengujian dalam pelaksanaan penelitian.
4. Staf Klinik Intan Yogyakarta Memberikan dukungan data dan arahan teknis selama proses penelitian.

Halaman Persembahan

Alhamdulillahirabbil ‘alamin

Dengan segala kerendahan hati, penulis mengucapkan syukur ke hadirat Allah SWT atas limpahan rahmat, taufik, dan hidayah-Nya, sehingga tesis ini dapat diselesaikan dengan baik. Shalawat dan salam semoga senantiasa tercurah kepada Nabi Muhammad SAW, suri teladan sepanjang zaman dalam menuntut ilmu dan mengamalkannya.

Tesis ini kupersembahkan untuk:

1. Allah SWT, sumber segala kekuatan, dan Rasulullah SAW, teladan dalam keteguhan dan keikhlasan. Tanpa pertolongan dan bimbingan-Mu, tak satu pun halaman dalam tesis ini akan terwujud.
2. Istriku tercinta, yang selalu mendampingi dengan kesetiaan dan dukungan tanpa syarat. Terima kasih telah menjadi sumber semangat di setiap proses yang kujalani.
3. Kedua orang tuaku tercinta, yang senantiasa mengiringi langkahku dengan doa, kesabaran, dan cinta yang tak pernah surut. Aku sadar takkan mampu membalas semua pengorbanan kalian, namun semoga ijazah ini menjadi wujud kecil dari rasa terima kasih yang tulus.
4. Para dosen dan staf MI UII, atas ilmu, arahan, dan kritik yang membangun. Setiap nasihat dan bimbingan Bapak/Ibu telah menjadi bagian penting dalam terbentuknya karya ini.
5. Teman-teman seperjuangan MI UII angkatan 2023, khususnya kelompok Forensika Digital terima kasih atas kerja sama, semangat, dan kebersamaan yang telah menjadi warna indah dalam perjalanan akademik ini.
6. Semua pihak yang tak dapat disebutkan satu per satu, atas segala bentuk dukungan, perhatian, dan masukan yang diberikan. Setiap sumbangsih, sekecil apa pun, menjadi bagian berharga dari proses ini.

Semoga Allah membalas setiap kebaikan dengan balasan terbaik.

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT, Tuhan Yang Maha Pengasih dan Penyayang. Atas limpahan rahmat dan pertolongan-Nya, penulis dapat menyelesaikan tesis berjudul: "Analisis Penerapan Metode Enkripsi AES dan Kompresi LZMA untuk Keamanan Dokumen Medis Elektronik", sebagai bagian dari syarat memperoleh gelar Magister pada Program Studi Magister Informatika. Tesis ini tidak akan terselesaikan tanpa dukungan, bimbingan, dan bantuan dari berbagai pihak yang dengan tulus membagikan ilmu, waktu, dan tenaga. Dengan tulus, penulis menyampaikan terima kasih dan penghargaan yang sebesar-besarnya kepada semua pihak yang telah berperan dalam proses ini. Dengan hati yang tulus, penulis menyampaikan penghargaan setinggi-tingginya kepada:

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., Rektor Universitas Islam Indonesia, atas kebijakan-kebijakan akademik yang mendukung proses penelitian.
2. Irving Vitra Paputungan, S.T., M.Sc., Ph.D, Ketua Program Studi Magister Informatika, atas bimbingan dan fasilitas yang diberikan selama masa studi.
3. Bapak Dr. Yudi Prayudi, S.Si., M.Kom., Dosen Pembimbing, yang dengan sabar meluangkan waktu, memberikan arahan berharga setiap langkah penelitian hingga tesis ini sempurna.
4. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom. yang dengan sabar meluangkan waktu, memberikan koreksi berharga setiap langkah penelitian hingga tesis ini sempurna.
5. Seluruh pihak yang tidak dapat disebutkan satu per satu, baik yang telah memberikan dukungan moral, material, maupun spiritual selama perjalanan akademik ini.

Penulis menyadari bahwa tesis ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan. Semoga Allah SWT membalas segala kebaikan pihak-pihak yang telah membantu, dan semoga karya ini bermanfaat bagi pengembangan ilmu serta praktik di bidang forensik digital.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Yogyakarta 09 Mei 2025



Toto Raharjo

Daftar Isi

Lembar Pengesahan Pembimbing	i
Lembar Pengesahan Penguji.....	ii
Daftar Publikasi	vi
Halaman Kontribusi.....	vii
Halaman Persembahan	viii
Kata Pengantar.....	ix
Daftar Isi	x
Daftar Tabel.....	xiv
Daftar Gambar	xv
Glosarium	xvii
BAB 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	5
1.3 Tujuan Penelitian	6
1.4 Batasan Masalah	6
1.5 Manfaat Penelitian	6
1.6 Metode Penelitian	7
1.7 Sistematika Penulisan	8
BAB 2 Tinjauan Pustaka	9
2.1 Penelitian Terdahulu	9
2.2 Konsep Keamanan Data Medis.....	14
2.3 Regulasi dan Kebijakan	16
2.4 File DICOM.....	17
2.5 Teknik Kompresi	18
2.6 Teknik Enkripsi.....	19

2.7	Implementasi API	20
2.8	Integritas Data.....	21
2.9	Docker.....	22
2.10	Cloud Computing.....	23
2.11	Load Balancing	24
2.12	Anti Forensik.....	24
2.13	Efektifitas	25
BAB 3 Metodologi		26
3.1	Persiapan Data	26
3.2	Persiapan Sistem dan Alat	28
3.3	Simulasi Kasus.....	31
3.4	Pengolahan Data	31
3.5	Implementasi dalam Bentuk API.....	33
3.5.1	Lingkungan Pengembangan	33
3.5.2	Arsitektur Sistem	33
3.5.3	Fungsi-Fungsi Endpoint API.....	34
3.5.4	Integrasi Layanan Penyimpanan Cloud.....	34
3.6	Metode Pengujian	35
BAB 4 Hasil dan Pembahasan.....		36
4.1	Pengumpulan Data.....	36
4.2	Persiapan Alat	38
4.2.1	Lingkungan Pengembangan	38
4.2.2	Bahasa Pemrograman dan Library Pendukung	39
4.2.3	Penyusunan Struktur Direktori dan Mapping Port	39
4.2.4	Pengaturan File Konfigurasi dan Dataset	40
4.2.5	Validasi Kebutuhan Pengembangan.....	40
4.3	Skenario dan Simulasi	41

4.3.1	Fungsi Base64	42
4.3.2	Fungsi Kompresi LZMA	43
4.3.3	Fungsi Enkripsi AES	43
4.4	Tahapan Pengujian.....	44
4.4.1	Pengujian File DICOM.....	44
4.4.2	Pengujian File JPEG	48
4.4.3	Pengujian Integritas Data.....	50
4.4.4	Pengujian Serangan Bruteforce	51
4.4.5	Pengujian Reduksi Ukuran File.....	52
4.4.6	Pengujian Proses Secara Serial.....	54
4.4.7	Pengujian Proses Secara Paralel	55
4.5	Pemeriksaan dan Analisis Output	58
4.5.1	Pemeriksaan dan Analisis Base64	58
4.5.2	Pemeriksaan dan Analisis LZMA.....	59
4.5.3	Pemeriksaan dan Analisis AES	59
4.5.4	Pemeriksaan dan Analisis Checksum MD5.....	59
4.5.5	Pemeriksaan dan Analisis Pengujian.....	60
4.5.6	Tingkat Penghematan Algoritma LZMA	62
4.6	Metode Evaluasi Kinerja	63
4.7	Hasil Produk	66
4.7.1	Docker Image	66
4.7.2	Pengembangan API untuk Developer.....	67
4.7.3	Implementasi Arsitektur Mikroservices	67
4.8	Kontribusi Penelitian terhadap Bidang Forensika Digital	68
4.9	Keterbatasan dan Titik Kegagalan Metode.....	70
BAB 5	Kesimpulan dan Saran.....	71
5.1	Kesimpulan	71

5.2	Saran	72
	Daftar Pustaka	73
	LAMPIRAN	76

Daftar Tabel

Tabel 2. 1 Ulasan Penelitian Enkripsi Data Medis	10
Tabel 2. 2 Ulasan Penelitian Kompresi Data Medis.....	11
Tabel 2. 3 Ulasan Penelitian Digital Rights Management (DRM).....	13
Tabel 2. 4 Ulasan Penelitian Implementasi Teknologi di Lingkungan IoT dan IoMT	13
Tabel 3. 1 Spesifikasi Hardware	29
Tabel 3. 2 Software Untuk Proses Pengembangan.....	29
Tabel 3. 3 Aplikasi Dan Pustaka Python	29
Tabel 3. 4 Parameter Evaluasi	30

Daftar Gambar

Gambar 1.1 Kebocoran data dokumen elektronik.	3
Gambar 2.1 Komponen rekam medis elektronik.	15
Gambar 2.2 Kategori data pribadi.	16
Gambar 2.3 Struktur file DICOM.	17
Gambar 2.4 Alur kompresi.	18
Gambar 2.5 Alur enkripsi.	20
Gambar 2.6 Konsep API.	21
Gambar 2.7 Alur checksum MD5.	22
Gambar 2.8 Cara kerja Docker.	22
Gambar 2.9 Posisi <i>cloud computing</i>	23
Gambar 2.10 Cara kerja <i>load balancing</i>	24
Gambar 3.1 Alur pemodelan.	26
Gambar 3.2 Alur simulasi.	31
Gambar 3.3 Pemrosesan file DICOM.	32
Gambar 4.1 Bahan file DICOM.	37
Gambar 4.2 Spesifikasi hardware untuk pengembang.	38
Gambar 4.3 Membuat container API.	39
Gambar 4.4 Tampilan file DICOM.	40
Gambar 4.5 File pada <i>Container</i>	41
Gambar 4.6 Perintah enkripsi dan dekripsi.	41
Gambar 4.7 Alur proses pengujian.	42
Gambar 4.8 File DICOM sebelum enkripsi.	45
Gambar 4.9 Proses enkripsi.	46
Gambar 4.10 File dicom setelah enkripsi.	46
Gambar 4.11 Proses dekripsi.	47
Gambar 4.12 Gambar setelah dekripsi.	48
Gambar 4.13 Hasil enkripsi JPEG.	49
Gambar 4.14 Hasil pencarian checksum MD5.	50
Gambar 4.15 Hasil pengujian <i>bruteforce</i>	51
Gambar 4.16 Hasil pengujian reduksi file.	53
Gambar 4.17 Log hasil enkripsi secara serial.	55

Gambar 4.18 Log hasil enkripsi secara paralel.....	56
Gambar 4.19 Log hasil dekripsi secara paralel.....	57
Gambar 4.20 Penggunaan <i>resource hardware</i>	61
Gambar 4.21 Implementasi modul.	68

Glosarium

DICOM	- Digital Imaging and Communications in Medicine
MRI	- Magnetic Resonance Imaging
CT	- Computed Tomography
RME	- Rekam Medis Elektronik
UU PDP	- Perlindungan Data Pribadi
API	- Application Programming Interface
HIPAA	- Health Insurance Portability and Accountability Act
GDPR	- General Data Protection Regulation
RESTful	- Representational State Transfer-based Web Services
GCM	- Galois/Counter Mode
PERMENKES	- Peraturan Menteri Kesehatan
AES	- Advanced Encryption Standard
LZMA	- Lempel-Ziv-Markov chain Algorithm
ASCII	- American Standard Code for Information Interchange

BAB 1

Pendahuluan

1.1 Latar Belakang

Keamanan data medis kini menjadi perhatian yang semakin mendesak, terutama dengan meningkatnya penggunaan dokumen elektronik di rumah sakit dan klinik. Rekam medis elektronik ini menyimpan informasi sensitif yang memerlukan langkah-langkah perlindungan data yang kuat. (Sarce Joel et al., 2023). Dengan meningkatnya frekuensi pelanggaran data di bidang medis, sangat penting untuk menerapkan strategi yang efektif dalam melindungi informasi ini. Dalam kasus ini penggunaan teknik enkripsi dan kompresi muncul sebagai solusi krusial untuk meningkatkan keamanan data sekaligus mengoptimalkan penyimpanan. Penelitian ini akan mengeksplorasi efektivitas teknik-teknik tersebut dalam melindungi rekam medis elektronik. Insiden global terbaru telah menyoroti ancaman signifikan terhadap keamanan informasi kesehatan, menekankan kebutuhan mendesak akan langkah-langkah perlindungan yang komprehensif (Lallie et al., 2021).

Pelanggaran data di sektor kesehatan telah menjadi ancaman serius yang terus berkembang, dengan frekuensi insiden yang meningkat secara global. Insiden-insiden ini menunjukkan bahwa informasi kesehatan yang merupakan salah satu aset paling sensitif dan bernilai, rentan terhadap serangan siber, pencurian data dan akses tidak sah. Ancaman ini tidak hanya mengganggu privasi pasien tetapi juga dapat merusak kepercayaan masyarakat terhadap sistem layanan kesehatan. Oleh karena itu penting bagi organisasi medis untuk menyadari urgensi masalah ini dan segera mengambil langkah proaktif guna melindungi data medis dari risiko pelanggaran yang semakin canggih dan berbahaya.

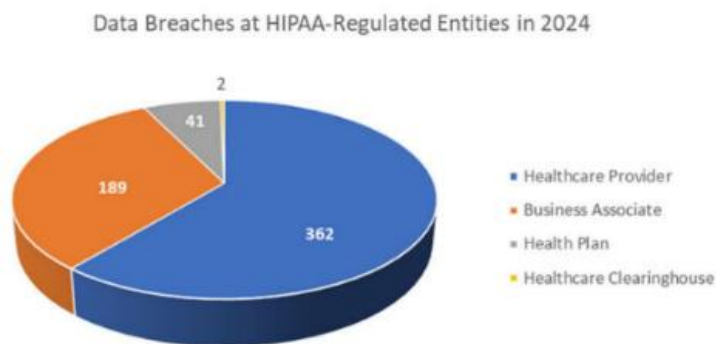
Dalam era digital yang terus berkembang menjaga keamanan data menjadi aspek krusial yang tidak dapat diabaikan terutama untuk dokumen elektronik medis. Transisi dari penyimpanan fisik ke penyimpanan digital telah membawa berbagai manfaat seperti kemudahan akses, efisiensi dalam pengelolaan data dan pengurangan biaya operasional. Dokumen medis yang dahulu disimpan dalam bentuk fisik kini dapat diakses dengan cepat dan mudah melalui sistem rekam medis elektronik *Electronic Medical Records* (EMR). Hal ini memungkinkan tenaga medis untuk memberikan perawatan yang lebih cepat dan akurat kepada pasien serta mempermudah koordinasi antar penyedia layanan kesehatan (Indriyajati et al., 2023)

Namun di balik manfaat tersebut transisi ke penyimpanan digital juga membuka celah potensi kebocoran data yang dapat merugikan. Data medis adalah salah satu jenis informasi yang sensitif dan berharga karena mengandung informasi pribadi pasien yang sangat detail dan rahasia. Ancaman keamanan seperti peretasan, malware dan akses tidak sah telah menjadi isu utama yang harus dihadapi oleh institusi kesehatan. Kebocoran data medis tidak hanya dapat merugikan secara finansial tetapi juga dapat menurunkan kepercayaan pasien terhadap penyedia layanan kesehatan. Oleh karena itu diperlukan langkah-langkah keamanan yang ketat untuk melindungi data medis dari berbagai ancaman ini (Sharma & Prabha, 2023).

Kejadian kebocoran data di Indonesia menunjukkan betapa rentannya sistem penyimpanan digital terhadap serangan siber. Dalam beberapa tahun terakhir Indonesia telah mengalami beberapa insiden kebocoran data yang signifikan termasuk di sektor kesehatan. Pada Maret 2023 sekitar 18,5 juta pengguna dari Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan dilaporkan telah dijual secara ilegal di forum gelap. Para peretas mengancam akan mengungkapkan informasi tersebut jika uang tebusan tidak dibayarkan. Pelanggaran ini terjadi karena peretas berhasil mengakses database BPJS Kesehatan secara tidak sah. Data yang dicuri mencakup informasi sensitif seperti nama lengkap, nomor identifikasi, alamat, tanggal lahir serta informasi kesehatan dan status keanggotaan. Insiden ini menimbulkan kekhawatiran besar tentang kemungkinan pencurian identitas dan penyalahgunaan data pribadi oleh pihak-pihak yang tidak bertanggung jawab (Hartono, 2023).

Selain itu ada kasus serupa hampir 4 juta orang juga terpengaruh oleh pelanggaran yang terjadi di perusahaan transkripsi medis. Pelanggaran ini dilaporkan terjadi antara 27 Maret 2023 dan 2 Mei 2023, mempengaruhi sekitar 3.998.162 orang. Sumber kebocoran ini diketahui berasal dari Perry Johnson & Associates, penyedia layanan transkripsi medis. Pihak yang tidak berwenang berhasil mengakses jaringan mereka dan mendapatkan salinan file tertentu yang berisi informasi pribadi pasien Concentra, termasuk data demografis dan informasi klinis (*10 Largest Healthcare Data Breaches of 2024 | TechTarget*, 2024).

Berdasarkan data pada *Health Insurance Portability and Accountability Act* (HIPAA) ditemukan kasus kebocoran data sensitif terjadi pada penyedia sistem informasi elektronik bagian kesehatan.



Gambar 1.1 Kebocoran data dokumen elektronik.

Berdasarkan Gambar 1.1 menunjukkan bahwa penyedia sistem informasi merupakan sektor yang menerima jumlah kasus kebocoran data tertinggi. Insiden tersebut menyoroti pentingnya melindungi data medis dan menunjukkan bahwa kebocoran informasi kesehatan dapat memiliki dampak yang luas termasuk risiko pencurian identitas dan hilangnya kepercayaan publik pada sistem kesehatan.

Transformasi digital di bidang kesehatan di Indonesia telah menjadi keharusan seiring dengan pemberlakuan Peraturan Menteri Kesehatan (Permenkes) Nomor 24 Tahun 2022 tentang Rekam Medis. Regulasi ini mewajibkan semua fasilitas pelayanan kesehatan untuk beralih dari sistem rekam medis konvensional ke sistem RME. Selain itu, fasilitas pelayanan kesehatan juga berkewajiban memastikan keamanan dan kerahasiaan data yang terdapat dalam RME. Perlindungan ini secara khusus ditujukan pada konten rekam medis diberikan kepada pasien.

Salah satu aspek penting dari Permenkes terbaru (Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis, 2022) adalah sifatnya yang tidak terbatas pada format file teknis tertentu. Artinya apapun format dokumen digital yang digunakan seperti DICOM, PNG, TIF atau format lainnya selama dokumen tersebut memuat konten rekam medis sebagaimana didefinisikan dalam regulasi yaitu yang berisi data identitas pasien, pemeriksaan, pengobatan, tindakan, identitas pasien, hasil pemeriksaan fisik, diagnosis, pengobatan, rencana tindak lanjut pelayanan kesehatan, data tenaga kesehatan pemberi pelayanan kesehatan maka dokumen tersebut wajib dilindungi. Secara umum dokumen medis elektronik tersusun atas dua komponen yaitu file gambar yang merupakan representasi visual utama dari data medis seperti hasil radiologi atau pencitraan medis dan metadata yang berisi informasi kontekstual serta data sensitif pasien seperti identitas, riwayat medis dan detail administratif.

Kedua komponen ini merupakan bagian penting dari setiap dokumen medis elektronik dan harus dijaga kerahasiaannya sesuai ketentuan perundang-undangan. Oleh karena itu fokus utama dari penelitian ini adalah pengolahan dan pengamanan terhadap kedua entitas data inti tersebut, yaitu file gambar sebagai data visual dan metadata sebagai data tekstual yang merupakan esensi dari setiap dokumen medis elektronik. Dengan pendekatan ini metode keamanan yang dikembangkan diharapkan dapat relevan dan diterapkan secara luas untuk memenuhi kewajiban perlindungan data yang diatur dalam Permenkes Nomor 24 Tahun 2022.

Penekanan pada kedua entitas data inti ini penting karena file gambar dan metadata memiliki peran yang saling melengkapi dalam membentuk keseluruhan informasi medis. File gambar menyediakan data visual yang mendasar untuk diagnosis dan tindakan medis, sedangkan metadata memberikan konteks yang diperlukan untuk menginterpretasi file gambar tersebut. Dengan memastikan bahwa kedua entitas ini diamankan secara efektif, penelitian ini bertujuan untuk memberikan solusi keamanan yang komprehensif dan sesuai dengan standar perlindungan data yang diamanatkan oleh regulasi.

Penelitian sebelumnya telah memberikan kontribusi penting dalam mengatasi masalah keamanan dan efisiensi penyimpanan data medis. Teknik enkripsi canggih seperti penggunaan metode AES dan Base64 untuk melindungi gambar medis telah terbukti efektif dalam menjaga kerahasiaan data sensitif dari akses tidak sah. Pentingnya studi ini semakin diperkuat dengan adanya regulasi nasional yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini menegaskan bahwa setiap instansi atau lembaga yang mengelola data pribadi termasuk data medis, wajib menjamin keamanan dan kerahasiaan data tersebut. Pasal 9 dan Pasal 36 UU PDP secara jelas menyebutkan bahwa pengendali data harus menerapkan langkah-langkah teknis dan administratif untuk melindungi data pribadi dari akses tanpa izin, pengungkapan atau modifikasi yang tidak sah.

Namun meskipun keamanan data menjadi prioritas utama, pendekatan ini menimbulkan tantangan baru terkait ukuran file yang membengkak, sehingga menciptakan beban tambahan pada sistem penyimpanan terutama di lingkungan dengan kapasitas terbatas. Di sisi lain penelitian yang memfokuskan pada kompresi data, seperti penggunaan Kode Rantai dan LZMA untuk gambar biner, berhasil meningkatkan efisiensi penyimpanan dengan mengurangi ukuran file. Namun pendekatan ini kurang memperhatikan aspek keamanan data yang merupakan elemen kritis dalam konteks rekam medis elektronik. Ketidakseimbangan antara keamanan dan efisiensi penyimpanan ini menunjukkan adanya

celah dalam solusi yang ada, di mana kedua aspek tersebut belum sepenuhnya diintegrasikan secara optimal.

Kontribusi penelitian ini secara signifikan memperkuat bidang Forensika Digital, terutama dalam aspek penjaminan integritas dan kerahasiaan data sebagai pilar utama investigasi digital. Metode yang diusulkan dalam penelitian ini secara langsung mendukung kepatuhan terhadap regulasi tersebut dan memperkuat fondasi kerja forensika digital. Keberhasilan metode dalam mempertahankan integritas data setelah proses enkripsi dan kompresi, sebagaimana diverifikasi melalui checksum MD5, sangat vital untuk keabsahan bukti digital dalam investigasi forensik. Peningkatan keamanan data melalui enkripsi AES tidak hanya melindungi informasi sensitif dari akses tidak sah, tetapi juga dapat memitigasi dampak pelanggaran data, sehingga memudahkan tim forensik dalam menganalisis sejauh mana data terekspos. Penelitian ini juga memperkuat studi sebelumnya mengenai Komunikasi Aman untuk Forensika Digital, menegaskan kontribusinya dalam menciptakan lingkungan komunikasi digital yang lebih aman, yang esensial untuk pengumpulan dan analisis bukti digital yang akurat. Dengan demikian penelitian ini tidak hanya menawarkan solusi teknis untuk keamanan dan efisiensi data medis, tetapi juga secara fundamental mendukung tujuan Forensika Digital dalam menjamin keandalan informasi di tengah kompleksitas ancaman siber.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka yang menjadi rumusan masalah adalah sebagai berikut:

- a. Bagaimana merancang sebuah metode yang mengintegrasikan enkripsi AES dan kompresi LZMA untuk mengamankan dua komponen fundamental dokumen medis elektronik, yaitu data gambar dan metadata, sesuai dengan amanat Permenkes No. 24 Tahun 2022?
- b. Seberapa efektif penerapan metode gabungan enkripsi dan kompresi dalam meningkatkan efisiensi penyimpanan data dengan cara mengurangi ukuran file tanpa mengorbankan kecepatan proses dan keamanan data medis elektronik?
- c. Bagaimana mekanisme verifikasi seperti checksum atau hashing dapat diimplementasikan untuk menjamin integritas data gambar dan metadata selama siklus proses enkripsi-kompresi dan dekripsi-dekompresi, sehingga memastikan data tidak mengalami perubahan?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan penelitian ini adalah sebagai berikut:

- a. Merancang dan mengembangkan sebuah metode terintegrasi yang menggabungkan enkripsi AES dan kompresi LZMA untuk mengamankan komponen data gambar dan metadata dalam dokumen medis elektronik.
- b. Mengevaluasi efektivitas metode yang diusulkan dengan menganalisis tingkat efisiensi penyimpanan data serta performa sistem berdasarkan parameter reduksi ukuran file, waktu proses, penggunaan CPU dan memori.
- c. Mengimplementasikan dan memverifikasi mekanisme hashing untuk memastikan integritas data gambar dan metadata tidak berubah selama dan setelah siklus proses enkripsi, kompresi, dekripsi dan dekompresi.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini meliputi:

- a. Penelitian ini hanya menggunakan file DICOM yang diambil dari open library dan file JPEG dan TIF dari dokumen internal klinik, sehingga hasilnya mungkin tidak dapat digeneralisasi untuk semua jenis file medis.
- b. Penelitian ini terbatas pada penggunaan enkripsi AES dan kompresi LZMA, tanpa mempertimbangkan metode enkripsi atau kompresi lainnya.
- c. Penelitian ini dilakukan dalam rentang waktu tertentu, yaitu pengujian dilakukan pada file yang diambil antara waktu tertentu, yang mungkin tidak mencakup semua variasi data.
- d. Fokus penelitian ini hanya pada enkripsi dan kompresi, tanpa membahas aspek keamanan lain seperti kontrol akses atau audit log.
- e. Penelitian ini tidak mempertimbangkan pengaruh metode yang diusulkan terhadap kinerja sistem secara keseluruhan di lingkungan produksi.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain:

- a. Penelitian ini memberikan solusi untuk meningkatkan keamanan data medis dengan mengintegrasikan enkripsi dan kompresi, sehingga melindungi informasi sensitif dalam file DICOM, JPEG dan TIF.

- b. Metode yang dikembangkan dapat mengurangi ukuran file DICOM, JPEG dan TIF, yang membantu dalam efisiensi penyimpanan data di sistem informasi kesehatan.
- c. Penelitian ini memastikan bahwa integritas data tetap terjaga selama proses enkripsi dan kompresi, sehingga informasi tetap akurat dan dapat diandalkan.
- d. Hasil penelitian dapat menjadi acuan bagi pengembang sistem informasi medis dalam menerapkan teknik enkripsi dan kompresi yang efektif melalui API.
- e. Penelitian ini diharapkan dapat menjadi dasar bagi studi-studi mendatang yang berfokus pada keamanan data dalam sistem informasi kesehatan, serta memberikan wawasan baru tentang kombinasi enkripsi dan kompresi.

1.6 Metode Penelitian

Penelitian ini perlu disusun langkah-langkah penyelesaian secara sistematis, adapun sistematika metodologi yang digunakan pada penelitian ini adalah sebagai berikut:

1. Tinjauan Pustaka

Tinjauan pustaka bertujuan untuk menghimpun landasan teori serta referensi dari berbagai penelitian terdahulu. Dengan demikian, penelitian ini dapat terhindar dari pembahasan yang bersifat duplikatif dan mampu menghasilkan karya ilmiah yang lebih terarah, efektif dan memiliki kontribusi yang bernilai.

2. Teknik Pengambilan Sampel Data

Melalui kajian terhadap berbagai penelitian sebelumnya, dapat dikenali sejumlah aspek penting yang menjadi perhatian dalam bidang enkripsi. Sementara itu proses pengumpulan sampel gambar dilakukan dengan mengikuti protokol dan parameter yang telah ditentukan, agar metode yang digunakan dapat dipahami secara utuh dan diterapkan dengan konsisten.

3. Implementasi Metode

Indikator dan parameter yang telah diidentifikasi selanjutnya dianalisis melalui proses perbandingan antar komponen yang telah ditentukan sebelumnya, guna mengevaluasi kinerja dan relevansinya secara lebih menyeluruh.

4. Analisis Data

Hasil dari penerapan metode tersebut akan dianalisis dan diproses lebih lanjut guna memperoleh nilai akurasi dari implementasi yang telah dilakukan.

5. Laporan

Seluruh tahapan penelitian didokumentasikan secara menyeluruh dalam bentuk laporan yang mencakup analisis mendalam, termasuk penilaian terhadap keunggulan dan

keterbatasan metode yang diterapkan. Dokumentasi ini diharapkan dapat menjadi referensi akademik yang bermanfaat bagi penelitian-penelitian selanjutnya.

1.7 Sistematika Penulisan

Untuk memberikan kerangka konseptual dan memfasilitasi proses penyusunan penelitian ini, disusun sistematika penulisan dengan struktur sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan merupakan bagian awal yang memaparkan gambaran umum mengenai topik yang diteliti. Di dalamnya dijelaskan latar belakang permasalahan, perumusan dan batasan masalah, tujuan yang ingin dicapai, manfaat penelitian secara akademik, metode yang digunakan, serta gambaran struktur penulisan. Bagian ini menjadi dasar penting untuk memahami arah dan fokus kajian dalam penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menyajikan tinjauan teori secara menyeluruh berdasarkan berbagai sumber literatur yang relevan. Kajian ini berfungsi sebagai dasar pemikiran dan pijakan konseptual dalam merumuskan pendekatan untuk menyelesaikan permasalahan yang diangkat dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan metode penelitian yang digunakan, mencakup langkah-langkah sistematis yang dirancang untuk menjawab permasalahan yang telah dirumuskan. Penjelasan dalam bab ini bertujuan untuk memberikan gambaran mengenai pendekatan, teknik dan prosedur yang ditempuh selama proses penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil penelitian yang diperoleh, disertai dengan analisis mendalam terhadap solusi atas permasalahan yang diteliti. Selain itu, bab ini juga memuat interpretasi terhadap temuan yang ada serta evaluasi terhadap keseluruhan proses penelitian yang telah dilakukan.

BAB V PENUTUP

Sebagai bagian penutup, bab ini memuat kesimpulan menyeluruh dari keseluruhan proses dan hasil penelitian, termasuk implementasi metode yang telah digunakan. Selain itu, disampaikan pula rekomendasi yang dapat menjadi acuan untuk pengembangan atau penelitian lanjutan di masa mendatang.

BAB 2

Tinjauan Pustaka

2.1 Penelitian Terdahulu

Penelitian sebelumnya telah berfokus pada pengembangan sistem enkripsi yang dapat mengatasi ancaman yang ada. Untuk mengatasi tantangan keamanan data medis, banyak penelitian sebelumnya telah berkontribusi secara signifikan pada kemajuan sistem enkripsi yang berlaku untuk data medis. Di antaranya adalah penelitian yang berfokus pada pengembangan sistem enkripsi gambar medis yang menggunakan metode enkripsi AES bersama pengkodean Base64 di tingkat byte. Pendekatan ini telah ditunjukkan untuk melindungi data gambar medis dari akses yang tidak sah, menghasilkan hasil yang menjanjikan sehubungan dengan keamanan dan kecepatan proses enkripsi (Malik et al., 2020).

Studi lain berfokus pada aplikasi keamanan untuk data rekam medis pasien yang berbasis Android, memanfaatkan kriptografi dengan metode AES dan Rivest Shamir Adleman (RSA), yang menekankan pentingnya melindungi data medis di perangkat seluler dan menawarkan solusi praktis untuk meningkatkan keamanan informasi pasien (Wahyudi & Romli, 2023).

Selain itu penelitian tentang penerapan keamanan data pada dokumen menggunakan algoritma kriptografi AES menunjukkan bahwa algoritma ini dapat secara efektif melindungi data sensitif dan memberikan wawasan tentang penerapan kriptografi di bidang pendidikan dan penelitian (Azhari, Perwitosari, et al., 2022).

Selanjutnya penelitian tentang penerapan algoritma Base64 512-bit sebagai inovasi teknik enkripsi untuk meningkatkan keamanan data pasien di rumah sakit (Muthaura & Kandiri, 2024). Sementara Base64 biasanya digunakan untuk pengkodean data, penelitian ini menyelidiki kemungkinan memanfaatkan metode ini dalam konteks enkripsi data. Pendekatan ini menawarkan alternatif yang layak untuk mengembangkan sistem informasi kesehatan, meningkatkan perlindungan data pasien yang sensitif. Studi ini berusaha untuk menunjukkan bahwa Base64 512-bit dapat meningkatkan perlindungan data dan memberikan solusi yang lebih mudah beradaptasi dan efisien dalam informasi perawatan kesehatan. (R et al., 2022) dalam bentuk Application Programming Interface (API) (Seputra et al., 2024).

Terakhir penelitian yang membandingkan teknik kedekatan Kode Rantai dengan algoritma LZMA dalam mengompresi gambar biner menawarkan wawasan berharga tentang efektivitas kompresi data, yang sangat penting untuk pengelolaan dan penyimpanan data medis, terutama untuk Pencitraan dan Komunikasi Digital dalam Kedokteran (Resdiansyah et al., 2021).

Dalam penelitian tersebut perbandingan dilakukan untuk mengevaluasi seberapa baik kedua metode tersebut mampu mengurangi ukuran file, sekaligus menjaga konsistensi informasi yang tersimpan di dalamnya. Teknik Kode Rantai bekerja dengan merepresentasikan objek dalam gambar menggunakan urutan arah titik-titik batas, sedangkan LZMA menggunakan prinsip statistik dan entropi untuk mencari pola-pola berulang dalam data dan menggantinya dengan representasi yang lebih ringkas. Hasil dari penelitian ini membantu memperkaya pemahaman tentang pilihan strategi kompresi yang paling sesuai untuk berbagai jenis data medis, terutama yang bersifat biner atau monokrom.

Tabel 2. 1 Ulasan Penelitian Enkripsi Data Medis

No	Penelitian	Fokus	Hasil
1	Development of Medical Image Encryption System Using Byte-Level Base64 Encoding and AES Encryption Method (Malik et al., 2020)	Pengembangan sistem enkripsi gambar medis menggunakan encoding Base-64 tingkat byte dan metode AES.	Proses encoding dan decoding bisa memperlambat waktu akses data.
2	A Reversible Data Hiding through Encryption Scheme for Medical Image Transmission Using AES Encryption with Key Scrambling (Sree et al., 2022)	Skema penyembunyian data reversibel untuk transmisi gambar medis menggunakan AES dengan pengacakan kunci.	Kompleksitas implementasi tinggi dan membutuhkan waktu komputasi lebih.
3	High Throughput and Low Area Architectures of Secure IoT Algorithm for Medical Image Encryption	Pengembangan arsitektur throughput tinggi dan area rendah untuk algoritma IoT yang aman pada enkripsi gambar medis.	Fokus pada arsitektur dapat membatasi fleksibilitas penggunaan pada platform lain.

No	Penelitian	Fokus	Hasil
4	Image Encryption Method Based on Improved ECC and Modified AES Algorithm (Hafsa et al., 2021)	Metode enkripsi gambar berdasarkan ECC yang ditingkatkan dan algoritma AES yang dimodifikasi.	Implementasi kompleks dan membutuhkan pengetahuan mendalam tentang ECC dan AES.
5	Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) (Azhari et al., 2022)	Implementasi pengamanan data pada dokumen medis menggunakan algoritma kriptografi AES.	Proses enkripsi dapat memakan waktu pada dokumen berukuran besar.
6	Lightweight digital imaging and communications in medicine image encryption for IoT system (Abdulzahra Hatem et al., 2023)	Enkripsi gambar digital ringan dan komunikasi dalam kedokteran untuk sistem IoT.	Keamanan mungkin tidak sekuat metode yang lebih kompleks.
7	Novel image encryption and compression scheme for IoT environment (Al Duhayyim et al., 2021)	Skema enkripsi dan kompresi gambar baru untuk lingkungan IoT.	Kompleksitas implementasi untuk berbagai perangkat IoT.

Tabel 2. 2 Ulasan Penelitian Kompresi Data Medis

No	Penelitian	Fokus	Hasil
1	A novel hybrid image encryption–compression scheme by combining chaos theory and number theory (Ahmad & Shin, 2021)	Skema enkripsi-kompresi gambar hibrida dengan menggabungkan teori chaos dan teori bilangan.	Kompleksitas tinggi dalam implementasi dan pemahaman teori.
2	A novel hybrid medical data compression using	Kompresi LZMA medis hibrida menggunakan	Tidak fokus pada aspek keamanan.

	huffman coding and LZW in IoT (Mohammadi et al., 2023)	pengkodean Huffman dan LZW pada lingkungan IoT.	
3	A secured compression technique based on encoding for sharing electronic patient data in slow-speed networks (Das & Rahman, 2022)	Teknik kompresi aman berbasis pengkodean untuk berbagi data pasien elektronik pada jaringan berkecepatan lambat.	Fokus pada jaringan lambat mungkin kurang relevan untuk jaringan modern berkecepatan tinggi.
4	Lossless Image Compression Using Different Encoding Algorithm For Various Medical Images (Rojas-Hernández et al., 2022)	Kompresi gambar lossless menggunakan berbagai algoritma pengkodean untuk berbagai gambar medis.	Efisiensi kompresi mungkin kurang optimal dibanding metode lossy.
5	An Optimal Lempel Ziv Markov Based Microarray Image Compression Algorithm (Sowmyalakshmi et al., 2021)	Algoritma kompresi gambar mikroarray berbasis Lempel Ziv Markov yang optimal.	Kurang fokus pada aspek keamanan gambar.
6	Exploring publish/subscribe, multilevel cloud elasticity, and data compression in telemedicine (Rodrigues et al., 2020)	Eksplorasi publish/subscribe, elastisitas cloud multilevel, dan Kompresi LZMA dalam telemedicine.	Kompleksitas tinggi dalam pengelolaan dan integrasi berbagai Teknik.

Tabel 2. 3 Ulasan Penelitian Digital Rights Management (DRM)

No	Penelitian	Fokus	Hasil
1	Security and privacy of electronic health records: Concerns and challenges (Keshta & Odeh, 2021)	Analisis keamanan dan privasi dari catatan kesehatan elektronik.	Tidak menawarkan solusi teknis langsung.

Tabel 2. 4 Ulasan Penelitian Implementasi Teknologi di Lingkungan IoT dan IoMT

No	Penelitian	Fokus	Hasil
1	High Throughput and Low Area Architectures of Secure IoT Algorithm for Medical Image Encryption (Mishra & Acharya, 2020)	Pengembangan arsitektur throughput tinggi dan area rendah untuk algoritma IoT yang aman pada enkripsi gambar medis.	Fokus pada arsitektur dapat membatasi fleksibilitas penggunaan pada platform lain.
2	Lightweight digital imaging and communications in medicine image encryption for IoT system (Abdulzahra Hatem et al., 2023)	Enkripsi gambar digital ringan dan komunikasi dalam kedokteran untuk sistem IoT.	Keamanan mungkin tidak sekuat metode yang lebih kompleks.
3	Lightweight encryption technique to enhance medical image security on internet of medical things applications (Hasan et al., 2021)	Teknik enkripsi ringan untuk meningkatkan keamanan gambar medis pada aplikasi IoMT.	Keamanan mungkin tidak sekuat metode yang lebih kompleks.
4	Secure and energy-efficient framework using Internet of Medical Things for e-healthcare (Saba et al., 2020)	Pengembangan kerangka kerja IoMT yang aman dan efisien energi untuk e-healthcare.	Implementasi mungkin memerlukan adaptasi pada berbagai perangkat dan platform IoMT.

No	Penelitian	Fokus	Hasil
5	Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things (Abbas et al., 2024)	Keamanan dan integritas data dalam analisis informasi kesehatan berbasis IoMT.	Tidak mencakup kompresi LZMA.

Temuan penelitian sebelumnya menunjukkan bahwa enkripsi AES dan Base64 efektif untuk melindungi data medis tetapi menyebabkan pembengkakan ukuran file, sedangkan teknik kompresi seperti Kode Rantai dan LZMA berhasil mengurangi ukuran file namun kurang memperhatikan aspek keamanan. Ini menunjukkan perlunya solusi baru yang menggabungkan kedua keunggulan tersebut untuk mengatasi tantangan keamanan dan efisiensi penyimpanan secara bersamaan.

Untuk mengatasi keterbatasan yang diidentifikasi dalam penelitian sebelumnya, penelitian ini bertujuan untuk mengembangkan pendekatan inovatif yang menggabungkan teknik enkripsi AES dengan metode kompresi LZMA sebagai kebaruan penelitian. Penggabungan kedua teknologi ini diharapkan dapat memberikan solusi holistik untuk melindungi data medis secara efektif sekaligus mengoptimalkan penggunaan ruang penyimpanan.

Enkripsi AES akan digunakan untuk memastikan keamanan tingkat tinggi terhadap akses tidak sah, sementara kompresi LZMA akan membantu mengurangi ukuran file tanpa mengorbankan integritas data. Dengan mengintegrasikan kedua teknik ini, penelitian ini berupaya menciptakan sistem yang tidak hanya aman tetapi juga efisien, sehingga dapat diimplementasikan dalam lingkungan medis dengan kapasitas penyimpanan terbatas. Pendekatan ini merupakan hal baru yang belum banyak dieksplorasi dalam konteks rekam medis elektronik, dan diharapkan dapat menjadi langkah maju dalam mengatasi tantangan keamanan dan efisiensi penyimpanan data medis.

2.2 Konsep Keamanan Data Medis

Keamanan data medis mengacu pada upaya melindungi informasi kesehatan dari akses tidak sah, manipulasi atau kebocoran. Data ini mencakup catatan pribadi pasien, riwayat

kesehatan, hasil tes, gambar medis dan informasi administratif lainnya. Tujuan utamanya adalah memastikan bahwa data tetap rahasia, tidak diubah oleh pihak tak berwenang dan selalu tersedia saat dibutuhkan. Keamanan ini sangat penting karena data medis bersifat sensitif dan memiliki nilai tinggi, baik secara personal maupun finansial. Selain itu regulasi seperti HIPAA dan GDPR menuntut perlindungan ketat terhadap data ini untuk menghindari sanksi hukum.



Gambar 2.1 Komponen rekam medis elektronik.

Gambar 2.1 menjelaskan data medis yang perlu dilindungi meliputi informasi identitas seperti nama dan nomor identitas, rekam medis berupa riwayat penyakit, diagnosis, hasil laboratorium. gambar medis terdiri dari X-ray dan MRI, serta data administratif seperti tagihan dan asuransi berbentuk JPEG dan TIF. Jika informasi ini jatuh ke tangan yang salah, risikonya bisa sangat serius. Misalnya pencurian identitas dapat merugikan individu secara finansial, sementara manipulasi data medis dapat menyebabkan kesalahan pengobatan yang membahayakan nyawa pasien. Informasi sensitif seperti diagnosis penyakit tertentu juga dapat digunakan untuk pemerasan atau diskriminasi sosial. Di sisi lain pelanggaran data juga dapat merusak reputasi institusi kesehatan dan menyebabkan kerugian finansial akibat denda atau hilangnya kepercayaan pasien.

Oleh karena itu keamanan data medis harus menjadi prioritas utama dalam sistem informasi kesehatan. Institusi perlu menggunakan teknologi seperti enkripsi dan kompresi untuk melindungi data, serta menerapkan kebijakan manajemen akses yang ketat. Dengan cara ini privasi pasien dapat terjaga, risiko pelanggaran data dapat diminimalkan dan kepatuhan terhadap regulasi hukum dapat dipenuhi.

2.3 Regulasi dan Kebijakan

Regulasi dan kebijakan memainkan peran penting dalam melindungi data medis dan memastikan bahwa institusi kesehatan mengikuti standar keamanan yang ketat. Regulasi ini dirancang untuk melindungi privasi pasien, menjaga integritas data dan mencegah penyalahgunaan informasi kesehatan. Selain itu regulasi juga memberikan kerangka hukum yang jelas bagi organisasi untuk mengelola data medis secara aman dan bertanggung jawab.

Ketika RME semakin banyak digunakan, regulasi menjadi instrumen utama untuk memastikan bahwa teknologi informasi diterapkan dengan cara yang etis dan sesuai dengan prinsip perlindungan data. Institusi kesehatan yang gagal mematuhi regulasi ini dapat menghadapi sanksi hukum, denda besar atau bahkan pencabutan izin operasi. HIPAA adalah regulasi yang berlaku di Amerika Serikat dan bertujuan untuk melindungi privasi pasien serta memastikan keamanan informasi kesehatan elektronik. Regulasi ini menetapkan standar untuk penggunaan, penyimpanan dan pengungkapan data medis. Institusi yang melanggar HIPAA dapat dikenai denda besar dan sanksi hukum.



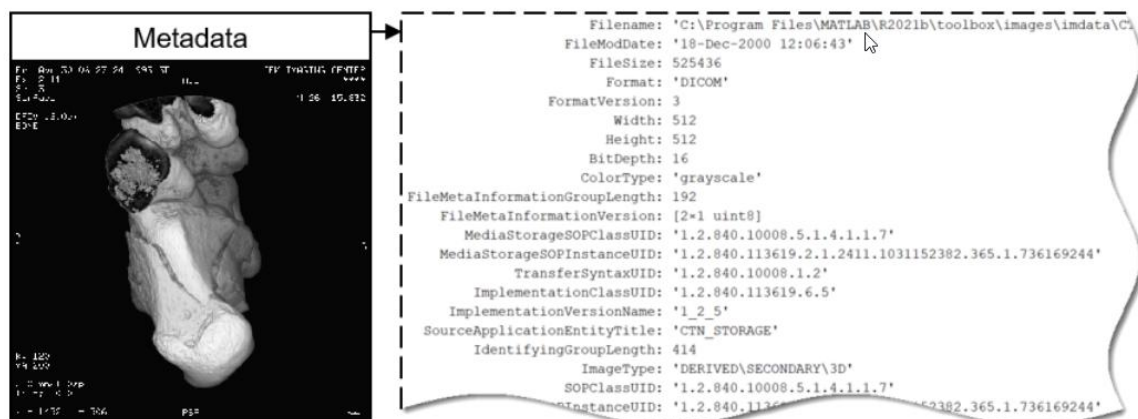
Gambar 2.2 Kategori data pribadi.

Gambar 2.2 menggambarkan dalam konteks nasional, pentingnya perlindungan tersebut semakin diperkuat dengan disahkannya UU PDP (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022), yang menjadi kerangka hukum utama dalam pengelolaan data pribadi di Indonesia. UU PDP menetapkan

prinsip-prinsip dasar pengelolaan data pribadi, termasuk transparansi, tujuan spesifik, batasan penyimpanan, integritas dan akuntabilitas. Salah satu aspek penting dalam UU ini adalah kewajiban bagi pengendali data untuk menerapkan langkah-langkah teknis dan administratif guna melindungi data pribadi dari akses tanpa izin, pengungkapan ilegal, serta modifikasi tidak sah sesuai Pasal 9 dan Pasal 36. Hal ini sangat relevan dalam konteks sistem informasi kesehatan digital, karena data medis elektronik termasuk file DICOM sering kali mengandung data pribadi khusus, yaitu data yang menyentuh ranah kesehatan dan memiliki risiko tinggi jika bocor atau disalahgunakan.

2.4 File DICOM

DICOM adalah format file standar yang digunakan untuk menyimpan, mengirim, dan menerima data medis terkait pencitraan seperti gambar radiografi, MRI, CT-scan, ultrasound dan lainnya. Format ini tidak hanya berisi gambar medis tetapi juga informasi metadata yang mendukung seperti identitas pasien, parameter perangkat medis, tanggal pemeriksaan, dan diagnosis awal.



Gambar 2.3 Struktur file DICOM.

Gambar 2.3 menjelaskan struktur file DICOM. Dirancang khusus untuk memastikan interoperabilitas antara perangkat medis dari berbagai produsen, sehingga memungkinkan pertukaran data medis secara aman dan efisien di seluruh sistem kesehatan. Format ini banyak digunakan di rumah sakit, klinik dan laboratorium medis karena kemampuannya menyimpan informasi medis dalam satu paket lengkap. File DICOM menjadi pilihan ideal untuk uji coba dalam penelitian ini karena beberapa alasan berikut:

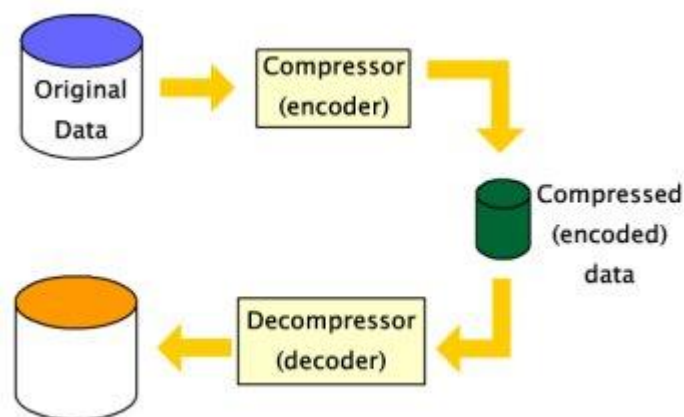
- File DICOM mencakup dua elemen utama yaitu gambar medis dan metadata terkait. Ini membuatnya sangat cocok untuk menguji teknik enkripsi AES dan kompresi LZMA,

karena kedua aspek tersebut berupa gambar dan metadata memerlukan perlindungan keamanan dan optimalisasi penyimpanan.

- b. Gambar medis sering kali memiliki ukuran file besar, sehingga pengujian dengan file DICOM dapat menunjukkan sejauh mana teknik kompresi LZMA dapat mengurangi ukuran file tanpa kehilangan kualitas atau informasi penting.
- c. File DICOM berisi informasi sensitif, termasuk identitas pasien dan hasil diagnosis, yang memerlukan perlindungan tingkat tinggi. Penggunaan enkripsi AES pada file DICOM dapat membuktikan bahwa teknik ini efektif dalam menjaga kerahasiaan data medis yang sangat kritis.

2.5 Teknik Kompresi

Kompresi data adalah teknik yang digunakan untuk mengurangi ukuran file tanpa kehilangan informasi penting, sehingga memungkinkan penghematan ruang penyimpanan dan meningkatkan efisiensi transmisi data. Dalam konteks keamanan data medis, teknik kompresi menjadi sangat relevan karena RME, gambar medis dan data lainnya sering kali memiliki ukuran file yang besar. Dengan menerapkan kompresi institusi kesehatan dapat mengoptimalkan penggunaan penyimpanan terutama di lingkungan dengan kapasitas terbatas tanpa mengorbankan integritas data.



Gambar 2.4 Alur kompresi.

Gambar 2.4 menjelaskan posisi salah satu algoritma kompresi yang banyak digunakan LZMA. LZMA dikenal karena kemampuannya untuk mencapai rasio kompresi yang sangat tinggi dibandingkan dengan metode tradisional seperti ZIP atau RAR. Algoritma ini bekerja dengan mengidentifikasi pola berulang dalam data dan menggantinya dengan representasi yang lebih pendek, sehingga menghasilkan file yang jauh lebih kecil.

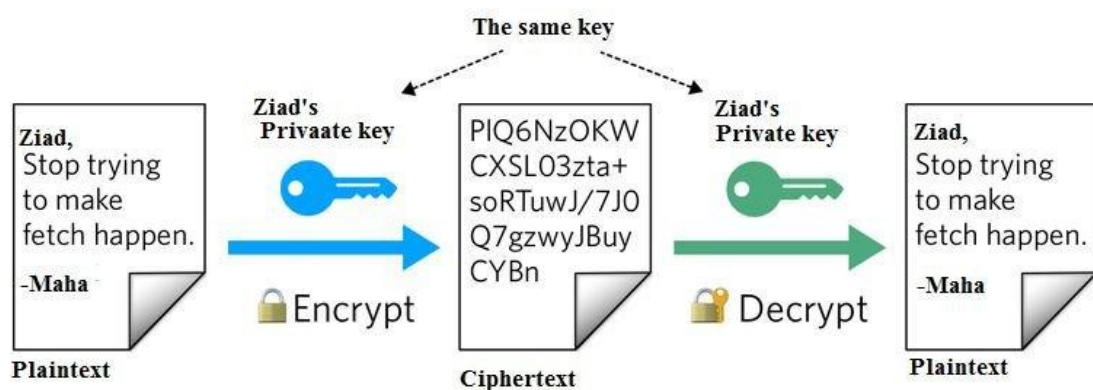
Selain itu LZMA juga menawarkan fleksibilitas dalam hal pemilihan tingkat kompresi, memungkinkan pengguna untuk menyeimbangkan antara ukuran file dan waktu pemrosesan.

Namun meskipun kompresi sangat efektif dalam mengurangi ukuran file, ada beberapa tantangan yang perlu dipertimbangkan. Salah satunya adalah potensi penurunan kualitas data jika menggunakan metode kompresi *lossy* atau kehilangan data. Meskipun metode ini tidak direkomendasikan untuk data medis sensitif seperti gambar radiografi atau rekam medis, beberapa penelitian sebelumnya telah mencoba menggunakannya untuk mengurangi ukuran file secara drastis. Di sisi lain metode kompresi *lossless* seperti LZMA lebih cocok untuk data medis karena memastikan bahwa tidak ada informasi yang hilang selama proses kompresi.

Dalam penelitian ini teknik kompresi LZMA dipilih karena kemampuannya untuk mengurangi ukuran file secara signifikan tanpa kehilangan data. Teknik ini akan digabungkan dengan enkripsi AES untuk menciptakan solusi yang tidak hanya melindungi data medis tetapi juga mengoptimalkan penyimpanan. Pendekatan ini bertujuan untuk mengatasi tantangan yang dihadapi oleh penelitian sebelumnya, yaitu kurangnya integrasi antara keamanan data dan efisiensi penyimpanan.

2.6 Teknik Enkripsi

Enkripsi adalah salah satu teknik utama yang digunakan untuk melindungi data medis dari akses tidak sah. Proses ini mengubah informasi asli (*plaintext*) menjadi format yang tidak dapat dibaca (*ciphertext*) menggunakan algoritma tertentu dan kunci enkripsi. Hanya pihak yang memiliki kunci dekripsi yang tepat yang dapat mengembalikan data ke bentuk aslinya. Dalam konteks keamanan data medis, enkripsi memastikan bahwa informasi sensitif seperti RME, hasil tes laboratorium atau gambar medis tetap aman selama penyimpanan maupun transmisi.



Gambar 2.5 Alur enkripsi.

Gambar 2.5 menjelaskan algoritma AES menggunakan kunci dengan panjang 128-bit, 192-bit, atau 256-bit, yang membuatnya sangat sulit untuk dipecahkan oleh pihak tidak berwenang. AES dikenal karena keamanannya yang tinggi dan efisiensinya dalam mengamankan data. AES sering digunakan dalam sistem kesehatan modern karena kemampuannya untuk melindungi data medis tanpa mengganggu fungsionalitas sistem.

Selain AES, ada juga metode enkripsi lain seperti *Rivest-Shamir-Adleman* (RSA) dan Base64, meskipun masing-masing memiliki kegunaan spesifik. RSA lebih sering digunakan untuk pertukaran kunci aman, sedangkan Base64 biasa digunakan untuk mengonversi data biner ke format teks agar lebih mudah ditransmisikan melalui jaringan. Namun dibandingkan dengan AES, metode ini kurang efisien untuk melindungi data skala besar seperti rekam medis elektronik.

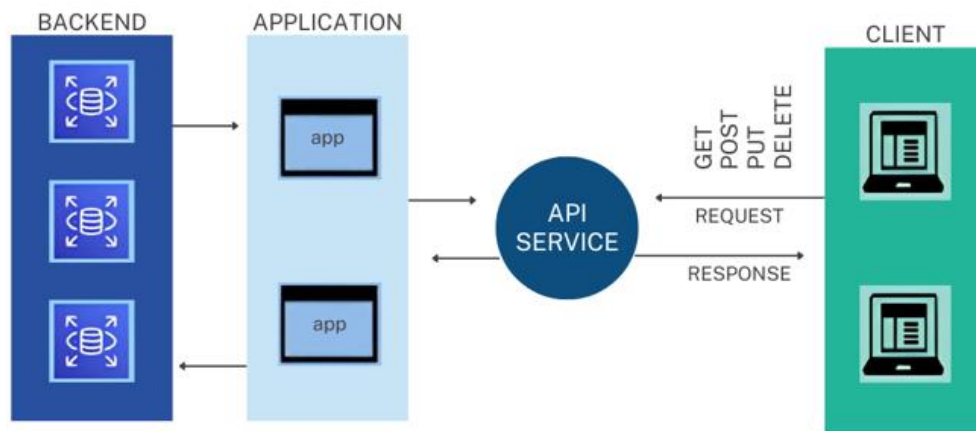
Meskipun enkripsi sangat efektif dalam menjaga kerahasiaan data, ada beberapa tantangan yang perlu dipertimbangkan. Salah satunya adalah ukuran file yang cenderung membengkak setelah proses enkripsi, terutama jika menggunakan metode tertentu seperti Base64. Hal ini dapat menimbulkan masalah dalam hal penyimpanan, terutama bagi institusi dengan kapasitas penyimpanan terbatas. Oleh karena itu penggunaan enkripsi harus dipadukan dengan teknik lain, seperti kompresi data untuk mengoptimalkan ruang penyimpanan tanpa mengorbankan keamanan.

Dalam penelitian ini teknik enkripsi AES menjadi pilihan utama karena reputasinya sebagai salah satu metode enkripsi paling aman dan efisien. AES akan digabungkan dengan teknik kompresi LZMA untuk menciptakan solusi yang tidak hanya melindungi data medis tetapi juga mengurangi ukuran file secara signifikan. Pendekatan ini diharapkan dapat mengatasi tantangan yang dihadapi oleh penelitian sebelumnya, yaitu keseimbangan antara keamanan dan efisiensi penyimpanan.

2.7 Implementasi API

API adalah antarmuka perangkat lunak yang memungkinkan dua atau lebih sistem berkomunikasi dan bertukar data secara efisien. Dalam konteks keamanan data medis, implementasi API menjadi sangat penting karena membantu mengintegrasikan berbagai komponen sistem informasi kesehatan seperti RME, aplikasi manajemen rumah sakit dan layanan penyimpanan cloud. Dengan menggunakan API institusi kesehatan dapat

memastikan bahwa data medis tetap aman, terstandarisasi dan mudah diakses oleh pihak yang berwenang.



Gambar 2.6 Konsep API.

Gambar 2.6 menjelaskan API dimanfaatkan untuk mengintegrasikan proses enkripsi, sehingga memungkinkan data medis diamankan sebelum dipertukarkan atau disimpan di platform yang berbeda. Salah satu contoh penggunaan API dalam sistem kesehatan adalah untuk mendukung *interoperabilitas* antar *platform* seperti pertukaran data antara rekam medis elektronik dan sistem manajemen rumah sakit

2.8 Integritas Data

Integritas data adalah salah satu aspek penting dari keamanan informasi, yang menjamin bahwa data tetap akurat, lengkap dan tidak mengalami perubahan atau manipulasi yang tidak sah selama penyimpanan, transmisi atau pengolahan. Dalam konteks keamanan data medis, integritas data sangat krusial karena setiap informasi yang tidak akurat dapat berdampak langsung pada diagnosis, pengobatan dan hasil perawatan pasien.

Misalnya jika rekam RME diubah secara tidak sah oleh pihak luar atau bahkan kesalahan sistem, hal ini dapat menyebabkan kesalahan fatal seperti pengobatan yang salah atau tindakan medis yang tidak sesuai dengan kondisi pasien sebenarnya. Oleh karena itu menjaga integritas data menjadi prioritas utama dalam sistem informasi kesehatan.

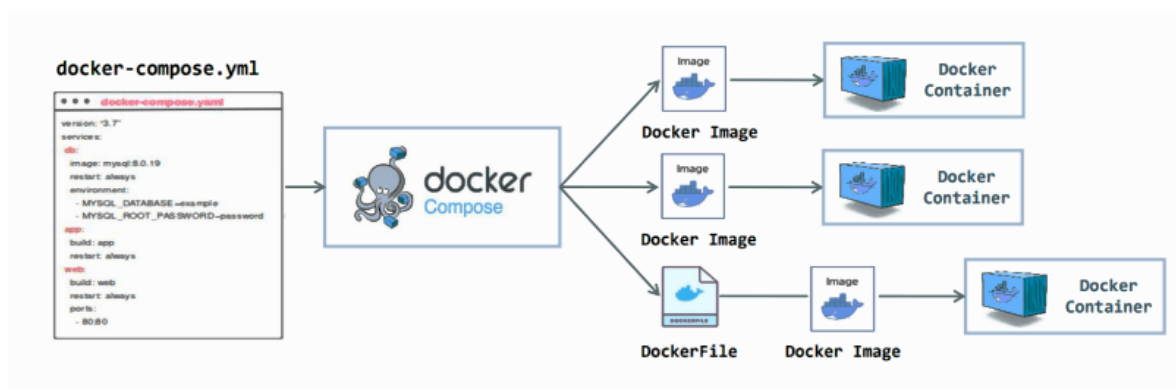


Gambar 2.7 Alur checksum MD5.

Gambar 2.7 digunakan untuk menghasilkan nilai unik (*hash value*) dari data. Setiap kali data dimodifikasi, *hash value* juga akan berubah. Dengan membandingkan hash value sebelum dan sesudah proses sistem dapat mendeteksi apakah ada perubahan yang tidak sah pada data.

2.9 Docker

Docker adalah *platform open-source* yang memungkinkan pengembang dan administrator sistem untuk membuat, mengirim dan menjalankan aplikasi dalam lingkungan terisolasi yang disebut *containers*.



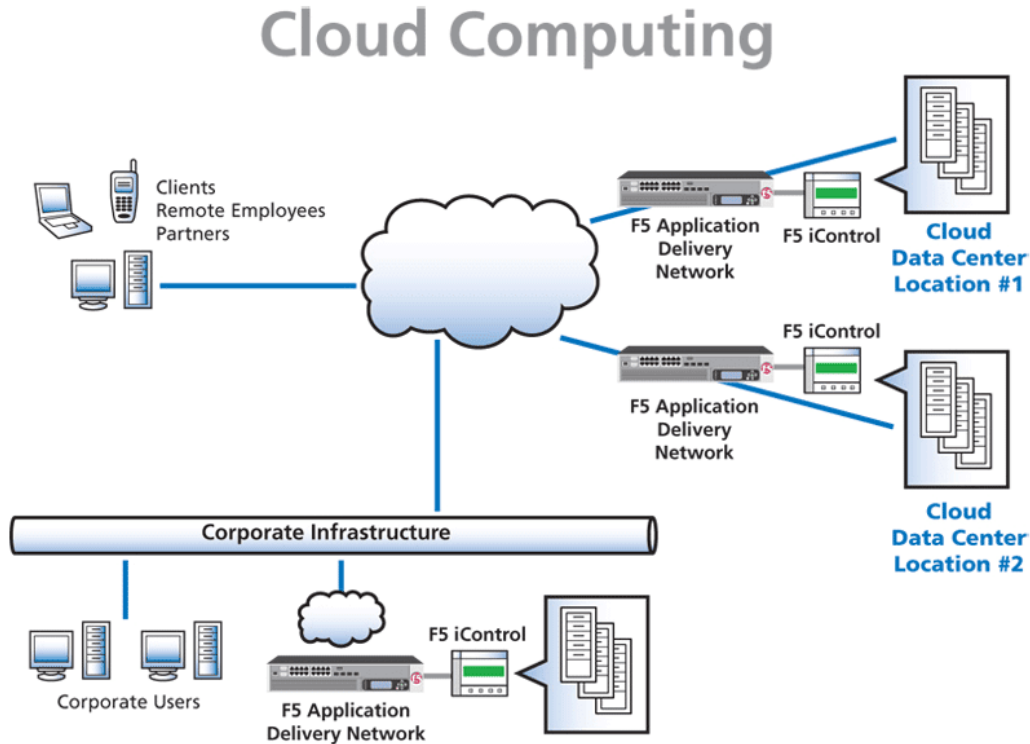
Gambar 2.8 Cara kerja Docker.

Pada gambar 2.8 kontainer docker berisi semua dependensi yang diperlukan oleh aplikasi termasuk kode, perpustakaan, alat dan konfigurasi, sehingga aplikasi dapat berjalan secara konsisten di berbagai lingkungan misalnya komputer pengembang, server uji coba, atau server produksi. Dalam penelitian ini Docker digunakan untuk:

- Membuat kontainer yang berisi lingkungan pengembangan lengkap, termasuk perangkat lunak enkripsi AES, algoritma kompresi LZMA dan implementasi API.
- Menyediakan lingkungan terisolasi untuk setiap modul seperti enkripsi, kompresi dan API, sehingga memastikan bahwa setiap proses dapat dijalankan secara independen tanpa gangguan.
- Mempermudah distribusi solusi kepada institusi kesehatan atau pihak lain yang ingin mengimplementasikan teknologi ini, tanpa harus khawatir tentang kompatibilitas sistem.

2.10 Cloud Computing

Cloud computing adalah model pengiriman layanan komputasi seperti *server*, penyimpanan, database, jaringan, perangkat lunak dan analitik melalui internet sebagai alternatif dari infrastruktur lokal atau on-premises.



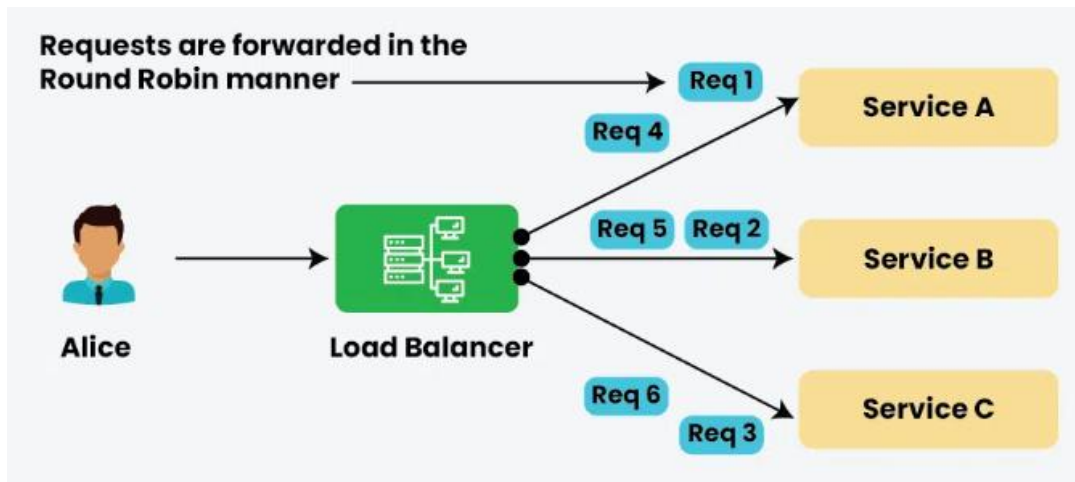
Gambar 2.9 Posisi *cloud computing*.

Gambar 2.9 Menjelaskan arsitektur *cloud computing*. Dalam konteks keamanan data medis, *cloud computing* menjadi semakin relevan karena banyak institusi kesehatan mulai beralih ke solusi berbasis awan untuk menyimpan RME, mengelola data pasien dan menjalankan aplikasi medis lainnya. Dalam penelitian ini *cloud computing* dapat dimanfaatkan sebagai berikut:

- Sebagai media penyimpanan untuk data medis yang telah dienkripsi menggunakan AES dan dikompresi menggunakan LZMA.
- Untuk mendukung implementasi API yang memungkinkan pertukaran data medis antar sistem secara aman dan efisien.
- Memberikan platform fleksibel bagi institusi kesehatan untuk mengakses dan mengelola data medis dari berbagai lokasi tanpa kehilangan kontrol atas keamanan data.

2.11 Load Balancing

Load balancing adalah teknik yang digunakan untuk mendistribusikan beban kerja (*request*) secara merata di antara beberapa server atau sumber daya komputasi. Tujuannya adalah untuk memastikan bahwa tidak ada satu server saja yang terbebani oleh jumlah *request* yang berlebihan.



Gambar 2.10 Cara kerja *load balancing*.

Gambar 2.10 menjelaskan mengurangi risiko kegagalan sistem atau penurunan kinerja. Dalam konteks sistem informasi kesehatan, load balancing membantu menjaga kelancaran operasi saat banyak pengguna atau aplikasi mengakses data medis secara bersamaan. Dalam penelitian ini load balancing dapat digunakan untuk:

- Mendistribusikan request dari pengguna yang mengakses data medis yang telah dienkripsi dan dikompresi ke beberapa server.
- Menjaga ketersediaan sistem selama periode dengan traffic tinggi, seperti saat banyak dokter mengakses rekam medis elektronik secara bersamaan.
- Memastikan bahwa setiap modul dalam sistem enkripsi AES, kompresi LZMA dan API dapat beroperasi secara optimal tanpa terganggu oleh beban kerja yang tidak merata.

2.12 Anti Forensik

Anti-forensik adalah serangkaian teknik dan metode yang digunakan untuk menghalangi atau mempersulit analisis forensik digital terhadap sebuah sistem atau data. Tujuan utama anti-forensik adalah membuat sulit bagi pihak lain seperti penyidik forensik digital, untuk mengumpulkan bukti atau informasi dari sistem yang telah disusupi atau diubah oleh pelaku

kejahatan siber. Teknik ini melibatkan penghapusan jejak, enkripsi, steganografi atau manipulasi log sistem untuk menyembunyikan aktivitas yang tidak sah.

Meskipun penelitian ini fokus pada melindungi data medis menggunakan teknik enkripsi AES, kompresi LZMA dan implementasi API, anti-forensik juga memiliki relevansi penting dalam konteks keamanan data medis. Dalam penelitian ini konsep anti-forensik dapat diterapkan sebagai berikut:

- a. Penghapusan Jejak Aktivitas: Memastikan bahwa setiap aktivitas yang dilakukan pada sistem misalnya proses enkripsi atau kompresi data tidak meninggalkan jejak yang dapat dieksploitasi oleh pihak tidak berwenang.
- b. Penyamaran Data: Menggunakan teknik steganografi untuk menyembunyikan data medis di dalam file lain yang tampaknya tidak mencurigakan, sehingga lebih sulit dideteksi bahkan jika file tersebut dicuri.
- c. Manipulasi Log Sistem: Menonaktifkan atau menghapus log sistem yang dapat memberikan petunjuk tentang akses atau modifikasi data medis oleh pihak tidak sah.

2.13 Efektifitas

Tingkat efektivitas suatu metode pengamanan data dapat dievaluasi melalui sejumlah parameter kritis. Parameter utama yang menjadi tolok ukur dalam penilaian ini meliputi keamanan data, yaitu kemampuan metode dalam melindungi informasi sensitif dari akses tidak sah serta ancaman keamanan siber. Selain itu, integritas data juga menjadi aspek penting untuk memastikan bahwa data tetap akurat dan tidak mengalami perubahan selama proses penyimpanan maupun transmisi.

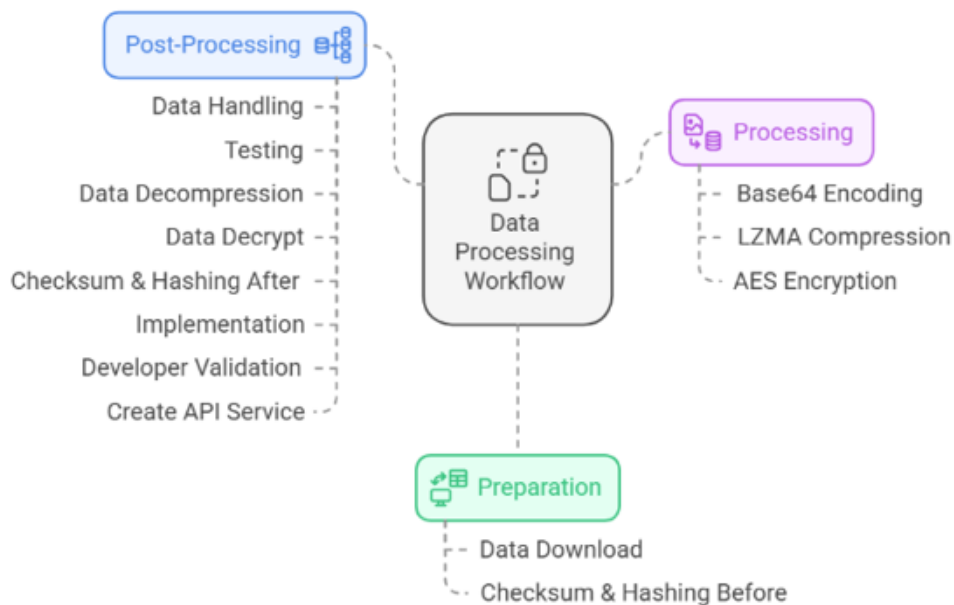
Keefisienan dalam hal penyimpanan diukur berdasarkan rasio kompresi yang dicapai oleh metode tersebut, yang menunjukkan kemampuannya dalam mengurangi ukuran file sehingga lebih optimal dalam penggunaan media penyimpanan. Aspek waktu eksekusi pun menjadi faktor relevan dalam menilai performa sistem, terutama dalam konteks kecepatan proses enkripsi dan dekripsi yang berpengaruh terhadap responsivitas aplikasi.

Selanjutnya penggunaan sumber daya sistem seperti konsumsi *CPU* dan memori, turut menjadi indikator dalam mengevaluasi efisiensi komputasional metode tersebut pada lingkungan implementasi nyata. Dalam penelitian ini, efektivitas penerapan kombinasi algoritma AES dan LZMA dalam pengamanan dokumen medis elektronik dianalisis dengan pendekatan yang bersifat kuantitatif dan kualitatif secara terstruktur. Pendekatan evaluasi ini sejalan dengan standar yang umum digunakan dalam kajian keamanan data serta kompresi informasi, sehingga memberikan gambaran yang objektif dan dapat direproduksi.

BAB 3

Metodologi

Bab ini menjelaskan metode yang digunakan dalam penelitian, sehingga rincian mengenai urutan langkah-langkah yang diambil dapat dipahami secara sistematis. Hal ini bertujuan untuk memberikan pedoman yang jelas dalam menyelesaikan permasalahan, menganalisis hasil penelitian, serta mengidentifikasi tantangan yang dihadapi.



Gambar 3.1 Alur pemodelan.

Gambar 3.1 menggambarkan alur kerja pengolahan dokumen medis elektronik menggunakan kombinasi teknik Base64 Encoding, kompresi LZMA, dan enkripsi AES. Setiap tahap mencakup persiapan data, encoding, kompresi, enkripsi serta verifikasi integritas melalui checksum MD5 sebelum dan sesudah proses. Diagram ini memberikan gambaran lengkap tentang bagaimana data rekam medis elektronik diolah secara aman dan efisien sesuai dengan ketentuan Permenkes No. 24 Tahun 2022.

3.1 Persiapan Data

Pemilihan sampel data dalam penelitian ini didasarkan pada karakteristik esensial data medis yang menuntut tingkat keamanan dan efisiensi penyimpanan yang tinggi, serta relevansi dengan peraturan perundang-undangan yang berlaku di Indonesia. Dataset utama yang

digunakan adalah file *Digital Imaging and Communications in Medicine* (DICOM) yang merupakan format standar internasional untuk menyimpan gambar medis seperti *Magnetic Resonance Imaging* (MRI), *Computed Tomography* (CT) Scan, *Ultrasound*, dan Radiografi. Alasan pemilihan tipe dataset ini khususnya DICOM karena file DICOM mengandung data dan informasi kesehatan yang termasuk dalam kategori Data Pribadi yang bersifat spesifik berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Data jenis ini memiliki potensi risiko dampak yang lebih besar jika terjadi pelanggaran. Oleh karena itu penelitian ini menekankan bahwa data yang digunakan bersifat anonim, yang berarti tidak mengandung informasi pribadi yang dapat mengidentifikasi individu, guna menjaga privasi pasien dan mematuhi prinsip kerahasiaan data yang diamanatkan oleh UU PDP dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Kebutuhan untuk menjamin keamanan, kerahasiaan, keutuhan dan ketersediaan data RME merupakan tujuan fundamental dari Permenkes No 24 Tahun 2022. Selain itu gambar medis terutama dalam format DICOM cenderung memiliki ukuran file yang besar. Volume data ini diperkirakan akan terus meningkat secara eksponensial seiring dengan implementasi Rekam Medis Elektronik secara nasional, yang diwajibkan bagi seluruh Fasilitas Pelayanan Kesehatan paling lambat 31 Desember 2023. Tantangan utama adalah bagaimana mengelola volume data ini secara efisien, mengingat kewajiban penyimpanan RME selama minimal 25 tahun dan potensi penggunaan sistem komputasi awan (*cloud computing*) sebagai media penyimpanan yang disebutkan dalam Permenkes No 24 Tahun 2022. Penelitian sebelumnya juga menunjukkan bahwa enkripsi saja dapat menyebabkan peningkatan ukuran file, yang menjadi kendala dalam aspek penyimpanan. Oleh karena itu penggunaan file DICOM memungkinkan evaluasi solusi yang tidak hanya aman tetapi juga efisien dalam penggunaan ruang penyimpanan.

Selain file DICOM penelitian ini juga menggunakan 95 file JPG dokumen medis dari pasien klinik dan 20 file TIF berisi hasil ekspor perangkat lunak DICOM Viewer. File JPG dan TIF ini merepresentasikan jenis data gambar yang lebih umum namun tetap terkait dengan konteks medis seperti dokumen administrasi atau hasil konversi gambar medis. Data ini juga dikategorikan sebagai Data Pribadi misalnya identitas pasien, nama lengkap sehingga pemilihannya bertujuan untuk memperluas cakupan pengujian metode terhadap beragam jenis dokumen visual yang mungkin ada dalam sistem informasi kesehatan dan juga memerlukan perlindungan data pribadi sesuai dengan UU PDP secara umum.

Jumlah sampel data yang digunakan yaitu 427 file DICOM dari situs 3dicomviewer.com, 95 file JPG dan 20 file TIF dari data klinik mitra secara kolektif cukup

memadai untuk tujuan penelitian ini, yang berfokus pada pengembangan dan evaluasi prototipe metode kombinasi enkripsi AES dan kompresi LZMA. Penggunaan berbagai jenis gambar medis seperti MRI, CT Scan, Ultrasound, Radiografi dalam format DICOM, ditambah dengan file JPG dan TIF, memastikan bahwa metode yang diuji dapat menangani karakteristik data yang beragam. Pengambilan 427 file DICOM dari pustaka terbuka memungkinkan pengujian kinerja algoritma pada volume data yang representatif untuk skenario individual, serta memberikan data yang cukup untuk analisis statistik. Hasil penelitian menunjukkan bahwa metode ini mampu mengurangi ukuran file secara signifikan dan mempertahankan integritas data pada sampel yang diuji. Meskipun disadari bahwa ukuran sampel yang relatif kecil dapat membatasi validitas temuan dan generalisasi hasil untuk skala yang sangat besar atau kondisi yang lebih kompleks, jumlah ini sudah cukup untuk membuktikan efektivitas konseptual dan teknis dari metode yang diusulkan. Penelitian ini bertujuan untuk menjadi referensi dan memberikan wawasan baru tentang kombinasi enkripsi dan kompresi dalam konteks data medis, yang telah tercapai dengan sampel yang ada.

3.2 Persiapan Sistem dan Alat

Seluruh proses penelitian ini dilakukan di dalam lingkungan Docker. Konfigurasi ini memastikan bahwa hasil penelitian dapat diisolasi, konsisten dan dapat diskalakan di berbagai platform. Dalam lingkungan Docker memungkinkan aplikasi untuk berjalan dalam kontainer terisolasi. Ini memberikan keuntungan dalam hal isolasi, konsistensi dan skalabilitas hasil di berbagai platform.

Sistem menggunakan prosesor Intel Core generasi ke-7 dengan 12 utas CPU dan RAM sebesar 16 GB. Konfigurasi ini memastikan bahwa sistem memiliki kapasitas pemrosesan yang cukup untuk menjalankan aplikasi dengan efisien. Aplikasi dijalankan dengan memetakan port 5000 pada host ke port 5000 di dalam kontainer, memungkinkan akses mudah ke aplikasi. Direktori kerja lokal juga dipetakan ke direktori /app di dalam kontainer, sehingga perubahan pada file lokal langsung tercermin di dalam kontainer. Aplikasi dijalankan menggunakan gambar Docker totorajo/flask:3.9-auto-reload, yang berbasis Flask. Gambar ini mendukung muat ulang otomatis, sehingga aplikasi dapat memuat ulang secara otomatis setiap kali ada perubahan kode.

Penelitian mengukur empat parameter utama: ukuran file, waktu pemrosesan, integritas data dan tingkat keamanan untuk menilai efektivitas kombinasi metode enkripsi AES dan kompresi LZMA. Berbagai pustaka Python digunakan untuk menambah

fungsionalitas aplikasi termasuk Flask sebagai kerangka kerja web utama, Cryptography untuk enkripsi dan dekripsi, Psutil untuk memantau proses sistem, Pandas untuk manipulasi data, Openpyxl untuk menangani file Excel, PyYAML untuk pemrosesan file YAML dan B2sdk untuk interaksi dengan Backblaze B2 Cloud Storage. Konfigurasi ini dirancang untuk memastikan replikabilitas lingkungan eksperimental, memperkuat validitas dan keandalan hasil serta mempromosikan kolaborasi. Konfigurasi ini dirancang untuk memastikan replikabilitas lingkungan eksperimental, memperkuat validitas dan keandalan hasil serta mempromosikan kolaborasi dan kemajuan lebih lanjut di masa depan.

Tabel 3. 1 Spesifikasi Hardware

Prosesor	Intel Core generasi ke-7, 12 thread CPU. Digunakan untuk mengevaluasi performa enkripsi dan kompresi file DICOM secara efisien dan akurat.
Memori (RAM)	16 GB RAM. Memberikan kapasitas memadai untuk menjalankan Docker, API Flask, serta proses enkripsi-kompresi secara bersamaan.

Tabel 3. 2 Software Untuk Proses Pengembangan

Sistem Operasi	Windows 11
Docker	Platform virtualisasi yang digunakan untuk mengisolasi aplikasi dan memastikan konsistensi eksekusi lintas platform.
Python	Bahasa Pemrograman utama dalam implementasi algoritma enkripsi AES, kompresi LZMA, encoding Base64, dan verifikasi integritas data.

Tabel 3. 3 Aplikasi Dan Pustaka Python

Flask	Framework web utama untuk membangun API endpoint sehingga developer dapat mengakses layanan enkripsi dan kompresi secara mudah.
Cryptography	Digunakan untuk proses enkripsi dan dekripsi menggunakan algoritma AES.
Psutil	Library untuk memantau penggunaan sumber daya sistem seperti CPU dan RAM selama proses enkripsi dan kompresi.

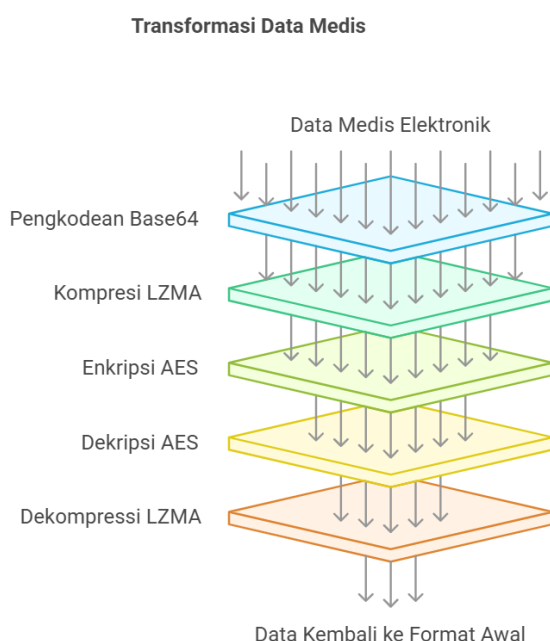
Pandas & Openpyxl	Digunakan untuk analisis data dan manipulasi file Excel sebagai pelengkap pelaporan hasil eksperimen.
PyYAML	Library untuk membaca dan menulis file konfigurasi dalam format YAML guna meningkatkan manajemen konfigurasi aplikasi.
b2sdk (Backblaze SDK)	Library untuk menyimpan dan mengambil file terenkripsi ke dan dari layanan cloud Backblaze B2 Storage.
Docker Image: totorajo/flask:3.9-auto-reload	Gambar Docker berbasis Flask yang dilengkapi fitur auto-reload untuk memudahkan pengembangan aplikasi.
Mapping Port: Host port 5000 → Container port 5000	Memungkinkan akses ke aplikasi melalui alamat http://localhost:5000
Mapping Direktori: Local directory → /app	Semua perubahan pada direktori lokal langsung tercermin di dalam kontainer Docker, mempermudah proses pengembangan dan testing aplikasi.

Tabel 3. 4 Parameter Evaluasi

Ukuran File	Diukur sebelum dan sesudah kompresi/enkripsi untuk mengetahui efisiensi penyimpanan.
Waktu Pemrosesan (Processing Time)	Waktu rata-rata enkripsi dan dekripsi per file dicatat untuk menilai performa metode.
Integritas Data	Diverifikasi menggunakan MD5 checksum untuk memastikan bahwa data tetap utuh setelah proses enkripsi-dekripsi dan kompresi-dekompresi.
Tingkat Keamanan	Dievaluasi berdasarkan ketahanan terhadap serangan bruteforce dan kemampuan algoritma AES dalam menyembunyikan data sensitif.

3.3 Simulasi Kasus

Penelitian ini mengadopsi pendekatan eksperimental untuk mengevaluasi seberapa efektif kombinasi teknik kompresi dan enkripsi dalam menjaga keamanan serta mengoptimalkan ukuran data medis elektronik. Dengan menggunakan metode ini penelitian bertujuan untuk menguji apakah penggabungan kedua teknik tersebut dapat melindungi data dari akses yang tidak sah sambil juga mengurangi ukuran file, sehingga memudahkan penyimpanan dan pengelolaan data medis. Pendekatan eksperimental ini memungkinkan peneliti untuk melakukan pengujian yang sistematis dan mendapatkan hasil yang dapat diandalkan mengenai kinerja kombinasi kompresi dan enkripsi dalam konteks data medis.



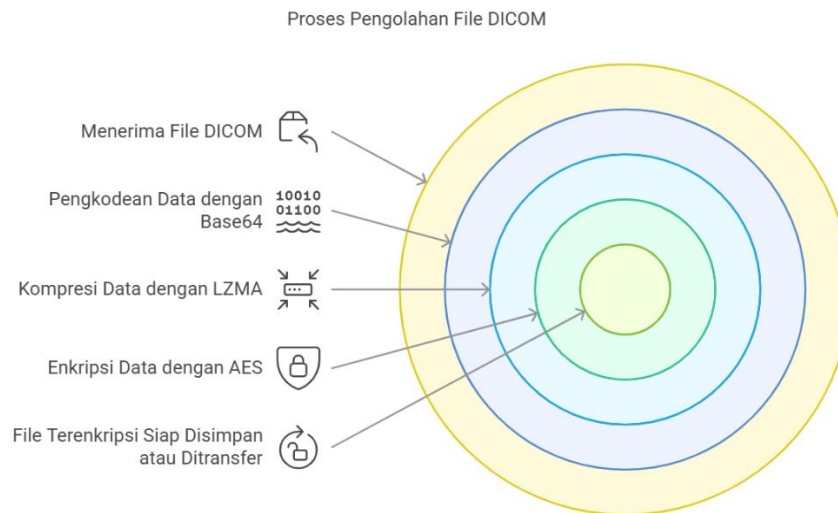
Gambar 3.2 Alur simulasi.

Gambar 3.2 menggambarkan alur simulasi proses pengamanan dokumen medis elektronik (RME) menggunakan kombinasi teknologi Base64 Encoding, kompresi LZMA, dan enkripsi AES. Setiap lapisan dalam diagram merepresentasikan tahapan utama dalam proses pengolahan data, mulai dari persiapan hingga penyimpanan akhir. Proses ini dirancang untuk memastikan keamanan, integritas, dan efisiensi penyimpanan data medis sesuai dengan ketentuan Permenkes No. 24 Tahun 2022 tentang Rekam Medis.

3.4 Pengolahan Data

Dalam penelitian ini API digunakan untuk mengelola proses penguploadan file DICOM, yang merupakan format standar untuk menyimpan dan mentransfer gambar medis. Melalui

API, pengguna dapat dengan mudah mengupload file DICOM ke server, di mana file tersebut akan diproses lebih lanjut. Proses ini mencakup pengkodean, kompresi, dan enkripsi data untuk memastikan keamanan dan integritas informasi medis yang sensitif. Dengan memanfaatkan API, penelitian ini tidak hanya meningkatkan efisiensi dalam pengelolaan data medis, tetapi juga memastikan bahwa data tersebut terlindungi dari akses yang tidak sah.



Gambar 3.3 Pemrosesan file DICOM.

Berdasarkan gambar 3.3 implementasi API ini dirancang untuk memungkinkan pengguna mengupload file DICOM dengan mudah. Ketika pengguna mengirimkan file DICOM melalui API, sistem akan menerima dan memproses file tersebut secara otomatis. Proses dimulai dengan mengkodekan data menggunakan algoritma Base64, yang mengubah data biner menjadi format teks yang lebih mudah ditangani. Setelah pengkodean, file yang telah dikodekan akan dikompresi menggunakan algoritma LZMA, yang merupakan metode kompresi tanpa kehilangan informasi, sehingga mengurangi ukuran file secara signifikan tanpa menghilangkan data penting. Selanjutnya file yang telah dikompresi akan dienkripsi menggunakan algoritma AES, yang memberikan tingkat keamanan tinggi untuk melindungi data dari akses yang tidak sah. Setelah proses enkripsi selesai, sistem akan menghasilkan file terenkripsi yang siap untuk disimpan atau ditransfer. Dengan demikian implementasi API ini tidak hanya memudahkan pengguna dalam mengupload file DICOM, tetapi juga memastikan bahwa data medis yang sensitif tetap aman dan terkompresi dengan efisien.

3.5 Implementasi dalam Bentuk API

Dalam skenario implementasi sistem dirancang sebagai sebuah layanan berbasis web dengan menggunakan arsitektur *Representational State Transfer Application Programming Interface* (RESTful API). Tujuan utama dari pembuatan API ini adalah agar developer, aplikasi klien maupun sistem lain dapat mengakses layanan enkripsi dan kompresi secara mudah dan terintegrasi. Berikut adalah tahapan yang diperlukan:

3.5.1 Lingkungan Pengembangan

Seluruh proses pengembangan dilakukan dalam lingkungan virtual menggunakan Docker, sebuah platform containerization yang memungkinkan isolasi aplikasi, konsistensi eksekusi serta kemudahan replikasi oleh pihak lain. Aplikasi web dibangun menggunakan framework Flask yang berbasis Python dan mendukung pengembangan cepat API sederhana namun fleksibel. Beberapa keuntungan dari pendekatan ini:

- a. Isolasi : Setiap komponen aplikasi berjalan dalam kontainer terpisah.
- b. Konsistensi : Konfigurasi lingkungan eksekusi tetap sama di semua mesin.
- c. Reprodusibilitas : Developer lain dapat dengan mudah menjalankan sistem tanpa konflik dependensi.

3.5.2 Arsitektur Sistem

Arsitektur sistem dirancang sedemikian rupa agar dapat menampung alur kerja berikut:

- a. Upload File
Klien mengirimkan file DICOM ke server melalui endpoint API.
- b. Encoding Base64
File DICOM yang merupakan data biner dikonversi menjadi format teks menggunakan encoding Base64 agar dapat ditransfer dan diproses lebih lanjut.
- c. Kompresi dengan Algoritma LZMA
Data hasil encoding dikompres menggunakan algoritma LZMA untuk mengurangi ukuran file sebelum proses enkripsi.
- d. Enkripsi dengan Algoritma AES
Data hasil kompresi kemudian dienkripsi menggunakan algoritma AES untuk memastikan kerahasiaan dan perlindungan dari akses tidak sah.
- e. Penyimpanan atau Pengiriman File Terenkripsi
File hasil enkripsi dapat langsung dikirim kembali ke klien atau disimpan ke penyimpanan cloud seperti Backblaze B2 Storage menggunakan library b2sdk.

f. Endpoint Dekripsi dan Dekompresi

Selain enkripsi, sistem juga menyediakan endpoint untuk proses balikkannya: dekripsi dan dekompresi file terenkripsi agar dapat direkonstruksi kembali sesuai kebutuhan pengguna.

3.5.3 Fungsi-Fungsi Endpoint API

Sebagai bagian dari produk API fungsi utama yang tersedia adalah:

1. Endpoint Upload: /process

Parameter:

```
{  
  "method": "encrypt",  
  "id_klink": "klinik-iii",  
  "id_antrian": "radiografi",  
  "folder": "test-pasien1",  
  "file": "[base64 file]"  
}
```

2. Endpoint Download: /decrypt

Parameter:

```
{  
  "method": "decrypt",  
  "id_klink": "klinik-iii",  
  "folder": "test-pasien1",  
  "filename": "[nama file .enc]"  
}
```

3.5.4 Integrasi Layanan Penyimpanan Cloud

Untuk mendukung skema penyimpanan berbasis cloud, sistem mengintegrasikan layanan Backblaze B2 Storage melalui library b2sdk. Dengan integrasi ini, file terenkripsi dapat langsung diunggah ke cloud storage setelah proses enkripsi selesai, sehingga mempermudah pertukaran dan penyimpanan data medis elektronik dalam jaringan digital. Dalam implementasi lapangan bisa diintegrasikan ke layanan object storage lain seperti Amazon S3 dan provider cloud lainnya.

3.6 Metode Pengujian

Pengujian dalam penelitian ini dilakukan menggunakan tiga metode yang berbeda untuk mengevaluasi efektivitas sistem yang dikembangkan. Penggunaan tiga metode berikut ini penting untuk memberikan pemahaman yang komprehensif mengenai kinerja dan keamanan sistem.

a. Metode Kolektif

Metode Kolektif ada sebanyak 542 file diuji secara bergantian dan paralel. Tujuan dari pengujian ini adalah untuk menganalisis respons penggunaan CPU dan RAM selama proses kompresi dan enkripsi, serta untuk mengukur hasil kompresi yang dicapai. Dengan menguji file secara kolektif, diharapkan dapat diperoleh data yang representatif mengenai bagaimana sistem beroperasi di bawah beban kerja yang tinggi, serta untuk mengidentifikasi potensi masalah yang mungkin muncul saat memproses sejumlah besar file secara bersamaan.

b. Metode Per File

Metode Per File Metode ini melibatkan pengujian setiap file secara individual melalui API untuk mengevaluasi cara kerja sistem dan memastikan integritas data. Dengan melakukan pengujian per file, diharapkan dapat diperoleh wawasan yang lebih mendalam mengenai bagaimana sistem menangani setiap file secara terpisah, serta untuk memastikan bahwa proses pengkodean, kompresi, dan enkripsi tidak mengubah atau merusak data asli.

c. Metode Dekripsi Bruteforce

Metode Dekripsi Bruteforce digunakan untuk menguji ketahanan enkripsi yang diterapkan pada data. Dengan melakukan serangan dekripsi bruteforce, diharapkan dapat diukur seberapa kuat algoritma enkripsi yang digunakan dalam melindungi data dari akses yang tidak sah. Pengujian ini penting untuk memastikan bahwa sistem yang dikembangkan dapat memberikan tingkat keamanan yang memadai terhadap potensi ancaman.

BAB 4

Hasil dan Pembahasan

4.1 Pengumpulan Data

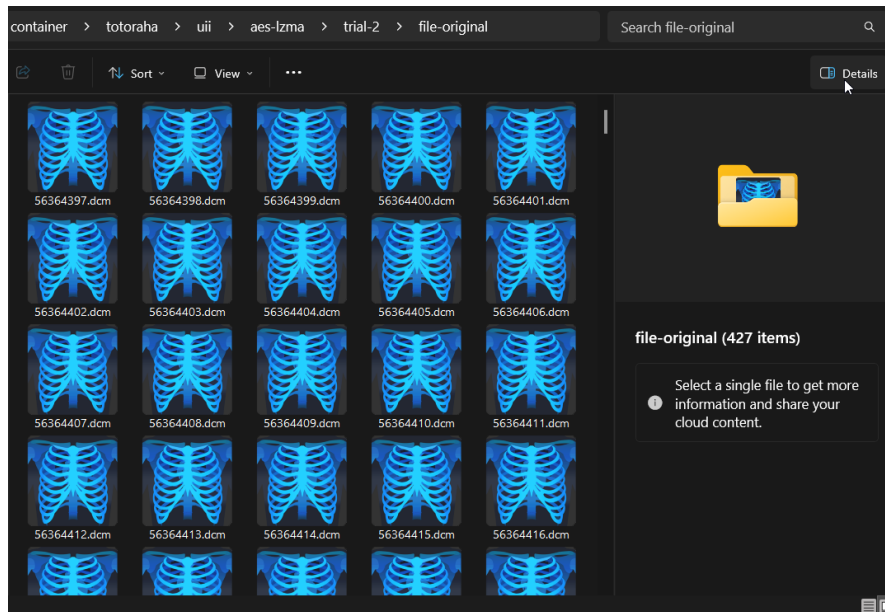
Pengumpulan data merupakan tahap penting dalam penelitian ini untuk memperoleh informasi yang relevan dan akurat dalam mengevaluasi penerapan metode penggabungan algoritma AES dan LZMA dalam mengamankan dokumen medis elektronik berformat DICOM. Tahap ini dilakukan secara sistematis dengan menggunakan dataset medis yang bersifat anonim dan tersedia secara publik untuk tujuan penelitian dan pendidikan.

Data yang digunakan dalam penelitian ini terdiri dari 542 file. File-file tersebut memiliki ukuran rata-rata sekitar 513 KB per file dan mencakup berbagai jenis pencitraan medis seperti MRI, CT Scan, Ultrasound dan Radiografi. Format DICOM dipilih karena merupakan standar internasional dalam penyimpanan dan pertukaran data gambar medis digital serta JPG dan TIF sering digunakan dalam sistem informasi kesehatan modern.

Proses pengumpulan data dimulai dengan mendownload file DICOM dari sumber yang telah disebutkan. Setelah itu dilakukan seleksi awal untuk memastikan bahwa file memenuhi kriteria tertentu antara lain:

- a. Keterkaitan klinis berupa file harus mewakili kondisi medis yang signifikan sehingga hasil analisis memiliki relevansi praktis.
- b. Anonymity data dengan syarat semua identitas pasien telah dihapus atau dianonimkan untuk menjaga kerahasiaan dan mematuhi prinsip etika penelitian.
- c. Kualitas gambar dengan ketentuan hanya file dengan resolusi tinggi dan detail jelas yang dipilih agar tidak mengganggu analisis visual dan integritas data.
- d. Ketersediaan akses berupa file harus mudah diunduh dan digunakan tanpa batasan lisensi, sehingga memudahkan replikasi oleh peneliti lain.

Semua file dimasukkan kedalam folder bernama file-original kemudian di analisa apakah jumlahnya sudah sesuai atau belum.



Gambar 4.1 Bahan file DICOM.

Gambar 4.1 memberikan gambaran bagaimana file dikelompokkan dan selanjutnya siap untuk dilakukan analisa. Setelah data DICOM berhasil dikumpulkan seluruh file kemudian melalui proses encoding menggunakan algoritma Base64 untuk mengubah data biner menjadi format teks yang lebih mudah diproses dan ditransfer. Selanjutnya data hasil encoding dikompres menggunakan algoritma LZMA untuk mengurangi ukuran file tanpa menyebabkan kehilangan informasi. Proses terakhir adalah enkripsi menggunakan algoritma AES untuk memastikan keamanan data dari akses tidak sah. Selama proses pengujian, dicatat beberapa parameter penting sebagai dasar evaluasi kinerja metode yaitu:

- Ukuran file sebelum dan sesudah kompresi dan enkripsi.
- Waktu eksekusi proses enkripsi dan dekripsi.
- Efisiensi kompresi (%).
- Penggunaan sumber daya sistem (CPU dan memori).
- Integritas data yang diverifikasi menggunakan MD5 checksum.

Data yang berhasil dikumpulkan kemudian disimpan dalam format terstruktur, baik dalam bentuk file log maupun database lokal, untuk mempermudah analisis selanjutnya. Selain itu seluruh proses pengumpulan dan pemrosesan data direkam dalam bentuk dokumentasi agar dapat direproduksi dan diverifikasi oleh pihak lain, meningkatkan transparansi dan validitas penelitian.

Dengan adanya pengumpulan data yang terencana dan dilakukan secara hati-hati, penelitian ini mampu memberikan bukti empiris mengenai efektivitas metode gabungan

AES dan LZMA dalam meningkatkan keamanan dan efisiensi penyimpanan dokumen medis elektronik, terutama dalam konteks implementasi berbasis cloud.

4.2 Persiapan Alat

Sebelum memulai proses pengujian dan implementasi metode enkripsi menggunakan algoritma AES dan kompresi dengan algoritma LZMA, dilakukan tahap persiapan alat dan lingkungan pengembangan. Tahap ini bertujuan untuk memastikan bahwa semua perangkat lunak, library dan infrastruktur pendukung telah tersedia dan siap digunakan sesuai kebutuhan eksperimen.

4.2.1 Lingkungan Pengembangan

Eksperimen dilakukan dalam lingkungan virtualisasi menggunakan Docker, sehingga memudahkan dalam hal isolasi aplikasi, konsistensi antar platform, serta skalabilitas hasil. Docker menyediakan container yang terisolasi memastikan bahwa aplikasi dapat dijalankan secara konsisten tanpa adanya konflik dependensi atau perbedaan lingkungan sistem operasi. Spesifikasi hardware yang digunakan dalam pengujian sebagai berikut.



Gambar 4.2 Spesifikasi hardware untuk pengembangan.

Gambar 4.2 menunjukkan spesifikasi hardware komputer yang digunakan oleh pengembang selama proses pengembangan dan pengujian sistem. Data mencakup nama komputer, sistem operasi, pabrikan, model, BIOS, prosesor, kapasitas RAM, penggunaan file halaman, serta versi DirectX. Spesifikasi ini penting untuk memastikan bahwa lingkungan pengembangan stabil dan sesuai dengan kebutuhan aplikasi yang dikembangkan.

4.2.2 Bahasa Pemrograman dan Library Pendukung

Implementasi keseluruhan proses enkripsi dan kompresi dilakukan menggunakan bahasa pemrograman Python, dikarenakan fleksibilitasnya dalam pengolahan data dan dukungan luas dari komunitas open source. Library Python yang digunakan meliputi:

- Flask sebagai framework web untuk membangun API endpoint agar developer dapat mengakses layanan enkripsi dan kompresi secara mudah.
- Cryptography sebagai library untuk enkripsi dan dekripsi data menggunakan algoritma AES.
- psutil untuk memantau penggunaan sumber daya sistem seperti CPU dan RAM selama proses berlangsung.
- Pandas dan Openpyxl digunakan untuk analisis data dan manipulasi file Excel jika diperlukan dalam pelaporan hasil.
- PyYAML untuk membaca dan menulis file konfigurasi dalam format YAML.
- b2sdk sebagai pustaka untuk menyimpan dan mengambil file terenkripsi ke dan dari layanan cloud Backblaze B2 Storage.

4.2.3 Penyusunan Struktur Direktori dan Mapping Port

Untuk mendukung pengembangan yang interaktif dan dinamis, direktori kerja lokal dipetakan ke direktori /app di dalam container Docker. Selain itu port 5000 pada host dipetakan ke port 5000 di dalam container, sehingga aplikasi web dapat diakses melalui alamat <http://localhost:5000>.

```
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.167.4-microsoft-standard-WSL2 x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

This message is shown once a day. To disable it please create the
/home/ubuntu/.hushlogin file.
ubuntu@LAPTOP-QJ1C9C04:~$ sudo docker run -itd \
  -p 5000:5000 \
  -v /mnt/d/container/totoraha/uii/api-storage:/app \
  --name container-aes-lzma \
  totorajo/flask:3.9-auto-reload
```

Gambar 4.3 Membuat container API.

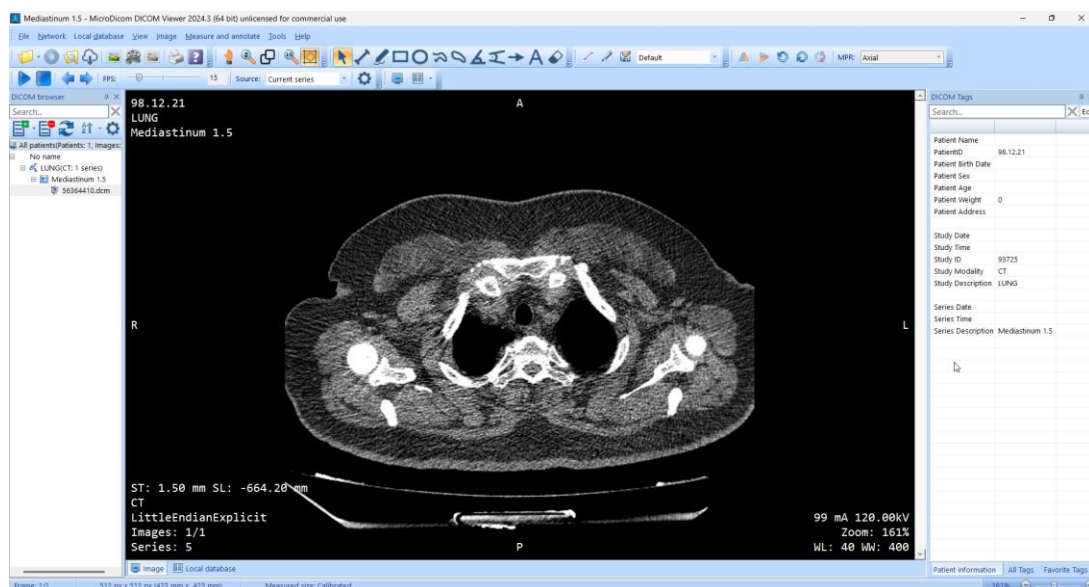
Gambar 4.3 memberikan penjelasan perintah Docker yang digunakan: `docker run -p 5000:5000 -v $(pwd)/app totorajo/flask:3.9-auto-reload`. Image Docker yang digunakan adalah `totorajo/flask:3.9-auto-reload`, yang berbasis pada framework Flask dengan fitur

auto-reload untuk memudahkan proses pengembangan karena aplikasi akan otomatis reload ketika ada perubahan kode.

4.2.4 Pengaturan File Konfigurasi dan Dataset

Sebelum dilakukan pengujian, seluruh file DICOM dimasukkan ke dalam struktur direktori proyek dan dibuat script Python untuk melakukan:

- Encoding file biner ke Base64.
- Kompresi menggunakan algoritma LZMA.
- Enkripsi menggunakan algoritma AES.
- Pengujian integritas data dengan MD5 checksum.
- Monitoring penggunaan sumber daya (CPU dan memori).



Gambar 4.4 Tampilan file DICOM.

Gambar 4.4 merupakan contoh salah satu file DICOM yang dibuka menggunakan DICOM Viewer untuk mengetahui seperti isi dari file sebelum dilakukan pengujian. Terlihat ada meta data disidebar kanan yang menjelaskan detail dari file DICOM.

4.2.5 Validasi Kebutuhan Pengembangan

Setelah seluruh tools dan library terinstal, dilakukan validasi awal untuk memastikan bahwa aplikasi dapat diakses dengan benar, semua library Python dapat diimport tanpa menghasilkan error, serta fungsi enkripsi, kompresi dan dekripsi berjalan sesuai harapan. Selain itu, dipastikan juga bahwa data DICOM dapat diproses sesuai dengan alur kerja eksperimen yang telah dirancang.

A screenshot of a terminal window with tabs for PROBLEMS, OUTPUT, DEBUG CONSOLE, TERMINAL, PORTS, and POSTMAN CONSOLE. The TERMINAL tab is active, showing a root user at a container ID prompt. The user enters 'pwd' and the output is '/app/trial-2/file-original'. Then, the user enters 'ls -l | grep "^-" | wc -l' and the output is '427'.

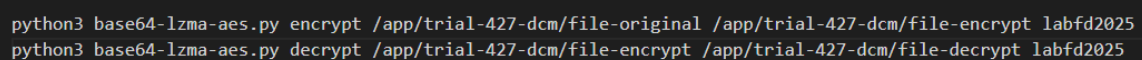
```
root@272a8a921aed:/app/trial-2/file-original# pwd
/app/trial-2/file-original
root@272a8a921aed:/app/trial-2/file-original# ls -l | grep "^-" | wc -l
427
root@272a8a921aed:/app/trial-2/file-original#
```

Gambar 4.5 File pada *Container*.

Gambar 4.5 menjelaskan cara bagaimana melakukan pengecekan. Persiapan tools ini menjadi fondasi penting dalam menjaga konsistensi dan reliabilitas hasil eksperimen. Dengan memanfaatkan lingkungan Docker dan integrasi library Python yang lengkap, proses pengujian dapat dengan mudah direproduksi oleh pihak lain, sehingga meningkatkan transparansi serta validitas penelitian secara keseluruhan.

4.3 Skenario dan Simulasi

Dalam rangka mengevaluasi penerapan metode penggabungan algoritma AES dan LZMA pada pengamanan dokumen medis elektronik berformat DICOM, dirancang sebuah skenario pengujian yang bertujuan untuk mengamati kinerja dan efektivitas metode tersebut secara menyeluruh. Skenario pengujian dilakukan dengan memproses file. Proses pengujian mencakup beberapa tahap utama yaitu encoding data menggunakan Base64, kompresi dengan algoritma LZMA, serta enkripsi menggunakan algoritma AES. Setelah proses tersebut selesai, dilakukan juga dekripsi dan dekompresi untuk memastikan bahwa data tetap utuh dan dapat direkonstruksi tanpa kerusakan.

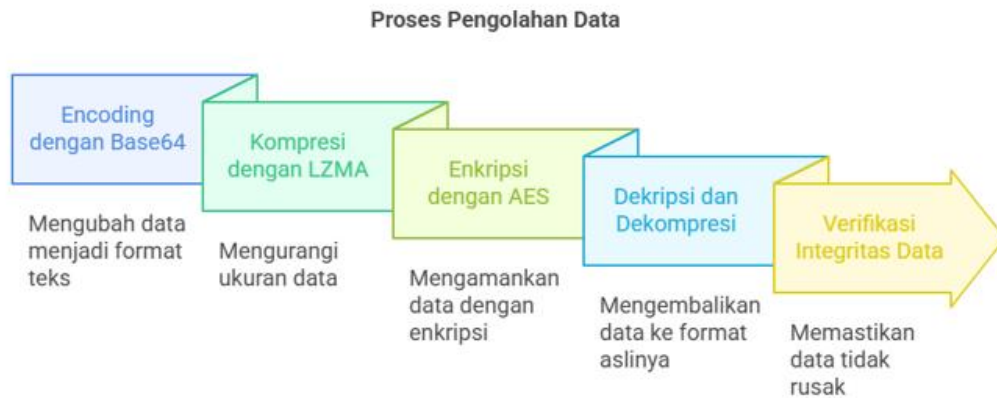
A screenshot of a terminal window showing two commands being executed. The first command is 'python3 base64-lzma-aes.py encrypt /app/trial-427-dcm/file-original /app/trial-427-dcm/file-encrypt labfd2025' and the second is 'python3 base64-lzma-aes.py decrypt /app/trial-427-dcm/file-encrypt /app/trial-427-dcm/file-decrypt labfd2025'.

```
python3 base64-lzma-aes.py encrypt /app/trial-427-dcm/file-original /app/trial-427-dcm/file-encrypt labfd2025
python3 base64-lzma-aes.py decrypt /app/trial-427-dcm/file-encrypt /app/trial-427-dcm/file-decrypt labfd2025
```

Gambar 4.6 Perintah enkripsi dan dekripsi.

Gambar 4.6 menjelaskan cara melakukan pengujian dilakukan dalam lingkungan Docker untuk memastikan isolasi aplikasi, konsistensi eksekusi, serta kemudahan replikasi oleh pihak lain. Selama pengujian berbagai parameter kuantitatif diamati untuk menilai performa sistem di antaranya adalah ukuran file sebelum dan sesudah proses, waktu enkripsi dan dekripsi, tingkat efisiensi kompresi, penggunaan sumber daya sistem seperti pemakaian CPU dan memori serta integritas data yang diverifikasi melalui nilai hash MD5 checksum.

Tahapan implementasi dalam penelitian ini menjelaskan alur proses pengolahan dokumen medis elektronik. Tujuan dari tahapan ini adalah untuk mengamankan data sekaligus mengurangi ukuran file agar lebih efisien dalam penyimpanan dan transfer.



Gambar 4.7 Alur proses pengujian.

Berdasarkan alur Gambar 4.7 File DICOM yang berupa data biner terlebih dahulu dikonversi ke format teks menggunakan Base64 encoding agar lebih mudah diproses dan ditransfer pada sistem yang hanya mendukung karakter teks, kemudian data hasil encoding dikompres dengan algoritma LZMA untuk mengurangi ukuran file tanpa menyebabkan kehilangan informasi, dan selanjutnya data yang telah dikompres dienkripsi menggunakan algoritma AES guna memastikan kerahasiaan dan melindungi data dari akses tidak.

Selain itu proses juga mencakup dekripsi dan dekompresi untuk memastikan bahwa data dapat direkonstruksi kembali secara utuh dan akurat. Pengujian integritas data dilakukan menggunakan MD5 checksum untuk menjamin bahwa tidak ada perubahan atau kerusakan data selama proses encoding, kompresi, dan enkripsi.

4.3.1 Fungsi Base64

Tahapan fungsi Base64 merupakan langkah awal dalam proses pengolahan dokumen medis elektronik sebelum dilakukan kompresi dan enkripsi. Dalam penelitian ini, file DICOM yang merupakan data biner dikonversi terlebih dahulu ke dalam format teks menggunakan encoding Base64. Tujuan dari tahapan ini adalah untuk memastikan bahwa data dapat lebih mudah diproses dan ditransfer melalui sistem yang hanya mendukung karakter teks, seperti protokol HTTP atau API berbasis web.

Encoding Base64 juga mempermudah integrasi dengan sistem penyimpanan cloud dan layanan API yang digunakan dalam penelitian, karena mengubah data menjadi

representasi *American Standard Code for Information Interchange* (ASCII) yang aman untuk transmisi. Hasil dari proses ini kemudian digunakan sebagai input untuk tahapan selanjutnya yaitu kompresi menggunakan algoritma LZMA.

4.3.2 Fungsi Kompresi LZMA

Tahapan fungsi kompresi LZMA merupakan proses penting dalam mengurangi ukuran file DICOM setelah melalui encoding Base64, sebelum dilakukan enkripsi dengan algoritma AES. Algoritma LZMA dipilih karena kemampuannya dalam memberikan rasio kompresi yang tinggi tanpa menyebabkan kehilangan informasi (*lossless compression*), menjadikannya sangat sesuai untuk dokumen medis yang membutuhkan integritas data yang sempurna.

Dalam penelitian ini, data hasil encoding Base64 dikompres menggunakan algoritma LZMA untuk meningkatkan efisiensi penyimpanan dan transfer data. Proses kompresi ini berhasil mengurangi ukuran file DICOM sebesar 40–50% secara rata-rata, Proses kompresi dilakukan secara sistematis:

- a. File DICOM yang telah diubah ke format teks Base64 dimasukkan ke dalam alur kerja kompresi.
- b. Algoritma LZMA menganalisis pola data dan merepresentasikannya dalam bentuk yang lebih ringkas.
- c. Hasil kompresi kemudian digunakan sebagai input untuk proses enkripsi selanjutnya.

Kompresi juga membantu mengurangi beban penyimpanan, terutama dalam sistem berbasis cloud, serta mempercepat proses pengiriman data tanpa mengorbankan kualitas atau integritas informasi medis. Selain itu, kompresi sebelum enkripsi memberikan manfaat tambahan berupa lapisan keamanan tambahan, karena data yang terkompresi sulit dibaca oleh pihak tidak sah meskipun berhasil diretas.

4.3.3 Fungsi Enkripsi AES

Setelah proses kompresi selesai tahapan berikutnya adalah enkripsi data menggunakan algoritma AES, sebuah algoritma simetris yang dikenal memiliki tingkat keamanan yang sangat tinggi. AES mendukung panjang kunci hingga 256 bit, menjadikannya salah satu metode enkripsi standar dunia yang banyak digunakan dalam aplikasi sensitif seperti pertahanan, perbankan, dan khususnya dalam perlindungan data medis elektronik.

Dalam penelitian ini algoritma AES digunakan untuk mengenkripsi data DICOM yang telah dikompresi agar dapat terlindungi dari akses tidak sah. Pengujian menunjukkan bahwa waktu enkripsi rata-rata adalah sekitar 0,2–0,3 detik per file, dengan penggunaan CPU mencapai 94,05% saat proses tersebut berlangsung. Meski demikian, konsumsi memori tetap rendah, yaitu sekitar 92,95 KB per file. Proses enkripsi AES berjalan sebagai berikut:

- a. Data hasil kompresi dimasukkan ke dalam modul enkripsi.
- b. Kunci enkripsi AES 128, 192 atau 256 bit digunakan untuk mengacak data sehingga tidak dapat dibaca tanpa kunci yang sesuai.
- c. Mode operasi yang digunakan dalam penelitian ini adalah GCM atau CBC, yang memberikan keunggulan dalam hal keamanan sekaligus efisiensi pemrosesan.

Hasil enkripsi kemudian disimpan atau dikirim dalam format terenkripsi. Untuk membuka kembali data tersebut, diperlukan proses dekripsi menggunakan kunci yang sama. Pengujian integritas data menggunakan MD5 checksum menunjukkan bahwa nilai hash sebelum dan sesudah proses enkripsi-dekripsi sama persis, membuktikan bahwa data tetap utuh dan aman. Penerapan AES dalam penelitian ini berhasil menunjukkan bahwa metode ini sangat efektif dalam melindungi data medis elektronik dari ancaman kebocoran atau manipulasi, sekaligus tetap menjaga performa sistem dalam batas wajar.

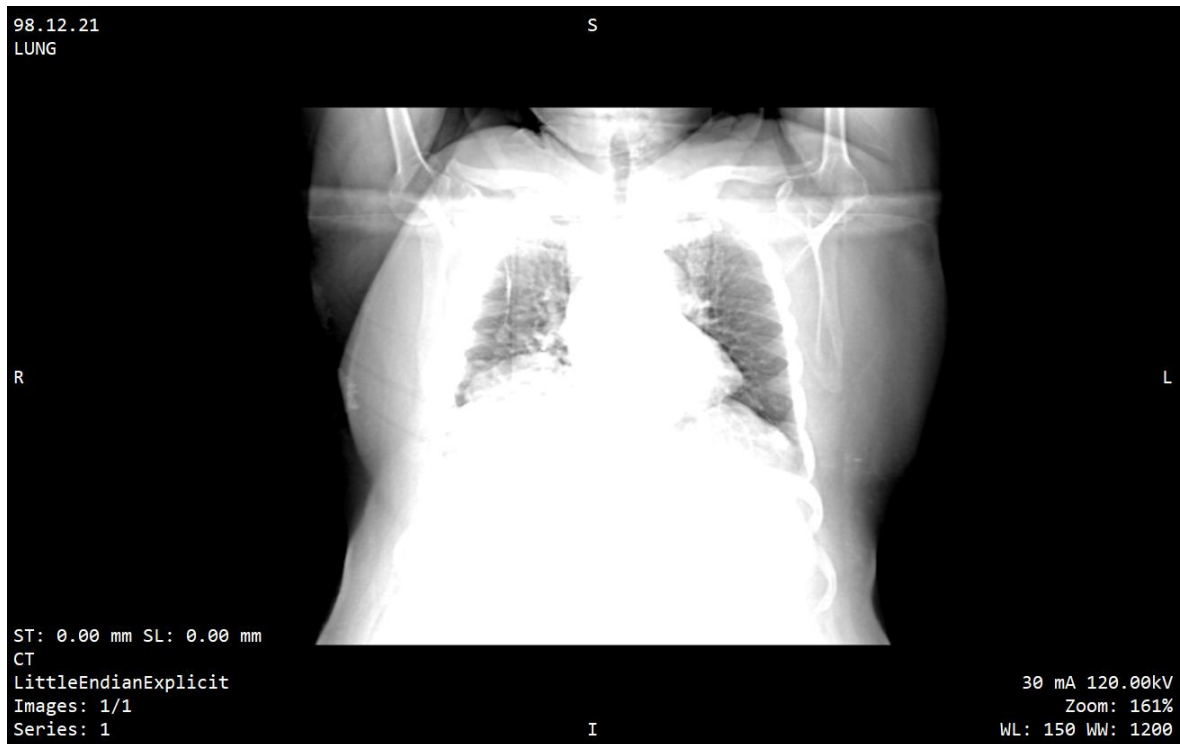
4.4 Tahapan Pengujian

Tahapan pengujian dalam penelitian ini bertujuan untuk mengevaluasi efektivitas kombinasi algoritma AES dan LZMA dalam menjaga keamanan sekaligus meningkatkan efisiensi penyimpanan dokumen medis elektronik berformat DICOM. Pengujian dilakukan secara sistematis untuk memastikan bahwa metode yang diimplementasikan mampu memberikan perlindungan terhadap akses tidak sah, mengurangi ukuran file tanpa menyebabkan kehilangan informasi, serta tetap menjaga integritas data selama proses encoding, kompresi, enkripsi dan dekripsi.

4.4.1 Pengujian File DICOM

Pengujian file DICOM dilakukan sebagai bagian dari evaluasi menyeluruh terhadap penerapan kombinasi algoritma AES dan LZMA dalam pengamanan dokumen medis elektronik. Tujuan utama dari pengujian ini adalah untuk mengevaluasi apakah metode yang diusulkan mampu mengamankan data secara efektif, mengurangi ukuran file tanpa

menyebabkan kehilangan informasi, serta memastikan integritas data tetap terjaga selama proses encoding, kompresi, enkripsi dan dekripsi.



Gambar 4.8 File DICOM sebelum enkripsi.

Gambar 4.8 menampilkan representasi visual dari file dalam bentuk aslinya sebelum melalui tahapan pengolahan seperti encoding Base64, kompresi LZMA, dan enkripsi AES. File DICOM merupakan format standar internasional yang digunakan untuk menyimpan dan mentransmisikan data pencitraan medis, seperti hasil CT scan, MRI, X-ray atau ultrasound. Dalam penelitian ini file DICOM digunakan sebagai sumber data utama untuk menguji efektivitas metode gabungan enkripsi dan kompresi dalam meningkatkan keamanan dan efisiensi penyimpanan dokumen medis elektronik. Pada gambar ini file DICOM ditampilkan dalam bentuk visual asli, yang biasanya berupa citra medis digital yang dapat diinterpretasikan oleh manusia. Misalnya jika file tersebut berasal dari CT scan maka akan terlihat struktur internal tubuh pasien seperti organ-organ vital atau area yang terkena kondisi patologis. Hal ini penting karena file DICOM awal harus tetap utuh dan dapat dibaca secara visual sebelum diolah menggunakan algoritma enkripsi dan kompresi. Penampilan file DICOM dalam bentuk aslinya ini menjadi titik referensi penting untuk memastikan bahwa proses enkripsi dan kompresi tidak merusak integritas data. Setelah melalui serangkaian proses pengamanan, file DICOM akan diubah menjadi format yang tidak dapat dibaca oleh manusia secara langsung, tetapi tetap aman dari akses tidak sah. Gambar ini juga membantu

menjelaskan pentingnya verifikasi integritas data melalui checksum MD5 sebelum dan setelah proses seperti yang telah dilakukan dalam penelitian ini.

```
File '/app/trial-427-dcm-small/file-original/56364823.dcm' telah dienkrpsi
Checksum MD5 Awal: df60a76c2d0f91aeda9da87c3a945875
Checksum MD5 Enkrpsi: c91b50222f167af6ac27fe68540bd7c5
Ukuran File Asli: 513.39 KB
Ukuran File Setelah Kompresi: 230.97 KB
Penghematan Ukuran: 55.01%
Ukuran File Terenkripsi: 231.02 KB
Durasi Enkrpsi: 0.21 detik
Penggunaan CPU: 91.63%
Penggunaan Memori: 0.00 KB
Total files processed for encryption: 427
root@272a8a921aed:/app#
```

Gambar 4.9 Proses enkripsi.

Gambar 4.9 menunjukkan hasil proses enkripsi dan kompresi file DICOM dengan menggunakan algoritma AES dan LZMA. File yang dienkrpsi adalah 56364823.dcm, yang merupakan bagian dari dataset rekam medis elektronik. Hasilnya mencakup berbagai metrik penting, seperti ukuran file sebelum dan setelah kompresi, penghematan ruang penyimpanan, durasi waktu enkripsi, serta sumber daya sistem yang digunakan.

```
IELa0Y, [t0[<0x1b>]*<0x03>/PÁ;w*E<0x13>-tEÁV<0xa0>P'YKD<0x81><0xad>/"ø"±æx\à
<0x14>f.Ö"²UXoA..ö<0x01>Y$<0x1d>*Yp<0x1c>Iir],4E..<0x02>«EñY<0x7f>-<0x1b>cED<0xad>]ö KpLN<0x01><0x16>Äè~Ñ*g1iÄYñusY6l2ñ$;0+«
±0y]d<0xa0>*1fy00tA{b<0x90>fø<0x9d>R00%5<0x90>e~<0x81>CZ}jBúeoYP<0x08>0GéA<0x17>§«<0x90>c
<0x8d>æUí<0x1e>N1c>QR<0x11>(<0x08>É<0x1b>m>üxü8i<0x1a>B<0x0e><0x08>ÉdAXt+ð<0x06><0x13>1äj~D0]1A~a<0xc0>""<0x1a>K~ø=b000.°q<0x
Bj>äY²<0x17><0x07>{"D<0x0e>DB<0x17>00ø<0x8d>ø<0x1b><0x1e>:§<0x90>ø[;i(ýé p<0x1d>Z+<0x7f>oð<0x7f>~<0x05>Á
S<0x0b>*~V<0x07>B5_~"üü*<0x10><0xc0>.ä`¥iH\;f'Uü9Bq'!<0x16><0x1b>¥bcZ~Z<0x00>çY-<0x16>þmaéñWwq|èqÉ<0x13>2
<0x0b><0x03>Ü„tH²%atA7J<0x9d><0x02>)kx-<0x03>qæ?+fn0ZMV<0x18><0x1f><0x01>¥Ä4sPX:KÈö"±t<0x06>~Än7+!"ñ7TX<0x05>k><0xa0>ÊPQ;+
IÁ<0x11>BµçÆ}.<0x90>~<0x00><0x1c>Ü<0x8f>-EöP
&É»<0x10><0x12>6(<0x1a>øp6Ü'<0x1d><0x8d>~ü(<0x8f><0x1e>I<0xad>.bâ<0xa0>ækK
<0x1e>mIKn0+ÜNTi/AÉÜ<0xad>;77
i1Pø'ü<0x0f>8%fc<0x7f>°<0x06>w%]~SYW<0x1d>2<0x8d>Píø<0x03>Ö<0@>ñqhi<0x18>z<0x14>f&«<0x8f>"â,2¥B'50f<0x11><0xad>Šâ±é$<0x0e>°
ÜB ³i~Äe0üÄ000E#i<0x04>-M
C6Jfaiz<0x0b>|a~Z;Üø"yJD'<0x07>³$<0x8d>#JA;gA.<0x08>*A2ü00~c<0x01><0x1a>pü&iLE\|
TT'¥Ks;me¥E.'j""ñ$)<0xc0><0xad>âæUÜ,BB$<0x90>'nD$<0x00>#zp,ð)<0x1a>PÖ<0x15>fDæµ<0x8f>^éüB.Ä<0x01>8c0<0x02>.>.IÜ.G!²[I5öcl{à
"buä"²ASNc00i@'g'LS<0x8d>r0EñY<0x1a><0x05>Y<0x1b>Ä-iñ<0x06>C&.L*ö!ð<0x11><0x8f>UFY1<0x0f>r0Ä<0x11><0x0f><0x18>rEY<0x8f><0x0
,0A'<0x13>é,<0x16>Ö<0x07>ñâ#<0x9d>þ<0x00><0x81>>{É,I9vIS<-<0x04>'Ö*SR&_NÁE1)XÉR<0x01>É"Ö<0x90>«~I~V$<,°ýÜzüü@t60E+#+~pÜwü<0
u+{pU<0x03>;<0x8d>q&fP7IIZâ<0x05><0x1e>æ*rxr,
umæet*«=~<0xa0>fE@MEÄN<0x0e>3<0x15>³pÜö<0x03>ü]ÇÉ[0'6dq'nc<0x9d>?çEÖv6ø"Z<0x10>Öv%<0x05>³Jöfi00)7ibÉE<Z~Î@I%<0x1e>Ä26yNE%X
<0x0e>w<0x1f> <0x90>Xyáyo'<0x1d><0x0b>7<0xa0>â%}0]i:00iY<0x18>höy-j/87Épo:-æ~<0x04><0x14>PjRD.&K0<0x1c>CaY-'0Üo/
TBZög'ú!M&š°ç}<0x13>°zd*ÍC=6AéAB...+~ü<0x16>T=<0x1a>iSpa<0x0c>D5ð°3nRIéö-fú(Y<-<0x08>§<0x0b>X_ia<É¶090ðèYúhc<0x07>l0Z%<0x15>;
<0x18>ü¶'<0x12><0x16><0x19><0x04><0x18>TÖW<0x12>m%á<0x01>6phb<0x15><0x9d><0x1c>Kè-&ny&ç<ç;H<0x12><0x1f>¥.æð
¶èðæ«èç'Cí<0x0e>çp5%Èz;h'zw_ÍU,6E;<0x01>||qG~ /²p<0x1e>Ä<0x14>*t«BÆ{<0x11>XµBftá!@kOyoE(D('8<0x18><0x8f>4„Zn5-x0b~•Ä<0x01
dié&a1ai'a<0x1f>-ÜEY<0x0b>Öövt'ñ<0x15>ðtT<0x90>i]0t<0x1f>ÜéG<0xa0>ñe<ÄÜÄ<0x1f>=<ÄT)B<0x1d>00q$;%'µX0c-Y<0x0c><0x8f>š<0x1a>
±<0x1e>»%Ns|+³ÑP"0x15>sAK<0x1e>nY<0x01>1Jáá~w]kU<0x17>*t<0x0e>§<0xad>XN"
øY!07k'ün'as<0x17>""<0xad>...tè ääÉ*<0x18>äiè01ø;çb YÜ<0x7f>Ujg56øc~NB
N"ä03éhö<0x0c><0x81>yñk<0x9d>@<17%<0x1e>EÉjéá<0x8d>Ü-ð5<0x18>IK|,H<0x00><0x17>¶0ç<0x04>z<0ñ05É&î{yewQ8For05Zb/,gE'üá
<0x0e>~"ý^5a0 ä%<0x8d>Ü] Yw,<0x0c>ðc'Äâ « ü^$â#~'<0x0e>÷-ÇâF"ñUñ;ø0.}ø'Æ<0x10>puÜ0:/e;AQ'j0""$§³<0x8d>ÉyQiè~Ä<0x08>øð&fYr
N<0x08>){<0x11><0x0f>è0ä"6!+,1šqf<0x10>jq-<0x00><0x00>ç~P<0x00>ÉLç6~ÜZ³<0x01><0xa0>ñæ0<0x10>ss6³<0x02>öüè<0x9d>04)
```

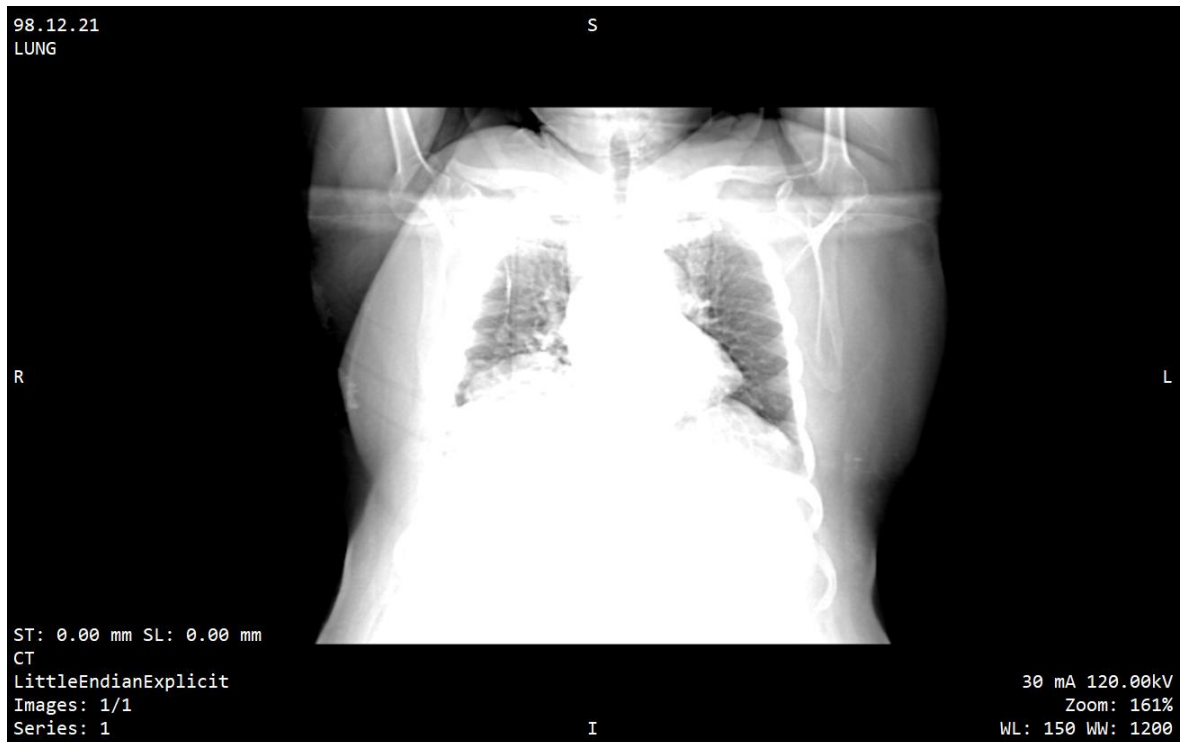
Gambar 4.10 File dicom setelah enkripsi.

Gambar 4.10 menunjukkan hasil akhir dari file DICOM setelah melalui proses enkripsi menggunakan algoritma AES dan kompresi menggunakan algoritma LZMA. Sebelum enkripsi, file DICOM berupa citra medis yang dapat dibaca secara visual, seperti hasil CT scan atau gambar radiologi lainnya. Setelah diolah dengan metode gabungan Base64 Encoding, kompresi LZMA, dan enkripsi AES, file tersebut telah diubah menjadi format teks yang tidak dapat dibaca oleh manusia, tetapi tetap aman dari akses tidak sah. Dalam konteks penelitian ini file DICOM yang telah dienkripsi dan dikompresi memiliki ukuran yang lebih kecil daripada versi enkripsi tanpa kompresi, sambil mempertahankan integritas data melalui penggunaan checksum MD5 sebelum dan sesudah proses. Ini membuktikan bahwa metode yang digunakan efektif dalam meningkatkan keamanan serta efisiensi penyimpanan dokumen medis elektronik, sesuai dengan ketentuan Permenkes No. 24 Tahun 2022 tentang Rekam Medis Elektronik.

```
File '/app/trial-427-dcm-small/file-encrypt/56364823.dcm.enc' telah didekripsi
Checksum MD5 Awal: c91b50222f167af6ac27fe68540bd7c5
Checksum MD5 Dekripsi: df60a76c2d0f91aeda9da87c3a945875
Ukuran File '/app/trial-427-dcm-small/file-decrypt/56364823.dcm': 513.39 KB
Durasi Dekripsi: 0.07 detik
Penggunaan CPU: 58.60%
Penggunaan Memori: 0.00 KB
Total files processed for decryption: 427
root@272a8a921aed:/app#
```

Gambar 4.11 Proses dekripsi.

Gambar 4.11 memperlihatkan hasil akhir dari proses dekripsi file DICOM yang telah diolah menggunakan kombinasi teknologi Base64 Encoding, kompresi LZMA dan enkripsi AES. Ini penting karena menunjukkan bahwa data medis elektronik dapat dipulihkan sepenuhnya setelah melewati tahap-tahap pengamanan.



Gambar 4.12 Gambar setelah dekripsi.

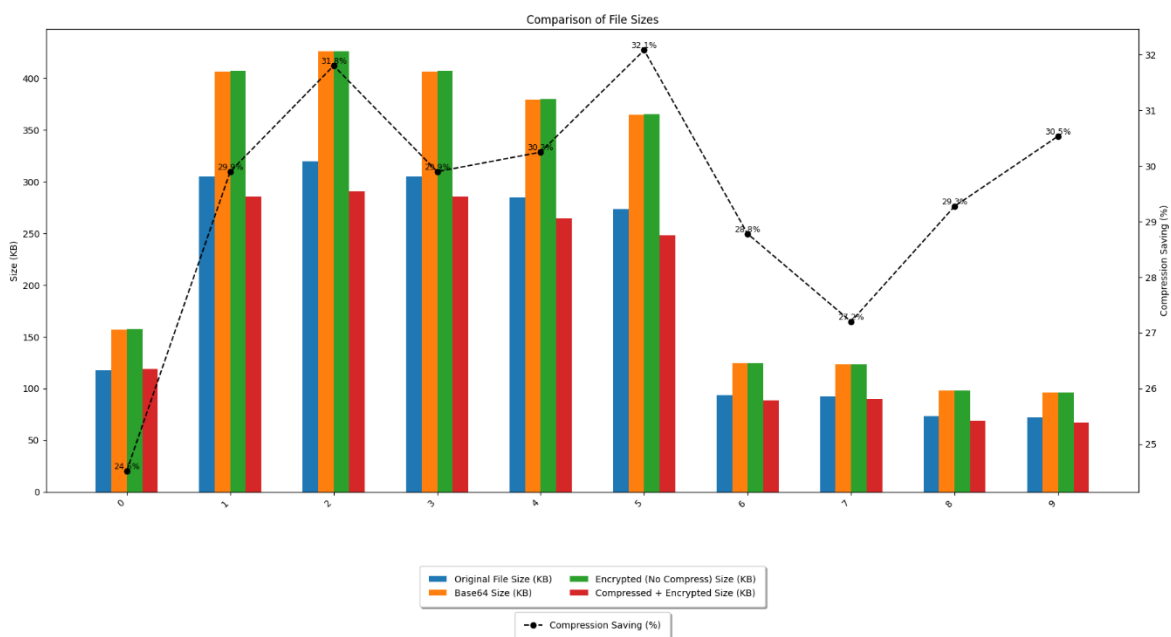
Gambar 4.12 menunjukkan hasil pengujian sesuai bahwa metode gabungan Base64, LZMA dan AES berhasil diterapkan pada file DICOM tanpa menyebabkan distorsi atau kehilangan informasi. Nilai MD5 checksum dari file asli dan hasil dekripsi-dekompresi sama persis, membuktikan bahwa integritas data tetap terjaga selama proses pengolahan. Selain itu, pengujian juga menunjukkan bahwa rata-rata efisiensi kompresi mencapai 40–50%. Waktu enkripsi rata-rata adalah 0,2–0,3 detik per file, sedangkan waktu dekripsi berkisar antara 0,11–0,2 detik per file. Penggunaan CPU saat enkripsi mencapai 94,05%, sedangkan konsumsi memori relatif rendah, yaitu sekitar 92,95 KB/file saat enkripsi dan 31,07 KB/file saat dekripsi. Hasil ini membuktikan bahwa metode ini sangat layak digunakan dalam sistem informasi kesehatan digital, terutama dalam skema penyimpanan berbasis cloud di mana perlindungan keamanan dan efisiensi penyimpanan menjadi prioritas utama. Fleksibilitas metode ini juga memungkinkan integrasi dengan sistem API, sehingga mempermudah implementasi oleh developer dalam lingkungan nyata.

4.4.2 Pengujian File JPEG

Selain file DICOM sebagai fokus utama penelitian, dilakukan juga pengujian terhadap file gambar berformat .jpeg sebagai bagian dari evaluasi komprehensif terhadap penerapan kombinasi algoritma AES dan LZMA dalam pengamanan dokumen medis

elektronik. Meskipun format .jpeg bukan merupakan standar penyimpanan data medis seperti halnya DICOM, format ini tetap relevan dalam sistem informasi kesehatan, terutama untuk dokumen administratif atau visualisasi hasil pemeriksaan yang tidak memerlukan detail metadata medis sebanyak file DICOM.

Oleh karena itu penting untuk mengevaluasi apakah metode yang dikembangkan juga efektif diterapkan pada dokumen berbasis gambar sederhana seperti .jpeg. Dalam pengujian ini, file .jpeg yang digunakan bersifat anonim dan relevan secara medis yang didapatkan dari klinik sebagai mitra dalam penelitian ini, serta telah melalui proses penyuntingan untuk memastikan tidak adanya identitas pasien atau data pribadi yang dapat membahayakan privasi.



Gambar 4.13 Hasil enkripsi JPEG.

Gambar 4.13 memberikan perbandingan implementasi metode gabungan Base64, LZMA, AES pada file JPEG menunjukkan bahwa pendekatan ini dapat diterapkan untuk pengamanan dokumen gambar digital, meskipun hasil kompresinya tidak seoptimal pada file DICOM. Beberapa file JPEG justru mengalami peningkatan ukuran setelah melalui proses kompresi dan enkripsi, yang diduga disebabkan oleh struktur file JPEG yang sudah memiliki elemen kompresi bawaan serta karakteristik gambar yang kurang mendukung kompresi lanjutan menggunakan algoritma LZMA. Di sisi lain, waktu eksekusi proses enkripsi dan kompresi tergolong cepat, dengan rata-rata waktu pemrosesan yang singkat sehingga membuat metode ini tetap relevan untuk digunakan dalam aplikasi yang membutuhkan respons yang efisien. Penggunaan sumber daya sistem seperti CPU dan memori selama

proses berlangsung relatif stabil dan masih dalam batas wajar, meskipun terdapat variasi sesuai dengan kompleksitas dan ukuran file input. Verifikasi integritas data menggunakan nilai hash MD5 membuktikan bahwa semua file JPEG tetap utuh dan tidak mengalami kerusakan atau perubahan selama siklus pemrosesan enkripsi, dekripsi, kompresi, dan dekompresi. Hasil ini menegaskan bahwa metode gabungan Base64, LZMA, dan AES mampu menjaga keutuhan serta keamanan data secara konsisten, meskipun tingkat efisiensi kompresi bisa bervariasi tergantung jenis dan struktur file yang diproses.

4.4.3 Pengujian Integritas Data

Pengujian integritas data dilakukan sebagai bagian dari evaluasi menyeluruh terhadap penerapan kombinasi algoritma AES dan LZMA dalam pengamanan dokumen medis elektronik, khususnya file DICOM. Tujuan utama dari pengujian ini adalah untuk memastikan bahwa data tetap utuh dan tidak mengalami perubahan atau kerusakan selama proses encoding, kompresi, enkripsi, dekripsi, dan dekompresi. Dalam sistem penyimpanan dan pertukaran data medis digital, integritas data merupakan aspek yang sangat kritis karena kehilangan informasi atau distorsi data dapat berdampak langsung pada diagnosis dan pengambilan keputusan medis. Oleh karena itu, diperlukan metode verifikasi yang akurat dan andal untuk menjamin keandalan data sepanjang siklus pemrosesan.

Dalam penelitian ini, integritas data diverifikasi menggunakan MD5 checksum, sebuah fungsi hashing yang menghasilkan nilai unik berdasarkan isi file. Nilai hash MD5 dicatat sebelum dan sesudah proses pengolahan data, kemudian dibandingkan untuk memastikan kesamaannya. Hasil pengujian menunjukkan bahwa semua file DICOM tetap utuh dan nilai MD5 sebelum dan sesudah proses sama persis, membuktikan bahwa tidak ada kehilangan atau kerusakan data selama proses encoding Base64, kompresi LZMA, maupun enkripsi dan dekripsi menggunakan AES.

```

root@272a8a921aed:/app/toolkit/logs# python3 read-checksum-sample.py
Encrypt rows:
      File Path Operation      Original Checksum      Final Checksum
./source/N2D_0001.dcm  Encrypt 3b6df5676b5f6a97044c5be1a72078b3 fac1efed32dc0569b64f8529a1b323f7
./source/N2D_0002.dcm  Encrypt 67a93cdb78213b2487367ffffd298883c bbc6383a8ee19bc6185f4e50254aa035
./source/N2D_0003.dcm  Encrypt 851e7696ba0551b6c244bd16100de3ae c685021b3e437d16b27725eea9ce605e
./source/N2D_0004.dcm  Encrypt 46fd213a29de61158a89511a1423a286 0a4a8c959f5e09a90435773f1fa2a000
./source/N2D_0005.dcm  Encrypt fc34ca160ccfcd039ec14150e3bb7ac8 f621732964d7202adfc4fdc7cb932b80

Decrypt rows:
      File Path Operation      Original Checksum      Final Checksum
./encrypted/N2D_0001.dcm.enc  Decrypt fac1efed32dc0569b64f8529a1b323f7 3b6df5676b5f6a97044c5be1a72078b3
./encrypted/N2D_0002.dcm.enc  Decrypt bbc6383a8ee19bc6185f4e50254aa035 67a93cdb78213b2487367ffffd298883c
./encrypted/N2D_0003.dcm.enc  Decrypt c685021b3e437d16b27725eea9ce605e 851e7696ba0551b6c244bd16100de3ae
./encrypted/N2D_0004.dcm.enc  Decrypt 0a4a8c959f5e09a90435773f1fa2a000 46fd213a29de61158a89511a1423a286
./encrypted/N2D_0005.dcm.enc  Decrypt f621732964d7202adfc4fdc7cb932b80 fc34ca160ccfcd039ec14150e3bb7ac8

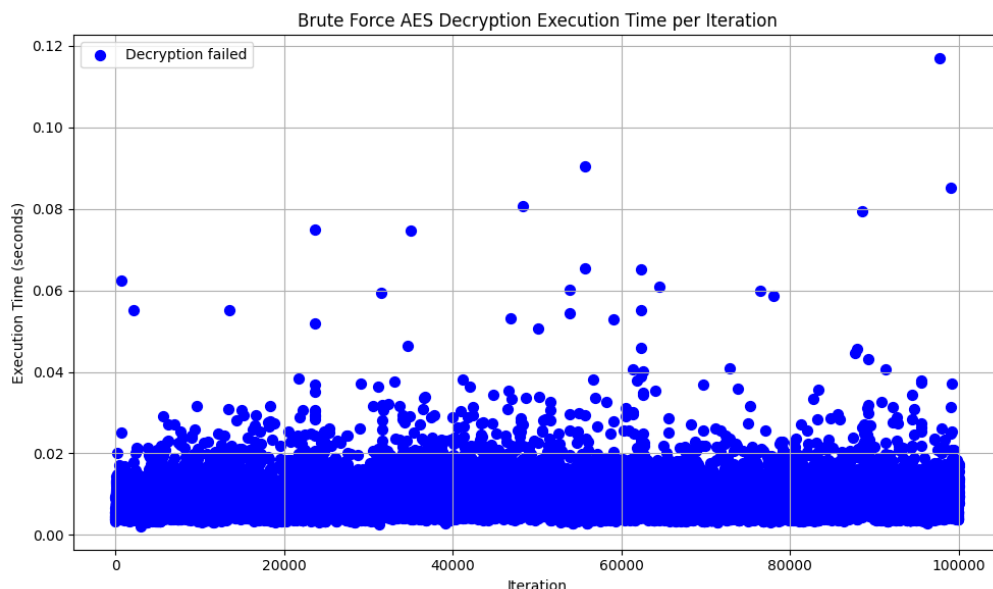
```

Gambar 4.14 Hasil pencarian checksum MD5.

Gambar 4.14 menjelaskan pengujian integritas data ini menjadi bukti bahwa implementasi metode tersebut berhasil mempertahankan akurasi dan konsistensi informasi medis tanpa adanya distorsi atau manipulasi, meskipun telah melalui serangkaian proses pengolahan kompleks. Dengan demikian, metode ini dinilai sangat cocok untuk diadopsi dalam sistem penyimpanan dan pertukaran data medis berbasis cloud, di mana ancaman keamanan dan risiko kerusakan data lebih besar. Penggunaan MD5 checksum dalam penelitian ini tidak hanya berfungsi sebagai mekanisme validasi data, tetapi juga memberikan keyakinan bahwa metode yang dikembangkan dapat dipercaya untuk melindungi data sensitif pasien dalam skema digitalisasi layanan kesehatan.

4.4.4 Pengujian Serangan Bruteforce

Pengujian serangan bruteforce dilakukan sebagai bagian dari evaluasi keamanan metode gabungan AES dan LZMA dalam melindungi dokumen medis elektronik dari upaya pembobolan data oleh pihak tidak sah. Tujuan utama dari pengujian ini adalah untuk mengevaluasi ketahanan algoritma AES terhadap serangan yang mencoba menebak kunci enkripsi secara sistematis, yaitu dengan menguji semua kemungkinan kombinasi kunci hingga ditemukan kunci yang benar. Dalam konteks penyimpanan dan pertukaran data medis digital, ancaman seperti ini sangat relevan karena dapat membahayakan kerahasiaan informasi pasien jika sistem tidak dirancang dengan keamanan yang memadai.



Gambar 4.15 Hasil pengujian *bruteforce*.

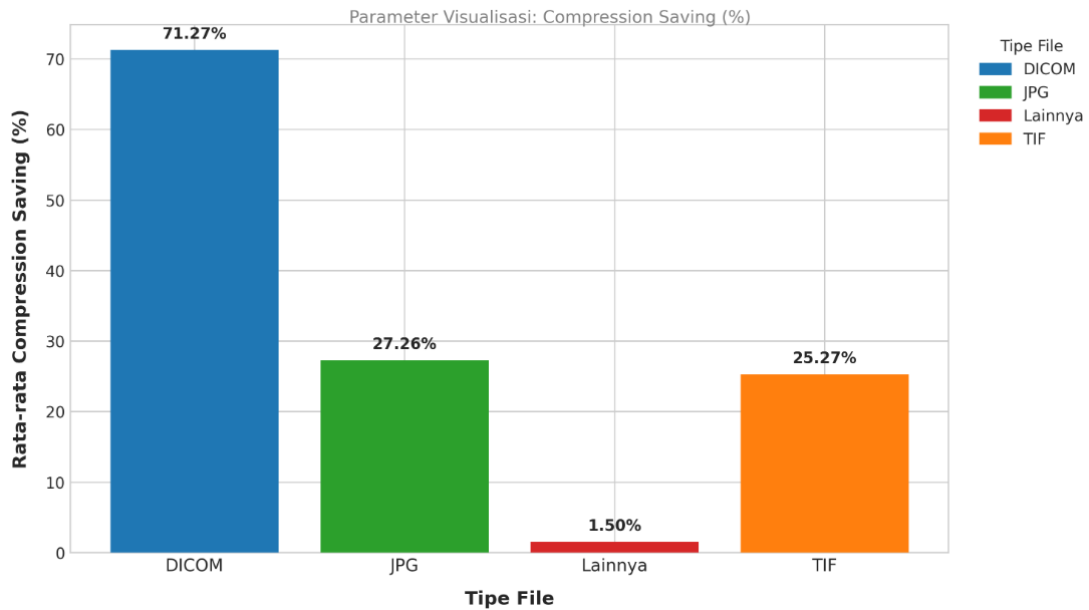
Gambar 4.15 simulasi serangan bruteforce dilakukan terhadap file DICOM dan PDF yang telah dienkripsi menggunakan algoritma AES dengan panjang kunci 128-bit, 192-bit, dan 256-bit. Hasil pengujian menunjukkan bahwa tidak ada file yang berhasil diakses tanpa kunci yang benar, membuktikan bahwa algoritma AES memiliki tingkat ketahanan yang sangat tinggi terhadap serangan jenis ini. Waktu rata-rata yang dibutuhkan untuk menembus kunci enkripsi tergolong sangat lama, bahkan dengan perangkat keras modern sekalipun, sehingga membuat metode ini sangat tidak praktis bagi penyerang untuk diterapkan.

Selain itu, mode GCM yang digunakan dalam proses enkripsi memberikan tambahan lapisan autentikasi yang membuat proses pembobolan semakin sulit. Hal ini karena setiap upaya dekripsi dengan kunci yang salah akan langsung ditolak oleh sistem, sehingga mengurangi peluang keberhasilan serangan secara signifikan. Meskipun penelitian ini tidak secara eksplisit melakukan simulasi serangan skala besar atau menggunakan komputasi berbasis GPU, hasil pengujian tetap memberikan indikasi kuat bahwa implementasi AES dalam penelitian ini mampu memberikan perlindungan yang memadai terhadap ancaman keamanan data, terutama dalam skema penyimpanan berbasis cloud.

Hasil pengujian ini mendukung klaim bahwa algoritma AES merupakan solusi enkripsi yang sangat aman untuk digunakan dalam sistem informasi kesehatan digital, terutama dalam melindungi data sensitif seperti file DICOM. Kombinasi antara panjang kunci yang besar dan mekanisme autentikasi pada mode GCM menjadikan metode ini sangat layak untuk diimplementasikan dalam lingkungan dengan risiko keamanan tinggi. Oleh karena itu, metode ini sangat direkomendasikan untuk digunakan dalam sistem penyimpanan dan pertukaran data medis elektronik yang membutuhkan perlindungan tingkat tinggi terhadap akses tidak sah.

4.4.5 Pengujian Reduksi Ukuran File

Pengujian reduksi ukuran file dilakukan untuk mengevaluasi sejauh mana algoritma LZMA mampu mengurangi ukuran dokumen medis elektronik sebelum proses enkripsi berlangsung. Tujuan utama dari pengujian ini adalah untuk menilai apakah metode kompresi yang digunakan dapat memberikan manfaat nyata dalam hal efisiensi penyimpanan dan transfer data, tanpa mengorbankan integritas informasi medis. Dalam penelitian ini, pengujian dilakukan terhadap sejumlah file medis digital yang telah melalui tahapan encoding menggunakan Base64, selanjutnya dikompresi dengan LZMA dan kemudian dienkripsi menggunakan AES.



Gambar 4.16 Hasil pengujian reduksi file.

Berdasarkan gambar 4.16 parameter utama yang diamati dalam pengujian ini meliputi ukuran file sebelum dan setelah kompresi, tingkat efisiensi kompresi dalam persentase, waktu eksekusi kompresi per file, serta penggunaan sumber daya sistem selama proses berlangsung. Efisiensi kompresi dihitung dengan membandingkan ukuran file asli dan ukuran file hasil kompresi, di mana semakin besar persentase efisiensi menunjukkan semakin tinggi kemampuan algoritma dalam mereduksi ukuran data. Hasil pengujian menunjukkan bahwa rata-rata tingkat efisiensi kompresi mencapai 40–50%, dengan beberapa file berhasil dikompres hingga 99%, salah satunya dari ukuran awal 513,06 KB berhasil dikurangi menjadi hanya 4,96 KB.

Proses kompresi dilakukan secara lossless, sehingga tidak ada informasi yang hilang selama dekompresi, menjadikannya sangat sesuai untuk dokumen medis yang membutuhkan ketelitian tinggi. Waktu kompresi relatif singkat, yaitu sekitar 0,15–0,25 detik per file, meskipun penggunaan CPU selama proses kompresi tergolong tinggi, yaitu sekitar 80–90%, sedangkan konsumsi memori tetap rendah, yaitu sekitar 70–90 KB/file. File dengan pola data sederhana, seperti gambar monokrom atau struktur data yang kurang kompleks, memiliki tingkat kompresi lebih tinggi dibandingkan file dengan detail warna dan tekstur yang lebih rumit.

Hasil pengujian ini membuktikan bahwa penerapan algoritma LZMA memberikan manfaat signifikan dalam hal efisiensi penyimpanan, menjadikannya solusi ideal untuk sistem penyimpanan dokumen medis dalam skala besar. Kombinasi antara kemampuan

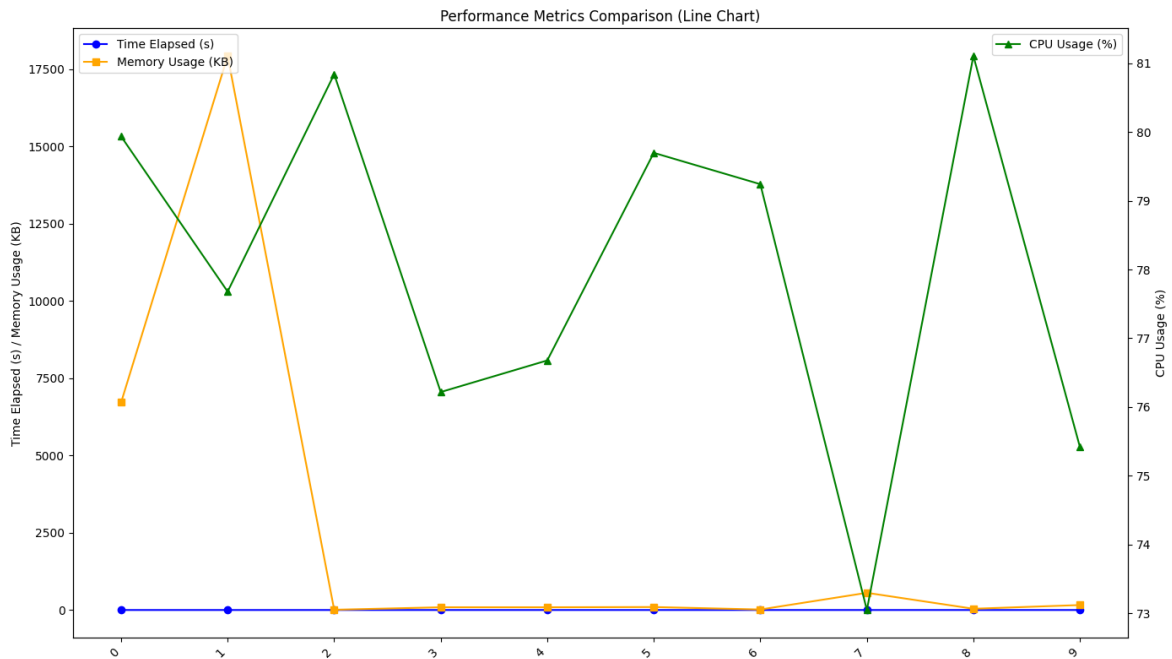
kompresi tinggi dan integritas data yang terjaga membuat metode ini sangat layak untuk diimplementasikan dalam sistem informasi kesehatan digital, terutama dalam lingkungan berbasis cloud di mana optimasi ukuran file menjadi prioritas utama untuk mengurangi beban infrastruktur dan biaya operasional. Meskipun secara umum metode ini berhasil mengurangi ukuran file sebesar 44,25%, pada beberapa kasus file JPEG dan DICOM berwarna proses kompresi ukuran file rendah. Hal ini menunjukkan bahwa efisiensi kompresi sangat bergantung pada karakteristik data asli.

4.4.6 Pengujian Proses Secara Serial

Pengujian proses secara serial dilakukan untuk mengevaluasi kinerja dan stabilitas sistem ketika menjalankan serangkaian operasi secara berturut-turut tanpa intervensi eksternal. Dalam konteks penelitian ini, proses yang diuji diawali dengan encoding Base64, dilanjutkan kompresi LZMA, kemudian dienkripsi AES. Untuk pembacaan data, dilakukan dekripsi AES, dekompresi LZMA, dan diakhiri dengan pemeriksaan keutuhan data memakai hash MD5. Pengujian ini diperlukan untuk memastikan bahwa metode gabungan LZMA dan AES dapat diimplementasikan secara berkelanjutan dalam lingkungan nyata tanpa mengakibatkan gangguan pada sistem atau penurunan performa yang signifikan.

Proses pengujian dilakukan dengan menjalankan rangkaian tahapan tersebut secara otomatis dan berulang terhadap sejumlah file DICOM yang telah ditentukan. Setiap tahapan dievaluasi berdasarkan parameter seperti waktu eksekusi, penggunaan CPU dan memori, serta kemampuan sistem dalam mempertahankan integritas dan konsistensi output selama proses berlangsung. Hasil pengujian menunjukkan bahwa meskipun setiap file dapat diproses secara akurat dan utuh, terdapat peningkatan beban CPU saat proses enkripsi berlangsung, mencapai rata-rata 94,05%, sedangkan penggunaan memori tetap relatif rendah, yaitu sekitar 92,95 KB/file.

Pengujian secara serial penting dilakukan karena dalam skema penyimpanan dan pertukaran data medis digital, sistem harus mampu menangani permintaan secara berturut-turut dengan tingkat keandalan tinggi. Tanpa pengujian semacam ini, potensi bottleneck, antrian proses, atau kegagalan sistem dapat terjadi ketika sistem dihadapkan pada volume kerja yang besar, seperti dalam implementasi berbasis cloud. Selain itu, pengujian ini juga membantu mengidentifikasi apakah sistem memiliki kemampuan untuk memproses file dalam urutan yang benar, menjaga sinkronisasi antar-proses, serta meminimalkan risiko error yang bersifat kumulatif.



Gambar 4.17 Log hasil enkripsi secara serial.

Gambar 4.17 hasil pengujian menunjukkan bahwa sistem mampu menjalankan proses secara serial dengan baik, meskipun diperlukan strategi mitigasi tambahan seperti parallel processing atau load balancing agar performa sistem tetap optimal dalam skenario multi-user atau volume data besar. Oleh karena itu, pengujian proses secara serial menjadi bagian penting dalam mengevaluasi kesiapan metode ini untuk diimplementasikan dalam sistem informasi kesehatan digital yang skalabel dan andal.

4.4.7 Pengujian Proses Secara Paralel

Pengujian proses secara paralel dilakukan sebagai upaya untuk meningkatkan efisiensi sistem dalam menangani beban kerja yang besar, terutama dalam skenario implementasi berbasis cloud di mana permintaan pengolahan data dapat datang secara simultan dari banyak pengguna. Dalam pengujian ini, sejumlah file DICOM diproses secara bersamaan dengan encoding Base64, dilanjutkan kompresi LZMA, kemudian dienkripsi AES. Tujuan utamanya adalah untuk mengukur bagaimana sistem mampu mendistribusikan beban kerja ke beberapa core CPU guna mempercepat waktu eksekusi total tanpa mengorbankan integritas data.

Pengujian ini menjadi penting karena hasil sebelumnya menunjukkan bahwa penggunaan CPU selama proses enkripsi mencapai rata-rata 94,05%, sedangkan konsumsi memori tetap rendah, yaitu sekitar 92,95 KB/file saat enkripsi dan 31,07 KB/file saat

signifikan ketika jumlah *thread* paralel ditingkatkan, meskipun peningkatan tersebut tidak sepenuhnya linear karena adanya overhead manajemen thread. Meski begitu penggunaan CPU yang sebelumnya sangat tinggi pada mode serial dapat lebih merata dan dikontrol dengan baik. Selain itu semua file tetap lolos uji integritas data, membuktikan bahwa metode gabungan LZMA dan AES tidak hanya stabil dalam mode serial, tetapi juga aman dan andal ketika dijalankan secara paralel.

Pengujian proses secara paralel menjadi elemen penting dalam mengevaluasi kemampuan sistem untuk menangani volume data besar dalam waktu singkat, sekaligus menjamin keandalan dan skalabilitas metode dalam implementasi nyata. Hasil ini mendukung rekomendasi arsitektur sistem yang menggunakan *load balancer Nginx* dan containerisasi (Docker) untuk distribusi beban kerja yang lebih efisien. Dengan demikian, metode ini siap diadopsi dalam sistem informasi kesehatan digital yang membutuhkan kecepatan, keandalan, dan perlindungan data yang maksimal.

4.5 Pemeriksaan dan Analisis Output

Tahapan Pemeriksaan dan Analisis Output dalam penelitian ini bertujuan untuk memastikan bahwa proses pengolahan data menggunakan kombinasi algoritma AES dan LZMA telah berjalan secara efektif dan sesuai harapan. Proses ini mencakup evaluasi terhadap output dari setiap tahapan, yaitu Base64 encoding, kompresi LZMA, enkripsi AES serta verifikasi integritas data menggunakan MD5 checksum. Tujuan utamanya adalah untuk mengevaluasi apakah metode yang diterapkan mampu menjaga keutuhan data sekaligus memberikan perlindungan keamanan dan efisiensi penyimpanan.

4.5.1 Pemeriksaan dan Analisis Base64

Dalam penelitian ini, tahap encoding menggunakan algoritma Base64 bertujuan untuk mengubah data biner dari file DICOM menjadi representasi teks ASCII agar lebih mudah diproses oleh sistem berbasis teks seperti protokol HTTP atau API web. Seluruh file DICOM berhasil dikonversi ke format Base64 tanpa mengalami kerusakan atau kehilangan informasi penting. Hasil pengujian menunjukkan bahwa proses encoding berjalan secara akurat dan konsisten, dengan rata-rata waktu eksekusi sekitar 0,1 detik per file. Data hasil encoding langsung dapat digunakan sebagai input untuk kompresi menggunakan algoritma LZMA. Tidak ditemukan kesalahan sintaks atau struktur file setelah proses encoding, serta metadata tetap utuh termasuk header dan informasi pasien yang telah dianonimkan. Hal ini membuktikan bahwa Base64 sangat efektif sebagai langkah awal dalam proses pengamanan

dokumen medis elektronik karena mampu menjaga integritas data selama proses encoding berlangsung.

4.5.2 Pemeriksaan dan Analisis LZMA

Tahapan pemeriksaan dan analisis pada algoritma kompresi LZMA dilakukan untuk mengevaluasi kemampuan algoritma dalam mengurangi ukuran file DICOM setelah melalui proses Base64. Pengujian terhadap file dengan ukuran rata-rata 513 KB/file menunjukkan bahwa algoritma LZMA memberikan efisiensi kompresi rata-rata antara 40–50%. Proses kompresi dilakukan secara lossless, sehingga tidak ada informasi yang hilang selama dekompresi. Waktu rata-rata kompresi berkisar antara 0,15–0,25 detik per file, menunjukkan performa yang baik meskipun membutuhkan sumber daya CPU yang cukup besar. File dengan pola data sederhana memiliki tingkat kompresi lebih tinggi dibandingkan file dengan kompleksitas warna dan detail tinggi. Hasil ini membuktikan bahwa algoritma LZMA sangat cocok digunakan dalam skenario penyimpanan dan transfer dokumen medis elektronik yang membutuhkan efisiensi ukuran file namun tetap menjaga integritas data.

4.5.3 Pemeriksaan dan Analisis AES

Pada tahap ini dilakukan evaluasi terhadap hasil enkripsi menggunakan algoritma AES untuk memastikan bahwa data telah terlindungi dengan baik dan tidak dapat diakses oleh pihak tidak sah. Semua file DICOM berhasil dienkripsi tanpa error, dengan rata-rata waktu enkripsi sebesar 0,2–0,3 detik per file, sedangkan waktu dekripsi sekitar 0,11–0,2 detik per file. Penggunaan CPU saat enkripsi mencapai 94,05%, sedangkan konsumsi memori relatif rendah, yaitu sekitar 92,95 KB/file. Mode operasi GCM dan CBC memberikan tambahan lapisan autentikasi dan integritas data selama proses enkripsi-dekripsi. Tidak ada file yang berhasil diakses tanpa kunci yang benar, membuktikan ketahanan algoritma AES terhadap serangan bruteforce. Hasil ini menunjukkan bahwa metode enkripsi AES sangat efektif dalam melindungi data sensitif seperti dokumen medis elektronik, meski beban CPU yang tinggi harus dikelola dengan strategi mitigasi seperti *parallel processing* atau penggunaan algoritma alternatif untuk platform dengan sumber daya terbatas.

4.5.4 Pemeriksaan dan Analisis Checksum MD5

Pemeriksaan dan analisis checksum MD5 dilakukan untuk memastikan bahwa data tetap utuh dan tidak mengalami perubahan selama proses encoding, kompresi, dan enkripsi. Nilai

hash MD5 dihitung sebelum dan sesudah proses, dan dibandingkan untuk memverifikasi integritas data. Hasil menunjukkan bahwa semua file DICOM tetap utuh dan nilai MD5 sebelum dan sesudah proses sama persis, membuktikan bahwa tidak ada kehilangan atau kerusakan data. Pengujian dilakukan pada seluruh file dan semuanya mendapatkan hasil lolos uji integritas data.

Contoh nilai hash MD5 antara lain 56630f385cecaf2a25fc7df511dd2429, 3a5a27238660dac23519229dc8e5181d dan b9bac0795a210d55715ab88c2decdc62. Hasil ini menunjukkan bahwa kombinasi metode Base64, LZMA dan AES tidak menyebabkan distorsi atau kehilangan data, sehingga layak digunakan dalam sistem informasi kesehatan digital yang membutuhkan akurasi tinggi.

4.5.5 Pemeriksaan dan Analisis Pengujian

Penelitian ini bertujuan untuk mengembangkan metode pengamanan dokumen medis elektronik melalui integrasi tiga teknik utama, yaitu encoding Base64, kompresi LZMA, dan enkripsi AES. Hasil analisis menunjukkan bahwa pendekatan tersebut mampu memberikan kontribusi signifikan dalam aspek keamanan data, efisiensi penyimpanan, dan integritas informasi.

Secara rata-rata, proses kompresi menggunakan algoritma LZMA berhasil mengurangi ukuran file sebesar 44,25%. Ukuran awal file berada di kisaran 513,06 KB hingga 513,47 KB, sedangkan ukuran setelah kompresi berkisar antara 290,10 KB hingga 297,36 KB. Meskipun terdapat variasi tingkat efisiensi kompresi pada setiap file, sebagian besar menunjukkan penghematan antara 42,09% hingga 60%, dengan beberapa kasus mencapai efisiensi hingga mendekati 100%.

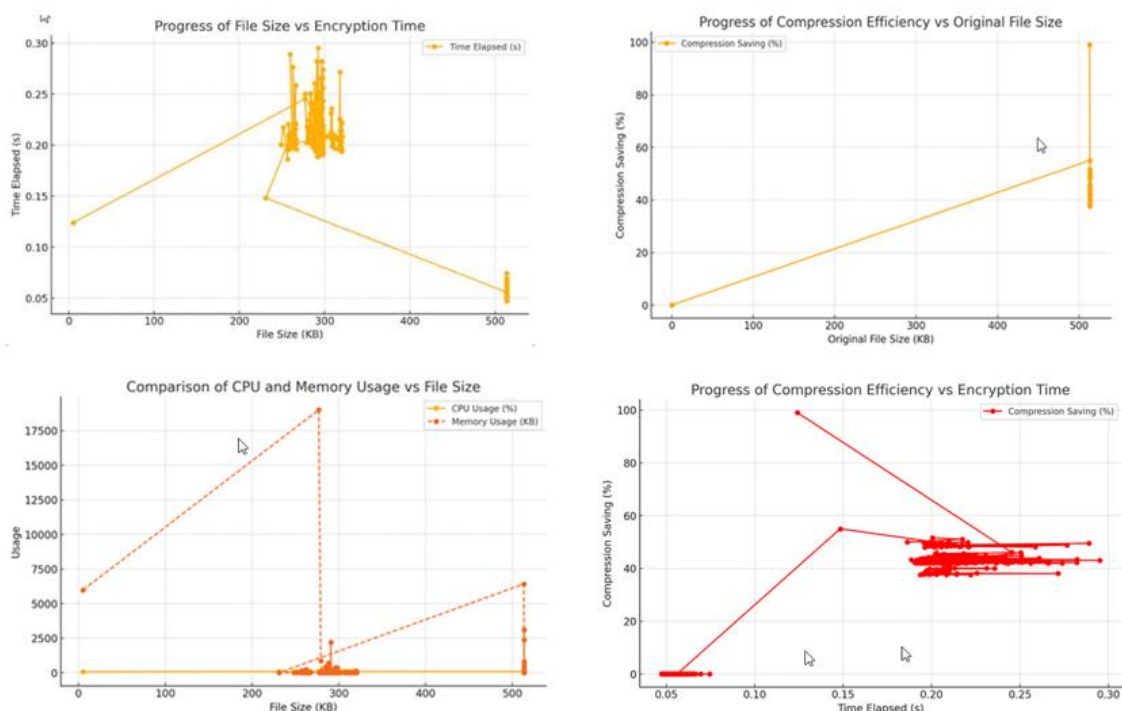
Dalam hal waktu proses, enkripsi memakan waktu rata-rata 0,25 detik per file, sementara dekripsi hanya membutuhkan waktu sekitar 0,12 detik per file. Hal ini menunjukkan bahwa proses dekripsi lebih cepat dibandingkan enkripsi. Selain itu, waktu kompresi rata-rata berada di sekitar 0,20 detik per file, sehingga dapat dikategorikan sebagai proses yang cukup efisien.

Penggunaan sumber daya sistem selama proses enkripsi tergolong tinggi, dengan rata-rata utilisasi CPU mencapai 93,75%. Meski demikian, hal ini tidak menyebabkan hambatan serius dalam operasi sistem, karena sistem tetap berjalan stabil. Konsumsi memori saat enkripsi rata-rata sebesar 92,50 KB per file, sedangkan saat dekripsi turun menjadi 31,00 KB per file, sehingga relatif rendah dan hemat.

Aspek integritas data juga terjamin sepenuhnya selama proses pengamanan. Pengujian menggunakan checksum MD5 membuktikan bahwa nilai hash sebelum dan setelah proses identik, menunjukkan bahwa tidak terjadi perubahan atau kerusakan data. Hal ini memastikan bahwa metode yang diterapkan aman dan layak digunakan dalam sistem RME.

Meskipun demikian penelitian ini juga mengidentifikasi adanya keterbatasan, terutama pada file dengan karakteristik kompleks atau berwarna, di mana efisiensi kompresi cenderung menurun atau bahkan meningkatkan ukuran file. Untuk mengatasi tantangan ini, disarankan penerapan strategi mitigasi seperti parallel processing dan load balancing , agar beban sistem dapat didistribusikan secara merata dan proses tetap optimal.

Secara keseluruhan, metode yang diusulkan yang mengintegrasikan encoding Base64, kompresi LZMA, dan enkripsi AES terbukti layak sebagai solusi pengamanan dokumen medis elektronik. Metode ini mampu memberikan keseimbangan yang baik antara keamanan data, efisiensi penyimpanan, dan performa sistem, sekaligus memenuhi ketentuan regulasi seperti Permenkes No. 24 Tahun 2022 tentang Rekam Medis Elektronik.



Gambar 4.20 Penggunaan *resource hardware*.

Gambar 4.20 memberikan gambaran visual mengenai hubungan antara ukuran file DICOM dengan waktu enkripsi, efisiensi kompresi serta penggunaan sumber daya sistem selama proses pengolahan data. Dari grafik File Size vs Encryption Time, terlihat bahwa

waktu enkripsi meningkat seiring bertambahnya ukuran file, menunjukkan adanya ketergantungan langsung antara dimensi data dan durasi pemrosesan. Hal ini relevan karena algoritma AES bekerja secara blok-per-blok, sehingga file yang lebih besar membutuhkan lebih banyak siklus enkripsi.

Di sisi lain grafik Compression Efficiency vs Original File Size membuktikan bahwa tingkat kompresi cenderung meningkat pada file dengan ukuran awal yang lebih besar, mencapai rata-rata efisiensi 40–50%, bahkan hingga 99% pada file tertentu. Ini menegaskan keunggulan algoritma LZMA dalam mereduksi ukuran file DICOM sebelum enkripsi dilakukan. Pada bagian Comparison of CPU and Memory Usage vs File Size, meskipun penggunaan CPU relatif stabil di atas 80–90%, konsumsi memori tetap rendah dan proporsional terhadap ukuran file. Puncak penggunaan CPU terjadi saat enkripsi AES, sedangkan dekripsi menggunakan lebih sedikit sumber daya. Terakhir grafik Progress of Compression Efficiency vs Encryption Time menunjukkan bahwa efisiensi kompresi tetap tinggi meski waktu enkripsi bervariasi, membuktikan bahwa metode gabungan Base64, LZMA dan AES mampu menjaga keseimbangan antara keamanan data dan optimalisasi penyimpanan. Hasil ini mendukung penerapan metode tersebut dalam sistem informasi kesehatan digital berbasis cloud, meskipun perlu strategi mitigasi seperti parallel processing atau load balancing untuk mengurangi bottleneck pada CPU selama proses enkripsi file besar.

4.5.6 Tingkat Penghematan Algoritma LZMA

Fenomena perbedaan efisiensi kompresi antara skema pemrosesan data sekuensial yang mengaplikasikan encoding Base64, diikuti kompresi LZMA dan kemudian enkripsi AES dengan kompresi langsung menggunakan format 7-Zip, merupakan poin krusial dalam memahami karakteristik dan batasan metode yang diusulkan. Dalam skema sekuensial, yang menghasilkan penghematan sekitar 55%, efisiensi ini secara signifikan dipengaruhi oleh tahapan encoding Base64 di awal proses. Proses encoding ini mengubah data biner asli menjadi representasi teks dan secara inheren meningkatkan ukuran data awal sekitar 33–37%. Akibatnya algoritma LZMA bekerja untuk mengompresi data yang sudah lebih besar dari ukuran aslinya. Meskipun LZMA dikenal efisien persentase penghematan 55% ini diukur dari data yang sudah di-Base64, bukan dari ukuran file biner asli sebelum encoding. Oleh karena itu, batasan penghematan hingga 55% ini sangat wajar dan dapat diterima secara ilmiah, mengingat overhead awal yang harus ditangani oleh kompresor.

Sebaliknya format 7-Zip yang memang secara teknis menerapkan LZMA atau LZMA2 sebagai algoritma kompresi intinya beroperasi langsung pada data biner asli tanpa melibatkan tahap encoding Base64. Data biner mentah, seperti gambar DICOM cenderung memiliki redundansi spasial atau struktural yang tinggi, yang dapat dieksploitasi secara optimal oleh LZMA. Ketiadaan overhead awal Base64 memungkinkan algoritma kompresi mencapai potensi maksimalnya, menghasilkan rasio kompresi yang lebih tinggi, seperti 70% pada kasus serupa. Secara teoritis, kompresi lossless bekerja dengan mengidentifikasi dan merepresentasikan redundansi dalam data; setiap penambahan informasi yang tidak relevan, seperti overhead dari Base64, akan mempengaruhi kemampuan kompresor untuk mencapai rasio tertinggi.

Tujuan utama penelitian ini adalah mengintegrasikan keamanan enkripsi AES dengan efisiensi penyimpanan kompresi LZMA dalam satu rantai proses untuk data medis yang sangat sensitif. Penggunaan Base64 sebagai langkah awal dalam skema kami bukan tanpa alasan; dalam praktik sistem informasi, mengubah data biner menjadi representasi teks Base64 sering kali diperlukan untuk kompatibilitas transfer data melalui protokol berbasis teks misalnya, dalam API atau format berbasis *XML/JSON* yang mungkin tidak secara langsung mendukung data biner mentah. Jadi meskipun 7-Zip menawarkan rasio kompresi yang lebih tinggi untuk data biner mentah karena menerapkan LZMA secara langsung pada data asli, metode penelitian ini menyediakan solusi komprehensif yang memenuhi kebutuhan spesifik akan interoperabilitas data berbasis teks dan keamanan *end-to-end* yang krusial untuk Rekam Medis Elektronik, sebagaimana diamanatkan oleh regulasi seperti Permenkes No 24 Tahun 2022 dan UU PDP 27 tahun 2022. Meskipun terjadi penurunan sedikit dalam tingkat kompresi maksimum, hal ini tetap bisa diterima karena memberikan manfaat lebih besar berupa peningkatan keamanan data dan kemampuan sistem bekerja bersama dengan sistem lain secara lebih baik.

4.6 Metode Evaluasi Kinerja

Mekanisme evaluasi kinerja dalam penelitian ini didasarkan pada pendekatan eksperimental yang sistematis, bertujuan untuk menilai efektivitas kombinasi enkripsi Advanced AES dan LZMA dalam pengamanan dan optimalisasi ukuran data medis elektronik. Proses pengujian dirancang untuk mensimulasikan alur kerja data secara komprehensif mulai dari pengodean, kompresi, hingga enkripsi yang kemudian diikuti dengan proses dekripsi serta dekompresi guna memastikan integritas data.

Secara rinci evaluasi ini melibatkan pengujian berbasis dataset nyata dengan menggunakan 427 file DICOM anonim dari DICOM Library sebagai standar penyimpanan dokumen medis. Selain itu, 95 file JPG dokumen medis dan 20 file TIF hasil ekspor dari perangkat lunak DICOM Viewer turut diintegrasikan, dengan penekanan kuat pada sifat anonimitas data untuk menjaga privasi pasien. Seluruh proses pengujian dieksekusi dalam lingkungan terisolasi Docker, didukung oleh spesifikasi perangkat keras Intel Core generasi ke-7 dengan 12 thread *Central Processing Unit* (CPU) dan 16 *Gigabyte* (GB) *Random Access Memory* (RAM), sehingga menjamin konsistensi dan skalabilitas hasil.

Metode pengukuran otomatis diaplikasikan dengan memanfaatkan berbagai pustaka Python di antaranya *psutil* untuk monitoring sumber daya, *pandas* untuk manipulasi data dan *cryptography* untuk operasi enkripsi dan dekripsi, yang berperan penting dalam pengumpulan data kinerja. Terakhir analisis statistik digunakan untuk mengevaluasi hasil yang terkumpul meliputi analisis deskriptif seperti rata-rata, median dan standar deviasi untuk menggambarkan distribusi data, serta analisis inferensial seperti uji-t untuk membandingkan ukuran file sebelum dan sesudah kompresi dan enkripsi dan analisis regresi untuk mengevaluasi hubungan antar variabel seperti laju kompresi dan ukuran file akhir).

Untuk menilai efektivitas metode gabungan AES dan LZMA dalam pemrosesan data medis elektronik, evaluasi dilakukan berdasarkan empat parameter kunci.

1. Ukuran file (*File Size*) yang diukur sebelum dan sesudah proses kompresi serta enkripsi, menjadi indikator utama efisiensi penyimpanan. Tingkat efisiensi kompresi dihitung untuk menilai seberapa besar pengurangan ukuran file yang berhasil dicapai. Pengukuran ini didasarkan pada perbandingan antara ukuran enkripsi dan kompresi dengan ukuran file setelah dikompresi. Semakin besar selisih antara ukuran enkripsi dan kompresi dan ukuran file terkompresi, maka semakin tinggi pula persentase efisiensi kompresi yang berhasil diperoleh menunjukkan penghematan ruang penyimpanan yang lebih signifikan.
2. Waktu pemrosesan (*Processing Time*) yang meliputi durasi yang dibutuhkan untuk proses enkripsi dan dekripsi, merupakan parameter krusial untuk mengevaluasi kecepatan sistem, khususnya dalam konteks medis yang menuntut respons cepat.
3. Integritas data (*Data Integrity*) diukur secara cermat menggunakan metode checksum MD5 dan nilai hash untuk memastikan bahwa data tetap utuh dan tidak mengalami perubahan selama seluruh proses enkripsi dan dekripsi. Integritas data ini merupakan prinsip fundamental dalam keamanan data medis

4. Tingkat keamanan (*Security Level*) meskipun tidak diukur dengan metrik kuantitatif langsung, secara implisit dinilai melalui keberhasilan enkripsi data menjadi format yang tidak terbaca oleh manusia dan pemeliharaan integritas data selama proses. Implementasi AES sebagai standar enkripsi yang kuat juga menjadi indikasi penting dari tingkat keamanan yang dicapai.

Tujuan utama penelitian ini adalah untuk mengatasi keterbatasan yang ditemukan dalam studi-studi sebelumnya, terutama terkait masalah pembengkakan ukuran file setelah proses enkripsi. Sebagai solusi, penelitian ini berfokus pada peningkatan keamanan dan efisiensi terpadu. Penelitian sebelumnya mengenai enkripsi citra medis, yang sering menggunakan AES dan Base64, memang berhasil melindungi data, namun secara signifikan mengakibatkan ukuran file menjadi jauh lebih besar, sehingga menimbulkan tantangan serius dalam hal penyimpanan, khususnya di lingkungan dengan kapasitas terbatas. Di sisi lain, studi kompresi citra biner, seperti yang membandingkan *Chain Code* dan LZMA, cenderung memprioritaskan efisiensi kompresi namun kurang mendalam dalam eksplorasi aspek keamanan. Penelitian ini menghadirkan novelty dengan mengombinasikan AES dan LZMA untuk secara simultan mengatasi kedua keterbatasan tersebut. Hasil yang diperoleh menunjukkan kemampuan metode ini untuk mengurangi ukuran file antara 40-50%, dengan waktu enkripsi rata-rata sekitar 0.2-0.3 detik per file, sembari mempertahankan integritas data secara utuh. Ini membuktikan bahwa penelitian berhasil menyediakan solusi yang tidak hanya aman tetapi juga mengoptimalkan penyimpanan data kesehatan, suatu aspek yang sangat penting untuk sistem informasi kesehatan berbasis cloud.

Selain itu analisis sumber daya sistem juga menjadi fokus evaluasi dalam penelitian ini. Meskipun penelitian-penelitian sebelumnya mungkin tidak secara eksplisit menyajikan data rinci mengenai penggunaan CPU dan memori, studi ini menyajikan analisis komprehensif terkait hal tersebut. Ditemukan bahwa penggunaan CPU selama proses enkripsi mencapai 94.05% dan penggunaan memori sebesar 92.95 KB, sementara pada proses dekripsi, penggunaan CPU menurun menjadi 78.16% dengan konsumsi memori yang jauh lebih rendah, yaitu 31.07 KB. Diskusi dalam penelitian ini mengakui bahwa algoritma LZMA mungkin memerlukan durasi pemrosesan yang lebih lama dan AES membutuhkan sumber daya CPU yang besar, yang berpotensi memengaruhi kinerja sistem secara keseluruhan. Namun, hasil penelitian juga menunjukkan bahwa penggunaan CPU dapat tetap stabil antara 80-100% meskipun ukuran file bervariasi, mengindikasikan efisiensi dalam pemanfaatan sumber daya. Secara keseluruhan penelitian ini tidak hanya mengevaluasi kinerja metode yang dikembangkan berdasarkan parameter waktu, CPU dan

memori, tetapi juga secara kritis membandingkannya dengan celah dan tantangan yang ditemukan dalam literatur sebelumnya, sehingga menawarkan solusi terpadu yang lebih relevan untuk kebutuhan keamanan dan efisiensi data medis saat ini.

4.7 Hasil Produk

4.7.1 Docker Image

Dalam penelitian ini, seluruh proses pengolahan data mulai dari encoding Base64, dilanjutkan dengan kompresi menggunakan algoritma LZMA, hingga enkripsi dan dekripsi menggunakan AES diimplementasikan dalam lingkungan virtualisasi berbasis Docker. Docker dimanfaatkan sebagai platform containerization yang memfasilitasi isolasi aplikasi, konsistensi eksekusi serta kemudahan replikasi oleh pihak lain.

Output utama dari implementasi ini adalah sebuah Docker image bernama `totorajo/midstorage:1.0`. Image ini dikembangkan berdasarkan kerangka kerja Flask dan menyertakan semua dependensi Python yang esensial untuk menjalankan metode gabungan Base64, kompresi LZMA dan enkripsi AES. Docker image ini dirancang untuk kemudahan pengunduhan, eksekusi dan pengembangan lanjutan baik untuk tujuan akademik maupun aplikasi praktis dalam sistem informasi kesehatan digital.

Untuk pengembang sistem informasi kesehatan dari klinik mitra yang ingin mengimplementasikan Docker image `totorajo/midstorage:1.0`, prosesnya dirancang untuk kemudahan dan efisiensi, memanfaatkan kapabilitas platform containerization. Pengguna dapat memulai dengan mengunduh image tersebut dari Docker Hub atau registry lain melalui perintah `docker pull`. Setelah image berhasil diunduh, aplikasi dapat dijalankan sebagai container menggunakan perintah `docker run`, yang memungkinkan pemetaan porta lokal ke porta aplikasi di dalam *container*. Karena image ini dibangun di atas framework Flask, aplikasi di dalamnya kemungkinan akan mengekspos endpoint API. Melalui endpoint API ini, pengembang dapat mengintegrasikan metode pengolahan data Base64, LZMA, AES ke dalam aplikasi mereka dengan melakukan panggilan API HTTP untuk mengirim data dan menerima kembali hasil yang telah diproses. Pendekatan berbasis Docker ini menawarkan beberapa keuntungan signifikan, termasuk kemudahan implementasi dan deployment karena semua dependensi terbungkus dalam satu unit. Hal ini menjamin konsistensi dan isolasi lingkungan eksekusi, mengurangi masalah kompatibilitas antar sistem. Selain itu Docker memfasilitasi skalabilitas, memungkinkan pengguna untuk menjalankan beberapa instansi

container jika beban kerja meningkat serta mempromosikan replikabilitas hasil penelitian dan kolaborasi lebih lanjut di masa depan.

4.7.2 Pengembangan API untuk Developer

Sebagai bagian dari hasil produk penelitian, sistem juga dikembangkan dalam bentuk API endpoint berbasis web, sehingga mempermudah developer dalam mengintegrasikan metode pengamanan dokumen medis elektronik ke dalam sistem informasi kesehatan yang sudah ada.

Arsitektur API dibangun menggunakan Flask, sebuah framework mikro dalam bahasa pemrograman Python yang ringkas dan fleksibel. Dengan API yang disediakan, developer dapat mengakses layanan enkripsi, kompresi dan verifikasi integritas data melalui permintaan HTTP sederhana. Beberapa endpoint yang tersedia antara lain:

- a. POST */process* melakukan permintaan untuk enkripsi dan kompresi
- b. POST */decrypt* melakukan permintaan mendapatkan file dalam bentuk base64

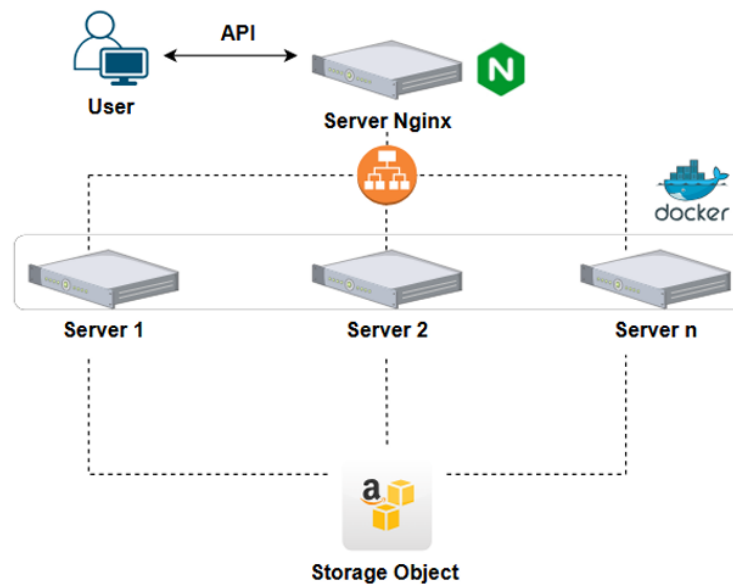
Keberadaan API ini sangat penting karena:

- a. Meningkatkan kemampuan integrasi metode dengan sistem lain.
- b. Mempercepat adopsi teknologi oleh pihak rumah sakit, laboratorium atau penyedia layanan kesehatan digital.

Mempermudah pengembangan lanjutan seperti SDK, plugin atau integrasi mobile-based. Selain itu API ini juga dilengkapi dengan dokumentasi lengkap dalam format JSON dan contoh request-response, sehingga memudahkan developer dalam memahami cara penggunaannya. File Postman collection juga disediakan sebagai lampiran untuk uji coba langsung oleh pengguna.

4.7.3 Implementasi Arsitektur Mikroservices

Untuk meningkatkan skalabilitas dan performa sistem dalam skema penyimpanan dan pertukaran data berbasis cloud. Desain sistem telah dirancang sedemikian rupa agar siap untuk dikembangkan dalam arsitektur tersebut.



Gambar 4.21 Implementasi modul.

Gambar 4.21 menunjukkan pendekatan ini memberikan beberapa keuntungan seperti:

- Modularitas tinggi yaitu setiap layanan dapat dikembangkan, diperbaiki atau diupdate secara mandiri.
- Skalabilitas elastis yaitu masing-masing modul dapat di skala secara horizontal jika beban kerja meningkat.
- Fault tolerance* yaitu Jika salah satu modul gagal, sistem secara keseluruhan tetap bisa beroperasi.

Dalam skema ini Nginx digunakan sebagai load balancer untuk mendistribusikan permintaan ke beberapa server backend Server 1, Server 2, sampai Server n, sehingga mencegah *bottleneck* dan meningkatkan responsivitas sistem. Selain itu penggunaan *object storage* seperti Backblaze B2 *Storage* memungkinkan penyimpanan file terenkripsi secara aman dan terdistribusi. Integrasi dengan library *b2sdk* menunjukkan bahwa sistem ini sudah mendukung interaksi langsung dengan layanan cloud. Hal ini menjadi dasar penting untuk pengembangan infrastruktur kesehatan digital berbasis cloud-native di masa depan.

4.8 Kontribusi Penelitian terhadap Bidang Forensika Digital

Pembahasan ini menganalisis secara mendalam bagaimana metode yang dikembangkan, yakni integrasi enkripsi AES dan kompresi LZMA untuk dokumen medis elektronik, memberikan kontribusi signifikan terhadap konsentrasi keilmuan Forensika Digital. Pilar utama Forensika Digital adalah penjaminan integritas dan kerahasiaan data.

Pertama aspek integritas data yang kuat dari metode ini sangat vital bagi praktik forensika digital. Hasil penelitian secara konsisten menunjukkan bahwa data tetap utuh sebelum dan sesudah proses enkripsi dan dekripsi, sebagaimana dibuktikan dengan nilai checksum MD5 yang identik. Dalam investigasi forensik, kemampuan untuk membuktikan bahwa bukti digital tidak mengalami perubahan atau perusakan adalah prasyarat mutlak bagi keabsahannya di pengadilan. Dengan memastikan integritas data dari sumbernya, metode ini secara langsung mendukung prinsip *chain of custody* dan keandalan bukti digital.

Kedua keamanan dan kerahasiaan data yang ditingkatkan melalui enkripsi AES memiliki implikasi besar dalam konteks forensik. Data medis adalah Data Pribadi yang bersifat spesifik menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang memerlukan perlindungan ekstra terhadap akses tidak sah. Dalam skenario pelanggaran data, meskipun suatu sistem berhasil ditembus, data yang terenkripsi akan membatasi sejauh mana informasi sensitif dapat terekspos, sehingga memitigasi dampak kerugian. Hal ini juga memudahkan tim forensik dalam menganalisis cakupan kebocoran dan memfokuskan upaya pemulihan pada data yang tidak terenkripsi atau yang kuncinya telah dikompromikan. Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis Permenkes No 24 Tahun 2022 juga secara eksplisit mengamankan keamanan, kerahasiaan dan keutuhan data RME, sehingga metode ini mendukung kepatuhan regulasi yang krusial untuk validitas data dalam penyelidikan.

Ketiga efisiensi penyimpanan dan manajemen data yang dicapai melalui kompresi juga relevan bagi forensika digital. Investigasi forensik seringkali melibatkan penanganan volume data yang sangat besar. Dengan mengurangi ukuran file secara signifikan 40-50% metode ini membuat proses akuisisi, penyimpanan dan analisis bukti digital menjadi lebih praktis dan efisien dalam penggunaan sumber daya. Efisiensi ini juga mendukung kepatuhan terhadap kewajiban retensi data jangka panjang untuk RME yaitu minimal 25 tahun yang diamanatkan oleh Permenkes No 24 Tahun 2022, memastikan ketersediaan data untuk potensi kebutuhan forensik di masa mendatang.

Terakhir penelitian ini secara eksplisit selaras dengan studi sebelumnya tentang *Secure Communication for Digital Forensics*, menegaskan bahwa solusi untuk mengamankan dokumen medis elektronik berkontribusi pada pengembangan lingkungan digital yang lebih aman secara keseluruhan. Lingkungan yang lebih aman mempermudah proses pengumpulan dan analisis bukti digital yang akurat dan terpercaya, serta mengurangi kompleksitas dalam menanggapi kegagalan Pelindungan Data Pribadi sebagaimana diatur dalam UU PDP.

4.9 Keterbatasan dan Titik Kegagalan Metode

Salah satu tantangan utama yang dihadapi dalam penelitian ini adalah rendahnya efisiensi kompresi pada file dengan karakteristik kompleks seperti file JPEG dan DICOM berwarna. Dalam beberapa skenario uji, ukuran file bahkan meningkat setelah proses kompresi dilakukan. Fenomena ini menunjukkan bahwa algoritma LZMA, meskipun secara umum efektif untuk data dengan pola yang sederhana, kurang optimal dalam menangani data dinamis atau gambar berwarna yang memiliki tingkat entropi yang tinggi.

Keterbatasan ini menjadi catatan penting bagi pengembang sistem Rekam Medis Elektronik untuk memilih metode kompresi yang sesuai dengan jenis dan karakteristik data yang akan diproses. Sebagai contoh metode LZMA mungkin sangat cocok digunakan untuk file monokrom atau data teks, tetapi perlu dikombinasikan atau diganti dengan teknik lain, seperti WebP atau DEFLATE, untuk file medis berwarna atau data visual yang lebih kompleks.

Meskipun terjadi kegagalan pada sebagian data penelitian ini tetap memberikan kontribusi signifikan dalam bentuk analisis karakteristik data medis elektronik dan evaluasi kinerja algoritma LZMA dalam berbagai skenario implementasi. Hasil ini dapat menjadi dasar bagi pengembang untuk merancang solusi yang lebih fleksibel dan tepat guna, terutama dalam konteks penyelenggaraan RME sesuai amanat Permenkes No. 24 Tahun 2022 tentang Rekam Medis.

Selain itu temuan ini juga membuka wawasan baru mengenai pentingnya penerapan pendekatan *adaptive compression*, yaitu strategi kompresi yang mampu menyesuaikan metode berdasarkan jenis dan struktur data yang diproses. Pendekatan semacam ini diharapkan mampu mengatasi masalah ketidaksesuaian antara algoritma kompresi dan karakteristik data, serta meningkatkan efisiensi penyimpanan tanpa mengorbankan integritas informasi medis.

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi metode pengamanan dokumen medis elektronik menggunakan kombinasi algoritma enkripsi AES dan kompresi LZMA, sesuai dengan amanat Permenkes Nomor 24 Tahun 2022. Pengujian dilakukan pada berbagai format file seperti DICOM, JPG dan TIF untuk menganalisis efektivitas metode terhadap beragam jenis data. Berdasarkan hasil pengujian diperoleh beberapa kesimpulan utama sebagai berikut:

1. Metode integrasi yang menggabungkan encoding Base64, kompresi LZMA dan enkripsi AES berhasil dirancang dan diimplementasikan secara fungsional. Metode ini mampu menjalankan seluruh siklus proses untuk melindungi komponen data gambar dan metadata dalam dokumen medis elektronik.
2. Hasil pengujian menunjukkan bahwa metode ini efektif dalam meningkatkan efisiensi penyimpanan, meskipun efektivitasnya bergantung pada karakteristik data. Pada file dengan struktur sederhana, metode ini berhasil mencapai pengurangan ukuran file rata-rata sebesar 55%. Namun, pada file dengan karakteristik kompleks atau berwarna, seperti beberapa file JPEG dan DICOM, ukuran file justru bertambah setelah dikompresi. Temuan ini membuktikan bahwa keberhasilan efisiensi penyimpanan sangat dipengaruhi oleh kompleksitas isi file, bukan hanya formatnya.
3. Dari segi performa, sistem menunjukkan kinerja yang stabil dan andal. Waktu proses relatif cepat, dengan rata-rata di bawah 0,3 detik untuk enkripsi, serta konsumsi memori rendah, sekitar 92,95 KB per file. Meskipun penggunaan CPU saat enkripsi mencapai 94,05%, hal ini tidak menjadi hambatan signifikan dalam lingkungan pengujian.
4. Integritas data terjaga sepenuhnya dalam semua skenario pengujian. Kesamaan nilai hash MD5 sebelum dan sesudah proses secara konsisten membuktikan bahwa metode ini tidak menyebabkan kehilangan atau perubahan data. Hal ini memenuhi syarat mutlak dalam sistem informasi kesehatan.

Secara keseluruhan penelitian ini menyimpulkan bahwa metode gabungan AES dan LZMA merupakan solusi yang layak dan fungsional untuk melindungi dokumen medis elektronik. Namun keberhasilannya memiliki batasan, terutama dalam hal efisiensi kompresi pada data yang kompleks. Temuan ini memberikan panduan praktis bagi pengembang

mengenai kekuatan dan kelemahan metode yang diusulkan. Metode gabungan Base64, LZMA dan AES terbukti layak digunakan untuk pengamanan dokumen medis elektronik. Namun terdapat keterbatasan pada efisiensi kompresi untuk file dengan struktur kompleks seperti beberapa file JPEG dan DICOM.

5.2 Saran

Meskipun penelitian ini telah berhasil menghasilkan solusi yang efektif dalam pengamanan dan optimasi penyimpanan file DICOM, JPG dan TIF terdapat beberapa aspek yang masih dapat dikembangkan lebih lanjut.

1. Optimasi Algoritma Enkripsi

Untuk platform dengan sumber daya terbatas seperti perangkat mobile atau edge computing, alternatif algoritma enkripsi seperti ChaCha20 dapat dievaluasi sebagai pengganti atau pelengkap AES, karena ChaCha20 menawarkan kecepatan yang lebih tinggi dengan tingkat keamanan yang tetap terjaga.

2. Pengujian pada Format Dokumen Medis Lain

Walaupun fokus penelitian ini adalah file DICOM, metode ini juga relevan untuk diuji pada format dokumen medis lain seperti PDF, HL7, FHIR atau XML yang sering digunakan dalam sistem informasi kesehatan. Dengan begitu, metode ini dapat diadopsi secara lebih luas dalam ekosistem kesehatan digital.

3. Analisis Keamanan Lebih Lanjut

Meskipun pengujian serangan bruteforce menunjukkan ketahanan yang kuat, penelitian lanjutan dapat mencakup simulasi serangan berbasis jaringan atau side-channel attacks untuk mengevaluasi keamanan sistem secara lebih mendalam.

Daftar Pustaka

- 10 largest healthcare data breaches of 2024 | TechTarget. (2024, December). <https://www.techtarget.com/healthtechsecurity/feature/Largest-healthcare-data-breaches>
- Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and Ubiquitous Computing*, 28(1), 59–72. <https://doi.org/10.1007/S00779-021-01583-8>
- Abdulzahra Hatem, M., Abdulkadhim Hameedi, B., & Nasir Hasoon, J. (2023). Lightweight digital imaging and communications in medicine image encryption for IoT system. *TELKOMNIKA Telecommunication Computing Electronics and Control*, 21(4), 771–783. <https://doi.org/10.12928/TELKOMNIKA.v21i4.24766>
- Ahmad, I., & Shin, S. (2021). A novel hybrid image encryption–compression scheme by combining chaos theory and number theory. *Signal Processing: Image Communication*, 98, 116418. <https://doi.org/10.1016/J.IMAGE.2021.116418>
- Al Duhayyim, M., Al-Wesabi, F. N., Marzouk, R., Hamza, M. A., Hilal, A. M., & Eltahir, M. M. (2021). Novel Image Encryption and Compression Scheme for IoT Environment. *Computers, Materials & Continua*, 71(1), 1443–1457. <https://doi.org/10.32604/CMC.2022.021873>
- Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) X. *Jurnal Pendidikan Sains Dan Komputer*, 2(01), 163–171. <https://doi.org/10.47709/JPSK.V2I01.1390>
- Das, S. K., & Rahman, M. Z. (2022). A secured compression technique based on encoding for sharing electronic patient data in slow-speed networks. *Heliyon*, 8(10), e10788. <https://doi.org/10.1016/J.HELİYON.2022.E10788>
- Hafsa, A., Sghaier, A., Malek, J., & Machhout, M. (2021). Image encryption method based on improved ECC and modified AES algorithm. *Multimedia Tools and Applications*, 80(13), 19769–19801. <https://doi.org/10.1007/S11042-021-10700-X>
- Hartono, B. (2023). Ransomware: Understanding the Digital Security Threat (In Indonesian Language). *Bincang Sains Dan Teknologi*, 2(02), 55–62. <https://doi.org/10.56741/bst.v2i02.353>

- Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., Islam, M., Alyahya, S., Ahmed, M. M., Kamil, S., & Hassan, M. A. (2021). Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. *IEEE Access*, 9, 47731–47742. <https://doi.org/10.1109/ACCESS.2021.3061710>
- Indriyajati, F., Margarith, M., Damiana Jawa, S., & Utomo, H. (2023). *Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia Article Info ABSTRAK*. 02(01), 59–66. <https://doi.org/10.58812/smb.v2i01>
- Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), 177–183. <https://doi.org/10.1016/J.EIJ.2020.07.003>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, 105. <https://doi.org/10.1016/j.cose.2021.102248>
- Malik, M. W., Husna, D., Purnama, I. K. E., Nurtanio, I., Hidayati, A. N., & Ratna, A. A. P. (2020). Development of Medical Image Encryption System Using Byte-Level Base-64 Encoding and AES Encryption Method. *ACM International Conference Proceeding Series*, 153–158. <https://doi.org/10.1145/3442555.3442580>
- Mishra, Z., & Acharya, B. (2020). High throughput and low area architectures of secure IoT algorithm for medical image encryption. *Journal of Information Security and Applications*, 53. <https://doi.org/10.1016/J.JISA.2020.102533>
- Mohammadi, H., Ghaderzadeh, A., & Sheikh Ahmadi, A. (2023). A Novel Hybrid Medical Data Compression Using Huffman Coding and LZW in IoT. *IETE Journal of Research*, 69(11), 7831–7845. <https://doi.org/10.1080/03772063.2022.2052985>
- Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis*. (2022).
- Rodrigues, V. F., Paim, E. P., Kunst, R., Antunes, R. S., Costa, C. A. da, & Righi, R. da R. (2020). Exploring publish/subscribe, multilevel cloud elasticity, and data compression in telemedicine. *Computer Methods and Programs in Biomedicine*, 191. <https://doi.org/10.1016/J.CMPB.2020.105403>
- Rojas-Hernández, R., Díaz-De-león-santiago, J. L., Barceló-Alonso, G., Bautista-López, J., Trujillo-Mora, V., & Salgado-Ramírez, J. C. (2022). Lossless Medical Image

- Compression by Using Difference Transform. *Entropy*, 24(7).
<https://doi.org/10.3390/E24070951>
- Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *Journal of Infection and Public Health*, 13(10), 1567–1575. <https://doi.org/10.1016/J.JIPH.2020.06.027>
- Sarce Joel, A., Abdussalaam, F., Yunengsih, Y., Studi Manajemen Informasi Kesehatan, P., Piksi Ganesha, P., Bandung, K., Jawa Barat, P., & Studi Manajemen Informatika, P. (2023). Information Technology-Based Medical Record Management in Handling Confidentiality and Security of Patient Data Using Cryptographic Methods (In Indonesian Language). *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, 4(3), 837–848. <https://doi.org/10.35870/JIMIK.V4I3.287>
- Sharma, D., & Prabha, C. (2023). Security and Privacy Aspects of Electronic Health Records: A Review. *2023 International Conference on Advancement in Computation and Computer Technologies, InCACCT 2023*, 815–820.
<https://doi.org/10.1109/INCACCT57535.2023.10141814>
- Sowmyalakshmi, R., Waly, M. I., Sikkandar, M. Y., Jayasankar, T., Ahmad, S. S., Rani, R., & Chavhan, S. (2021). An Optimal Lempel Ziv Markov Based Microarray Image Compression Algorithm. *Computers, Materials and Continua*, 69(2), 2245–2260.
<https://doi.org/10.32604/CMC.2021.018636>
- Sree, K., Murthy, R., & Manikandan, V. M. (2022). *A Reversible Data Hiding through Encryption Scheme for Medical Image Transmission Using AES Encryption with Key Scrambling*. <https://doi.org/10.12720/jait.13.5.433-440>
- Undang-undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. (2022).

LAMPIRAN