LAPORAN PROYEK SISTEM TERINTEGRASI STUDI KASUS: SECURE MESSAGING PLATFORM (CHAT & ENCRYPTION MICROSERVICES)

II3160 - TEKNOLOGI SISTEM TERINTEGRASI

Disusun Oleh:

Mudzaki Kaarzaqiel Hakim / 18223024

Nim teman sekelompok:

Raditya Zaki Athaya / 18223086

PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

2026

Daftar Isi

A. Deskripsi Sistem

Di tengah pesatnya perkembangan teknologi digital, persoalan privasi dalam komunikasi menjadi isu yang semakin krusial. Namun demikian, mayoritas platform pesan instan yang ada saat ini masih dirancang secara monolitik, sehingga menyulitkan proses audit keamanan secara mandiri. Berangkat dari permasalahan tersebut, kelompok kami menginisiasi perancangan sebuah sistem yang diberi nama "Secure Messaging Platform", yang mengedepankan pemisahan yang jelas antara logika pertukaran pesan dan mekanisme keamanan kriptografi. Sistem ini bertujuan untuk menyediakan layanan komunikasi pesan teks secara real-time dengan jaminan bahwa setiap pesan yang tersimpan di dalam basis data telah melalui proses enkripsi. Pendekatan ini diwujudkan melalui penerapan arsitektur microservices, di mana layanan pengelolaan pesan dan layanan keamanan dikembangkan sebagai komponen terpisah namun tetap saling terhubung.

Arsitektur sistem ini terdiri atas dua komponen utama yang saling berinteraksi melalui protokol HTTP dengan pendekatan RESTful API. Komponen pertama berperan sebagai pengelola aktivitas pengguna, meliputi pendaftaran akun, pengaturan daftar kontak, serta mekanisme pengiriman dan penerimaan pesan. Komponen ini menjadi antarmuka utama bagi pengguna akhir dan dirancang untuk menjamin kenyamanan serta responsivitas dalam berkomunikasi, tanpa mengekspos kompleksitas teknis sistem. Seluruh informasi pengguna, termasuk data profil dan riwayat percakapan, disimpan secara terpusat menggunakan basis data berbasis dokumen guna mendukung fleksibilitas pengelolaan data.

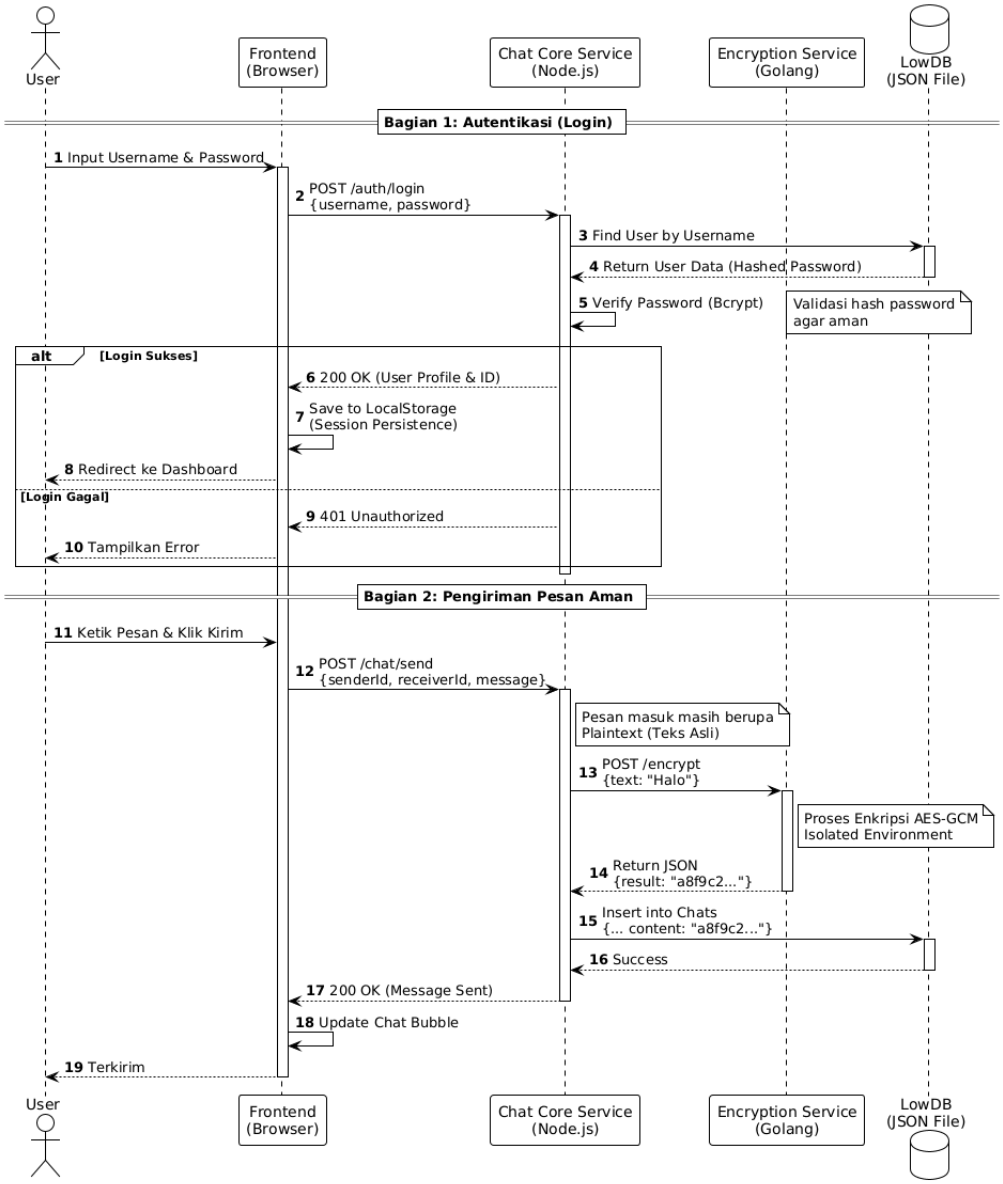
Komponen kedua merupakan layanan khusus yang difokuskan sepenuhnya pada operasi kriptografi dan berfungsi sebagai pusat keamanan sistem. Layanan ini tidak menyimpan data pengguna maupun isi pesan, melainkan hanya menangani permintaan untuk melakukan proses enkripsi dari teks asli (plaintext) ke bentuk terenkripsi (ciphertext), serta proses dekripsi sebaliknya. Dengan memisahkan tanggung jawab enkripsi ke layanan independen, sistem memungkinkan penggantian atau pembaruan algoritma keamanan tanpa memengaruhi fungsi utama aplikasi pesan. Pendekatan ini meningkatkan tingkat modularitas sekaligus mempermudah pemeliharaan dan pengembangan sistem di masa mendatang.

Proses kerja sistem diawali ketika seorang pengguna mengirimkan pesan melalui aplikasi. Sebelum pesan tersebut disimpan ke dalam basis data atau dikirimkan kepada penerima, sistem utama terlebih dahulu mengirimkan pesan dalam bentuk teks asli ke layanan enkripsi melalui jalur komunikasi internal yang aman. Layanan enkripsi kemudian memproses pesan tersebut menggunakan kunci kriptografi yang telah ditentukan dan mengembalikan hasilnya dalam bentuk teks terenkripsi. Hanya pesan yang telah dienkripsi inilah yang disimpan secara permanen, sehingga tingkat kerahasiaan data tetap terjaga meskipun terjadi pelanggaran keamanan pada basis data.

Pada saat pengguna penerima membuka pesan yang diterima, sistem akan menjalankan proses sebaliknya. Sistem utama mengambil pesan dalam bentuk terenkripsi dari penyimpanan,

lalu mengirimkannya ke layanan enkripsi dengan menyertakan konteks kunci yang sesuai untuk proses dekripsi. Setelah pesan berhasil dikembalikan ke bentuk teks yang dapat dibaca, hasil tersebut diteruskan ke aplikasi pengguna. Seluruh rangkaian proses ini berlangsung dalam waktu yang sangat singkat, sehingga keamanan komunikasi tetap terjamin tanpa mengorbankan kecepatan dan kenyamanan pengguna.

Untuk menggambarkan interaksi fungsional antara pengguna dan sistem, berikut adalah diagram *Use Case* yang memvisualisasikan fitur-fitur utama yang tersedia dalam *Secure Messaging Platform*:



Gambar Diagram Use Case

Diagram Use Case di atas merepresentasikan fungsionalitas inti yang dapat diakses oleh aktor tunggal yaitu "User". Proses dimulai dengan Registrasi Akun dan Login, yang merupakan gerbang utama bagi pengguna untuk mendapatkan token akses yang valid. Setelah terautentikasi, pengguna dapat memperluas jaringan komunikasi mereka melalui use case Tambah Teman, yang menerapkan logika persetujuan mutual untuk memastikan privasi. Aktivitas utama dalam sistem ini tercermin dalam use case Kirim Pesan dan Lihat Riwayat Chat. Penting untuk dicatat bahwa kedua aktivitas ini memiliki ketergantungan inklusif (include relationship) terhadap proses kriptografi di latar belakang; pengiriman pesan secara otomatis memicu proses Enkripsi Pesan, sedangkan pengambilan riwayat chat memicu proses Dekripsi Pesan. Mekanisme ini menegaskan bahwa meskipun pengguna berinteraksi dengan antarmuka chat standar, sistem secara aktif melakukan pengamanan data di setiap transaksi informasi tanpa intervensi manual dari pengguna.

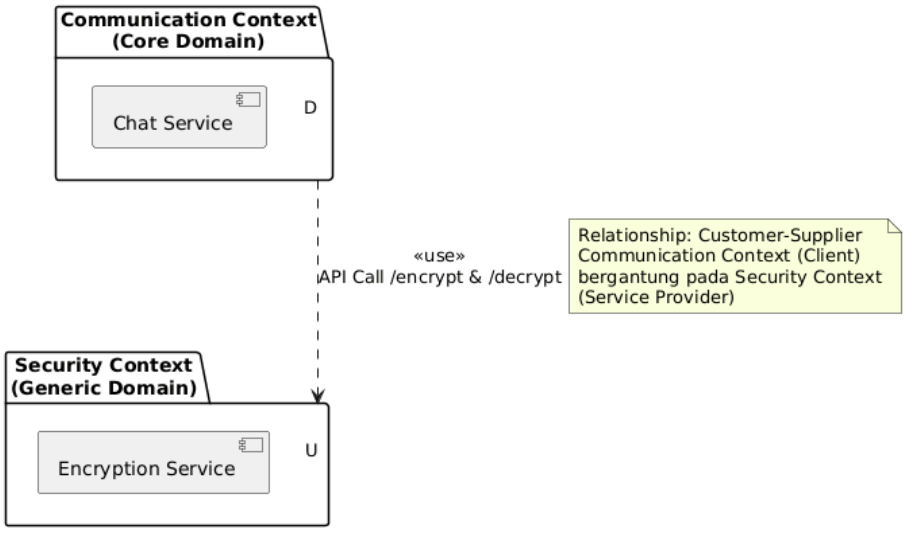
B. Bounded Context

Dalam pendekatan perancangan sistem terintegrasi yang mengacu pada prinsip Domain Driven Design atau DDD, sistem ini dibangun dengan mengidentifikasi dua Bounded Context utama yang memiliki pemisahan tanggung jawab fungsional serta struktur data yang berbeda secara jelas. Bounded Context pertama adalah Communication Context yang berfokus pada pengelolaan interaksi pengguna dan administrasi data terkait komunikasi. Pada domain ini, entitas User direpresentasikan sebagai identitas sosial yang mencakup informasi daftar kontak serta riwayat interaksi antar pengguna, sedangkan entitas Message diposisikan sebagai objek pertukaran informasi yang menyimpan atribut pengirim, penerima, dan waktu pengiriman. Tanggung jawab utama konteks ini terletak pada pengendalian hak akses komunikasi, namun konteks ini tidak bergantung pada detail teknis mekanisme pengamanan data. Pengetahuan domainnya dibatasi pada ketentuan bahwa isi pesan harus disimpan dalam bentuk yang tidak dapat dipahami secara langsung.

Bounded Context kedua adalah Security Context yang berperan sebagai domain terisolasi untuk menangani proses komputasi kriptografi dan prosedur matematis yang menyertainya. Di dalam konteks ini, konsep bisnis seperti pengguna, relasi sosial, atau histori percakapan tidak memiliki relevansi domain dan sepenuhnya diabstraksikan. Fokus operasional Security Context tertuju pada proses transformasi data dari bentuk Plaintext ke Ciphertext serta pengelolaan kunci enkripsi sebagai bagian dari mekanisme keamanan. Tanggung jawab utama konteks ini adalah menjamin aspek kerahasiaan dan integritas data melalui penerapan standar enkripsi AES GCM, tanpa mempertimbangkan sumber maupun tujuan akhir penggunaan data tersebut.

Interaksi antara kedua Bounded Context tersebut didefinisikan melalui pola hubungan Customer Supplier. Dalam pola ini, Communication Context berperan sebagai pihak yang bergantung pada layanan keamanan yang disediakan oleh Security Context untuk memenuhi

kebutuhan proteksi data sistem secara menyeluruh. Ketergantungan ini menegaskan bahwa keamanan data bukan merupakan tanggung jawab langsung domain komunikasi, melainkan disediakan oleh domain khusus yang berperan sebagai pemasok layanan kriptografi. Ilustrasi mengenai pemisahan domain serta hubungan antar Bounded Context tersebut disajikan pada diagram Bounded Context berikut ini.



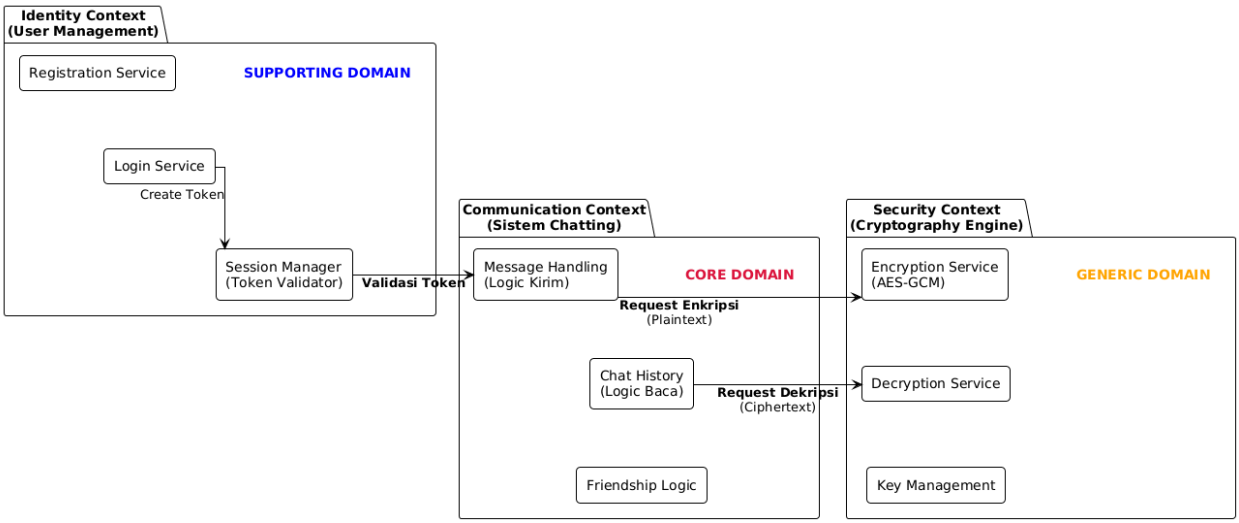
Gambar Diagram Bounded Context

C. Dekomposisi Subdomain

Diagram dekomposisi yang ditampilkan pada bagian ini memiliki dua tujuan utama, yaitu untuk mengelompokkan subdomain berdasarkan tingkat kepentingannya terhadap nilai bisnis serta untuk menggambarkan arsitektur sistem terdistribusi beserta pola interaksi antar konteks. Sebagaimana ditunjukkan dalam diagram, Communication Context yang berperan sebagai Core Domain bertindak sebagai pengendali utama alur sistem dan memiliki ketergantungan langsung terhadap dua domain lain yang bersifat pendukung. Seluruh interaksi antar konteks dirancang menggunakan mekanisme pemanggilan API secara sinkron, sehingga setiap proses berjalan secara berurutan dan terkoordinasi.

Pada setiap proses pengiriman pesan, sistem terlebih dahulu melakukan validasi sesi pengguna dengan memanggil layanan Session Manager yang berada dalam Identity Context untuk memastikan status autentikasi pengguna. Setelah pengguna dinyatakan sah, pesan dalam bentuk teks asli akan diteruskan ke Encryption Service yang berada di dalam Security Context untuk diproses melalui mekanisme pengamanan sebelum dilanjutkan ke tahap berikutnya. Pemisahan konteks yang divisualisasikan dalam diagram ini menegaskan bahwa meskipun ketiga domain saling berinteraksi secara intensif, masing masing tetap memiliki batasan yang jelas, sehingga pengembangan, pemeliharaan, maupun penggantian komponen dapat dilakukan secara independen tanpa berdampak langsung pada domain lainnya.

Mengacu pada prinsip Domain Driven Design, sistem Secure Messaging Platform dibagi ke dalam sejumlah subdomain khusus guna merepresentasikan prioritas dari perspektif bisnis maupun teknis. Diagram dekomposisi subdomain yang disajikan berikut ini memperlihatkan pembagian tersebut secara menyeluruh:



Gambar Diagram Dekomposisi Subdomain

Diagram dekomposisi diatas tidak hanya mengklasifikasikan subdomain berdasarkan prioritas bisnisnya, tetapi juga memvisualisasikan arsitektur terdistribusi dan alur interaksi antar konteks. Seperti yang terlihat pada diagram, Communication Context (Core Domain) bertindak sebagai orkestrator utama yang memiliki ketergantungan langsung terhadap dua domain lainnya.

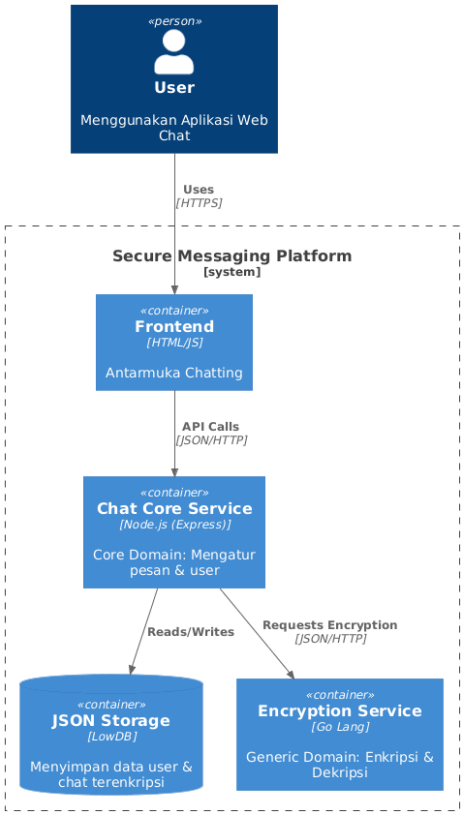
Dalam klasifikasi subdomain, Communication Management ditetapkan sebagai Core Domain karena merepresentasikan sumber utama nilai bisnis sistem, yaitu kemampuan untuk memfasilitasi pertukaran pesan antar pengguna. Subdomain ini memiliki kompleksitas logika bisnis tertinggi, mencakup pengelolaan aturan pengiriman pesan, penyimpanan riwayat percakapan, serta pengaturan relasi antar pengguna. Kategorisasi sebagai Core Domain didasarkan pada perannya sebagai fitur utama yang menjadi alasan utama penggunaan aplikasi. Subdomain ini dikembangkan secara khusus menggunakan teknologi Node.js dan LowDB guna memastikan performa serta fleksibilitas yang sesuai dengan kebutuhan sistem.

Cryptography Engine (yang dirancang oleh teman sekelompok / 18223086) diklasifikasikan sebagai Generic Domain karena berfungsi menangani proses enkripsi dan dekripsi pesan yang merupakan mekanisme standar dalam bidang keamanan informasi. Meskipun memiliki peran yang sangat penting dalam menjaga kerahasiaan data, logika kriptografi tidak dianggap sebagai keunikan bisnis sistem, melainkan sebagai solusi umum berbasis algoritma matematis yang telah terstandarisasi. Oleh karena itu, subdomain ini diimplementasikan sebagai layanan mikro yang

berdiri sendiri, sehingga dapat dimanfaatkan oleh Core Domain layaknya sebuah komponen utilitas tanpa menambah kompleksitas logika bisnis utama.

Sementara itu, User Identity ditempatkan sebagai Supporting Domain yang bertanggung jawab atas proses pendaftaran dan autentikasi pengguna. Subdomain ini dikategorikan sebagai pendukung karena meskipun fungsinya sangat penting untuk memastikan identitas dalam proses komunikasi, ia tidak menjadi fokus inovasi utama sistem. Pada implementasi saat ini, modul identitas digabungkan ke dalam layanan inti guna menyederhanakan struktur arsitektur, namun secara konseptual tetap berfungsi sebagai domain pendukung yang memungkinkan Core Domain berjalan dengan aman dan terkontrol.

Untuk mengimplementasikan rancangan domain tersebut, sistem dibangun menggunakan pendekatan arsitektur C4 Container yang mendefinisikan setiap komponen sebagai unit perangkat lunak yang dapat dijalankan dan dideploy secara terpisah. Seperti yang diperlihatkan pada diagram arsitektur di bawah ini, sistem ini terdiri dari empat kontainer utama:



Gambar Diagram Deployment Architecture

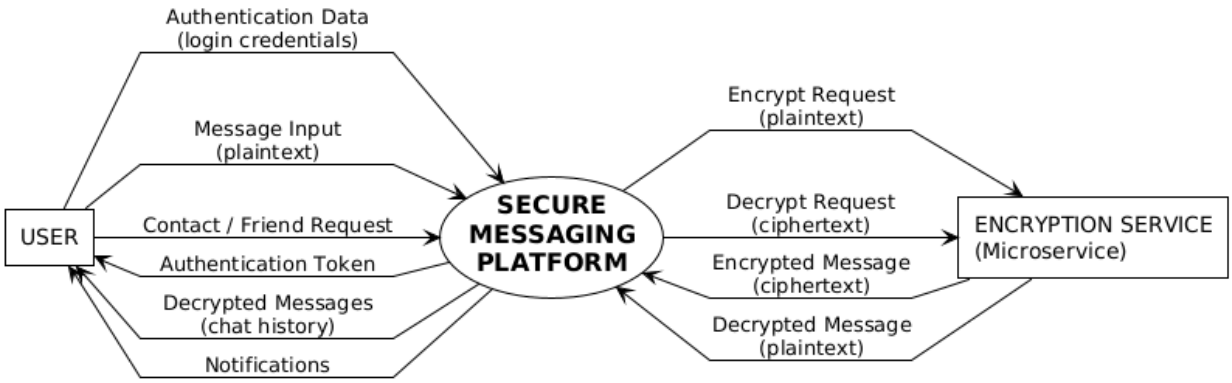
Komponen Frontend berbasis HTML dan JavaScript berfungsi sebagai antarmuka pengguna yang ringan dan berkomunikasi dengan layanan backend melalui protokol HTTPS yang aman. Chat Core Service berbasis Node.js menjadi wadah bagi Core Domain dan Supporting Domain,

dengan pemilihan Node.js didasarkan pada arsitektur event driven yang efisien dalam menangani beban komunikasi dengan intensitas operasi input output yang tinggi. Encryption Service yang diimplementasikan menggunakan bahasa Go berfungsi sebagai kontainer untuk Generic Domain, dengan pertimbangan performa dan efisiensi eksekusi dalam menangani operasi komputasi kriptografi seperti AES GCM. Adapun penyimpanan data menggunakan LowDB berbasis JSON yang menyediakan fleksibilitas dalam pengelolaan data pengguna dan pesan yang telah dienkripsi.

Seluruh komunikasi antar kontainer backend, khususnya antara Chat Core Service dan Encryption Service, dilakukan melalui antarmuka RESTful API dengan format data JSON. Pendekatan ini memastikan interoperabilitas yang tinggi antar layanan meskipun dibangun menggunakan teknologi yang berbeda.

Untuk mendefinisikan ruang lingkup sistem dan memetakan aliran informasi antara sistem utama dengan lingkungan luarnya, digunakan Diagram Konteks. Diagram ini memvisualisasikan Secure Messaging Platform sebagai satu kesatuan proses pusat (process circle) yang berinteraksi dengan dua entitas eksternal utama: User (Pengguna) dan Encryption Service (Layanan Enkripsi).

Penting untuk dicatat bahwa dalam diagram ini, Encryption Service digambarkan sebagai entitas eksternal. Pendekatan ini dipilih untuk mempertegas arsitektur terdistribusi dan mekanisme isolasi data, di mana sistem chat utama harus secara eksplisit "mengirimkan" data keluar batas sistemnya untuk diamankan, sebelum data tersebut dapat diproses atau disimpan lebih lanjut.



Gambar Diagram Context

Berdasarkan diagram konteks yang ditampilkan diatas, operasional sistem ditopang oleh dua jalur aliran data utama yang saling melengkapi. Jalur pertama merepresentasikan interaksi antara pengguna dan sistem, yang menggambarkan proses fungsional aplikasi. Pada alur ini, pengguna mengirimkan data berupa informasi otentikasi, pesan teks dalam bentuk asli (*plaintext*), serta permintaan penambahan kontak. Sebagai tanggapan, sistem mengembalikan token otentikasi

untuk validasi sesi, menyampaikan notifikasi sistem, dan menampilkan riwayat percakapan yang telah melalui proses dekripsi sehingga dapat dibaca oleh pengguna. Jalur kedua merepresentasikan mekanisme delegasi keamanan, di mana sistem utama secara sengaja tidak melakukan proses enkripsi secara internal. Sebagai gantinya, sistem mengirimkan permintaan yang memuat *plaintext* ke layanan eksternal Encryption Service untuk diproses. Layanan tersebut kemudian mengembalikan pesan dalam bentuk *ciphertext* kepada sistem utama untuk disimpan atau diteruskan sesuai kebutuhan. Pola pertukaran data dua arah ini menegaskan bahwa seluruh pemrosesan data sensitif dilakukan pada lingkungan yang terpisah dari logika bisnis inti, sehingga mendukung prinsip isolasi keamanan dan modularitas sistem.

LAMPIRAN

Link layanan terintegrasi	: https://chat-services.vercel.app/
API Message services	: http://hakim.tugastst.my.id/
API docs Message Services	: https://hakim.tugastst.my.id/api-docs/
API cipher services	: http://radit.tugastst.my.id/
src API Message services	: hakimmudzaki/chat-services
Src frontend	: hakimmudzaki/chat-services/tree/main/chat-frontend
Link youtube	: https://www.youtube.com/watch?v=PN2mIK4VamY

Link folder dokumen laporan 1 dan 2 : UAS TST