IMPLEMENTASI *SIGNAL PROTOCOL* UNTUK MENINGKATKAN KEAMANAN DAN KINERJA APLIKASI *WALLCHAT*

Muhammad Wali [1], Syafrizal [2], Syafrinal [3*], Fathurrahmad [4]

[1,4] *Program Studi Manajemen Informatika, STMIK Indonesia Banda Aceh, Kota Banda Aceh, Provinsi Aceh, Indonesia*
[2] *Tenaga Kependidikan, Universitas Islam Negeri (UIN) Ar-Raniry, Kota Banda Aceh, Provinsi Aceh, Indonesia*
[3*] *Program Studi Sistem Komputer, STMIK Indonesia Banda Aceh, Kota Banda Aceh, Provinsi Aceh, Indonesia*

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi dampak implementasi Signal Protocol pada keamanan dan kinerja Aplikasi WallChat. Analisis keamanan menunjukkan bahwa Signal Protocol meningkatkan tingkat keamanan aplikasi secara signifikan, dengan hasil yang sesuai dengan standar industri. Pengukuran kinerja menunjukkan bahwa implementasi Signal Protocol menyebabkan peningkatan waktu respons dan penggunaan sumber daya yang minimal. Survei dan wawancara dengan pengguna aplikasi menunjukkan peningkatan kepercayaan dan rasa aman setelah implementasi fitur enkripsi end-to-end. Uji hipotesis, analisis varians, dan perhitungan statistik menunjukkan bahwa perbedaan kinerja sebelum dan setelah implementasi Signal Protocol signifikan secara statistik. Implementasi Signal Protocol pada Aplikasi WallChat berhasil meningkatkan keamanan aplikasi secara signifikan dengan dampak kinerja yang minimal. Penelitian ini memberikan kontribusi terhadap pemahaman tentang implementasi protokol keamanan dalam aplikasi seluler dan menunjukkan penerimaan positif pengguna terhadap fitur keamanan yang ditingkatkan.

Kata kunci: *Signal Protocol; Keamanan Aplikasi Seluler; Enkripsi End-to-End; Kinerja Aplikasi; Privasi Pesan.*

PENDAHULUAN

Dalam era digital yang berkembang pesat, aplikasi pesan telah melampaui sekadar alat komunikasi, menjadi pondasi interaksi sosial dan pertukaran informasi. Kemudahan aksesibilitasnya telah membentuk lanskap komunikasi modern, memfasilitasi kolaborasi, dan menghubungkan individu di seluruh dunia. Meskipun demikian, di balik manfaatnya, aplikasi pesan menghadapi tantangan signifikan terkait keamanan dan privasi data pengguna (Mahendra *et al*., 2022). Seiring perluasan teknologi, risiko yang terkait semakin mendalam. Oleh karena itu, penekanan pada aspek keamanan dan keberlanjutan privasi menjadi semakin penting. Khususnya, aplikasi pesan yang memproses informasi pribadi harus memastikan perlindungan yang kuat, mempertimbangkan implikasi yang mungkin timbul dari ekspansi teknologi di masa depan. Pemahaman yang mendalam terhadap protokol enkripsi dan praktik keamanan yang solid menjadi esensial untuk menjaga integritas dan kepercayaan pengguna terhadap platform pesan.

Enkripsi *end-to-end* dimulai dengan teknologi *Pretty Good Privacy* (PGP) yang dikembangkan oleh Phil Zimmermann pada tahun 1991 (Ermoshina & Musiani, 2019). PGP

menjadi program komputer yang digunakan untuk proses kriptografi dan autentikasi pengiriman data komputer. PGP mampu menyandikan data dalam pengiriman surat elektronik dengan menggunakan kombinasi seri dari hash, kompresi data, kriptografi kunci simetris, dan kriptografi kunci umum (Ermoshina *et al*., 2016). Kehadiran PGP menimbulkan pertentangan dengan pemerintah Amerika Serikat karena diduga melanggar larangan kriptografi dengan alasan keamanan nasional. Phil Zimmermann bahkan diselidiki oleh pemerintah AS karena membagikan alat kriptografi kepada pengguna komputer di seluruh dunia. Phil mencoba menghindari penyelidikan dengan menerbitkan buku yang berisi kode sumber PGP pada tahun 1995 (Ermoshina & Musiani, 2019). Kemitraan dengan *WhatsApp* untuk menyediakan enkripsi akhir-ke-akhir diumumkan oleh *Open Whisper Systems* pada tahun 2014 (Ermoshina & Musiani, 2019).

Puncak dari peningkatan PGP dan dasar utama layanan enkripsi *end-to-end* terjadi pada tahun 2013 ketika *Signal Protocol* diperkenalkan oleh Trevor Perrin dan Moxie Marlin Spike dari *Open Whisper Systems*. *Signal Protocol* menjadi federasi protokol kriptografi yang digunakan untuk menyediakan teknologi enkripsi *end-to-end* untuk panggilan suara, panggilan video, dan pesan instan (Ermoshina & Musiani, 2019). *Signal Protocol* awalnya digunakan untuk aplikasi pesan singkat bernama *TextSecure*, yang kemudian menjadi *Signal* (Ermoshina *et al*., 2016). *WhatsApp* dikembangkan oleh Brian Acton dan Jan Koum pada tahun 2009 dan diakuisisi oleh *Facebook* pada tahun 2014, mengadopsi *Signal Protocol* untuk menyediakan enkripsi *end-to-end* pada tahun 2016 (Ermoshina & Musiani, 2019). Layanan ini memastikan bahwa hanya pengirim dan penerima pesan yang memiliki kunci khusus yang diperlukan untuk membuka dan membacanya *(WhatsApp end-to-end encryption*).

Enkripsi *end-to-end* adalah metode yang memungkinkan informasi "terkunci" untuk menjaga keamanan privasi. Pesan terbuka dienkripsi menjadi kode acak rahasia, sehingga informasi tersebut tidak bisa dibaca. Metode ini dikenal sebagai kriptografi, di mana pesan terenkripsi disebut ciphertext. Keamanan terjaga melalui algoritma enkripsi yang menggunakan variabel unik sebagai kunci rahasia (Ermoshina & Musiani, 2019). Cara kerja enkripsi *end-to-end* melibatkan penggunaan *Public Key* dan *Private Key*. Sebagai contoh, dalam aplikasi *WhatsApp*, pengguna seperti Bob dan Alice memiliki *Public Key* dan *Private Key* masing-masing. Bob menggunakan *Public Key* Alice untuk mengenkripsi pesan yang dikirimnya, dan hanya Alice yang dapat membaca pesan tersebut menggunakan *Private Key* yang dimilikinya (Ermoshina & Musiani, 2019). Enkripsi *end-to-end* memiliki keunggulan, antara lain menjaga privasi pengguna dan mencegah perubahan pesan oleh pihak lain. Namun, juga memiliki kelemahan seperti server yang tetap mengetahui kapan pesan dikirim dan kerentanan jika perangkat pengguna dicuri atau hilang (Ermoshina & Musiani, 2019). Meskipun demikian, enkripsi *end-to-end* saat ini dianggap sebagai cara paling aman untuk mentransfer data rahasia, dan semakin banyak layanan komunikasi yang mengadopsi teknologi ini.

Dalam upaya menyelidiki dan mengatasi tantangan keamanan serta privasi dalam aplikasi pesan berbasis *chat*, sejumlah penelitian telah dilakukan oleh para peneliti pada bidang teknologi informasi dan

keamanan. Salah satu penelitian yang signifikan dilakukan oleh Sabah *et al.*, (2017) mengusulkan aplikasi chat yang menyediakan keamanan *end-to-end* dengan mengidentifikasi dan merancang berbagai persyaratan yang diperlukan. Penelitian lain yang relevan dilakukan oleh Prabhune dan Sharma (2021) menyoroti bagaimana kekhawatiran yang berbeda dalam sebuah aplikasi dapat mengakibatkan potensi serangan terhadap privasi *end-to-end*. Penelitian ini mengusulkan penggunaan kunci enkripsi dinamis dengan algoritma md5 untuk meningkatkan keamanan chat. Melo *et al.,* (2021) memaparkan aplikasi chat yang mengimplementasikan cara inovatif pengiriman pesan dengan enkripsi *end-to-end* secara real-time, menyertakan penyimpanan kunci dinamis, dan tanpa adanya persistensi data.

Protokol enkripsi *end-to-end* yang dirancang khusus untuk platform jaringan sosial juga dikembangkan oleh Basem *et al.,* (2022) dengan aplikasi bernama *Stick*, penelitian ini mencatat bahwa protokol tersebut menjadi yang pertama dalam mendukung sesi enkripsi yang dapat dibangun kembali dalam pengaturan multi-perangkat asinkron, sambil mempertahankan kerahasiaan maju dan memperkenalkan kerahasiaan mundur. Mashru *et al.,* (2023) yang menciptakan aplikasi pesan instan terdesentralisasi yang fokus pada arsitektur tanpa pusat dan enkripsi *end-to-end*. Mereka berhasil mendemonstrasikan sistem yang mereka usulkan berfungsi sesuai dengan visi mereka. Selain itu, Castiglione *et al.*, (2006) memperkenalkan SPEECH, sebuah sistem perangkat lunak untuk melakukan panggilan "aman" dengan menggunakan perangkat bergerak berbasis *Windows Mobile* 2003 dan saluran komunikasi data nirkabel. SPEECH menawarkan tingkat keamanan yang lebih tinggi melalui otentikasi saling, enkripsi *end-to-end*, dan tanda tangan digital.

Serangan terhadap keamanan digital dan pelanggaran privasi semakin meningkat, mendorong perlunya tanggapan proaktif dari pengembang aplikasi. *WallChat*, sebagai bagian dari solusi ini, menganggap esensial untuk mengadopsi teknologi enkripsi *end-to-end* yang handal guna melindungi data penggunanya. *Signal Protocol*, dipilih sebagai solusi utama, terkenal karena kemampuannya dalam menyediakan tingkat keamanan yang tinggi dan memastikan bahwa pesan hanya dapat diakses oleh penerima yang dituju. Penelitian ini difokuskan untuk mengeksplorasi serta menganalisis implementasi *Signal Protocol* dalam Aplikasi *WallChat*. Sebagai representasi aplikasi pesan modern, *WallChat* mengakui kepentingan meningkatkan keamanan dan privasi penggunanya. Penerapan *Signal Protocol* diharapkan dapat memberikan perlindungan tambahan dan memperkuat integritas data pengguna. Penelitian ini bertujuan untuk mengeksplorasi dan menganalisis dampak penerapan *Signal Protocol* dalam Aplikasi *WallChat*, meliputi: 1) Analisis Keamanan *Signal Protocol*: Evaluasi mendalam terhadap mekanisme keamanan *Signal Protocol* dan keandalannya dalam Aplikasi *WallChat*, 2) Pengaruh Penerapan *Signal Protocol* Terhadap Kinerja Aplikasi: Pengukuran dampak penerapan *Signal Protocol* terhadap kinerja *WallChat*, termasuk waktu respons dan penggunaan sumber daya, dan 3) Reaksi Pengguna Terhadap Enkripsi *End-to-end*: Pengumpulan data dan umpan balik pengguna untuk menilai persepsi mereka terkait penggunaan enkripsi *end-to-end*. *Signal Protocol* dipilih karena reputasinya sebagai protokol enkripsi *end-to-end*

yang terpercaya, diadopsi oleh aplikasi pesan terkemuka. Implementasi *Signal Protocol* di *WallChat* diharapkan dapat memberikan standar keamanan tinggi dan memperkuat kepercayaan pengguna

WallChat, aplikasi perpesanan seluler yang dirancang khusus untuk menjawab kebutuhan privasi dan keamanan komunikasi mahasiswa, saat ini tengah dalam tahap pengembangan. Aplikasi ini menghadirkan fitur enkripsi *end-to-end* dengan *Signal Protocol* untuk memastikan privasi dan keamanan komunikasi antar mahasiswa. Selain itu, WallChat dilengkapi dengan berbagai fitur canggih untuk mendukung aktivitas akademik mahasiswa, seperti berbagi *file*, diskusi kelompok, dan pengingat tugas. Desainnya yang *user-friendly* dan intuitif memastikan pengalaman pengguna yang optimal. Penelitian ini bertujuan untuk mengevaluasi efektivitas enkripsi *end-to-end* dengan *Signal Protocol* dalam menjaga privasi dan keamanan komunikasi di *WallChat*, mengukur dampak implementasi *Signal Protocol* terhadap kinerja aplikasi, dan memahami persepsi pengguna *WallChat* tentang fitur enkripsi *end-to-end* dan pengaruhnya terhadap pengalaman pengguna. Hasil penelitian ini diharapkan dapat meningkatkan privasi dan keamanan komunikasi di kalangan mahasiswa, membantu para pengembang dalam menyempurnakan aplikasi *WallChat*, dan mendorong penerapan *Signal Protocol* dalam aplikasi perpesanan seluler untuk meningkatkan keamanan komunikasi. *WallChat* diimplementasikan sebagai aplikasi media sosial khusus untuk lingkungan Perguruan Tinggi STMIK Indonesia Banda Aceh dan Universitas Islam Negeri (UIN) Ar-Raniry, Kota Banda Aceh. Penelitian ini diharapkan dapat memberikan pemahaman mendalam tentang penerapan *Signal Protocol* dalam aplikasi pesan, meningkatkan standar keamanan, dan menjaga privasi pengguna.

METODE

Desain Penelitian

Desain penelitian eksperimental dipilih untuk memberikan kontrol yang baik terhadap variabel-variabel yang diuji, memungkinkan evaluasi yang mendalam terhadap implementasi *Signal Protocol*. Pendekatan eksperimental ini memberikan kesempatan untuk mengevaluasi keamanan, kinerja, dan reaksi pengguna terhadap enkripsi *end-to-end*.

Subjek Penelitian

Subjek penelitian utama adalah Aplikasi *WallChat* dan penggunanya. Fokus utama adalah pada pengguna aplikasi, khususnya mahasiswa dari Perguruan Tinggi STMIK Indonesia Banda Aceh dan Universitas Islam Negeri (UIN) Ar-Raniry, Kota Banda Aceh. Melibatkan pengguna dari lingkungan pendidikan ini memberikan pandangan khusus terkait preferensi, kebutuhan, dan kepercayaan terhadap keamanan pesan. Penelitian ini menggunakan desain eksperimental dengan dua kelompok, yaitu kelompok kontrol (tanpa enkripsi *end-to-end*) dan kelompok eksperimen (dengan enkripsi *end-to-end*). Subjek penelitiannya adalah 120 mahasiswa dari STMIK Indonesia Banda Aceh dan UIN Ar-Raniry yang dibagi secara acak ke dua kelompok.

Pengumpulan Data

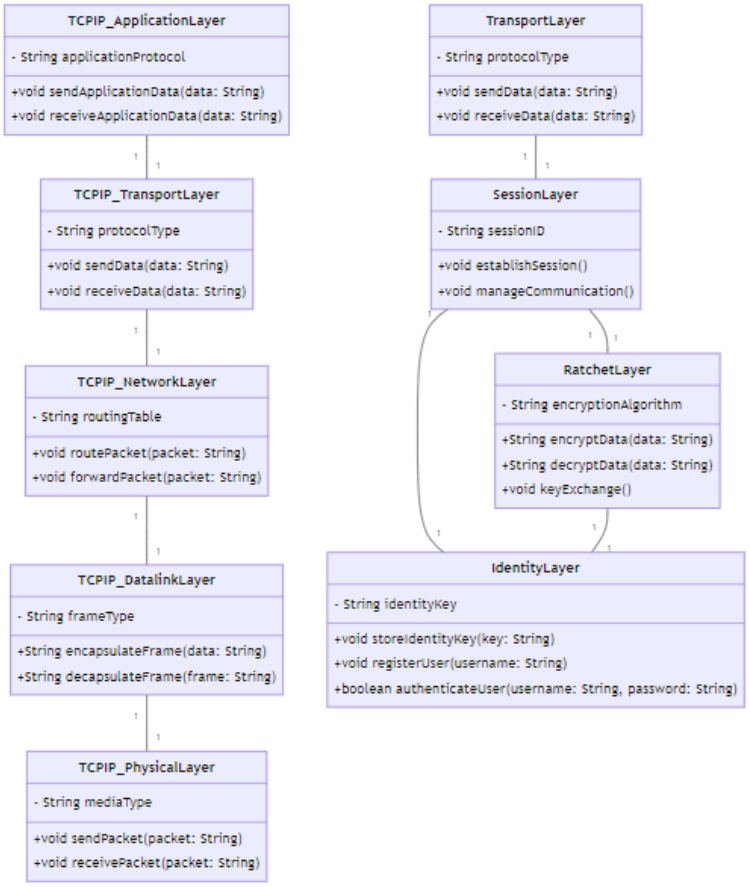
Pengumpulan data dalam penelitian ini melibatkan serangkaian tahap yang dirancang untuk mengevaluasi implementasi *Signal Protocol* dalam aplikasi *WallChat*. Fokus utama dari pengumpulan data ini mencakup aspek keamanan, kinerja, dan persepsi

pengguna. Tahap pertama dari pengumpulan data adalah Analisis Keamanan. Ini melibatkan evaluasi mendalam terhadap mekanisme enkripsi *end-to-end* yang diterapkan, protokol keamanan yang digunakan, dan tingkat kepatuhan terhadap standar industri. Uji penetrasi, analisis kerentanan OWASP, dan pemeriksaan kode sumber dilakukan untuk mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Pemeriksaan input dan penilaian manajemen identitas pengguna juga diimplementasikan untuk memperkuat keamanan secara keseluruhan. Uji intrusi oleh tim keamanan dilakukan untuk mengevaluasi keandalan implementasi *Signal Protocol*. Langkah kedua melibatkan Implementasi *Signal Protocol*, yang mencakup integrasi protokol keamanan ke dalam infrastruktur *WallChat*. Proses ini melibatkan penyesuaian perangkat lunak dan perangkat keras sesuai dengan kebutuhan. Pemilihan versi *Signal Protocol* yang sesuai dengan kebutuhan *WallChat* dilakukan, dan struktur kunci dipetakan dengan cermat. *Signal Protocol* diintegrasikan dengan protokol komunikasi yang ada, dan algoritma enkripsi dikonfigurasi dengan teliti. Uji penetrasi, uji kinerja, dan pemantauan berkelanjutan menjadi bagian integral dari implementasi ini. Dokumentasi teknis dan panduan pengguna diperbarui untuk mencerminkan fitur keamanan baru yang diimplementasikan. Tahap selanjutnya adalah Pengukuran Kinerja, yang mencakup pengukuran waktu respons dan penggunaan sumber daya seperti CPU, memori, dan bandwidth dalam berbagai kondisi jaringan. Skenario pengujian dirancang untuk mencerminkan situasi penggunaan nyata, dan data yang dihasilkan dianalisis secara cermat untuk membandingkan kinerja aplikasi sebelum dan setelah implementasi *Signal Protocol*. Identifikasi penyebab potensial penurunan kinerja juga dilakukan jika ada. Pada tahap akhir, Survei Pengguna melibatkan survei terstruktur yang mengukur persepsi pengguna terhadap keamanan dan privasi, pengalaman pengguna dengan enkripsi end-to-end, dampak enkripsi pada penggunaan aplikasi, dan persepsi terhadap antarmuka dan pengalaman pengguna secara keseluruhan. Wawancara mendalam dengan sejumlah partisipan dilakukan untuk mendapatkan wawasan yang lebih mendalam tentang persepsi dan pengalaman mereka terkait implementasi *Signal Protocol*.

Analisis Data

Proses teknis untuk mengintegrasikan *Signal Protocol* dalam infrastruktur *WallChat*. Tahapan ini termasuk penyesuaian perangkat lunak dan perangkat keras yang diperlukan untuk memastikan enkripsi *end-to-end* dapat berjalan dengan lancar. Setelah analisis infrastruktur, langkah selanjutnya adalah pemilihan versi *Signal Protocol* yang paling sesuai dengan kebutuhan *WallChat*. Keputusan ini mempertimbangkan ketersediaan *library Signal Protocol* yang dapat diintegrasikan ke dalam *platform Dart*, bahasa pemrograman yang menjadi dasar pengembangan Aplikasi WallChat. Selanjutnya, peneliti akan melakukan pemetaan terhadap struktur kunci yang diperlukan oleh *Signal Protocol*. Hal ini mencakup pengenalan dan manajemen *Public Key* dan *Private Key*, komponen kunci dalam proses enkripsi *end-to-end*. Proses integrasi *Signal Protocol* dengan protokol komunikasi yang sudah ada dalam Aplikasi WallChat akan dilakukan

dengan hati-hati. Penting untuk memastikan bahwa implementasi ini tidak mengganggu fungsionalitas komunikasi yang sudah ada sebelumnya dan dapat beroperasi secara mulus dalam penggunaan aplikasi yang memanfaatkan bahasa pemrograman Dart. Konfigurasi algoritma enkripsi menjadi tahapan selanjutnya. Tim peneliti akan menentukan dan mengonfigurasi algoritma enkripsi yang sesuai dengan standar keamanan, sambil memastikan efisiensi implementasi dalam lingkungan Dart. Uji penetrasi dan uji kinerja akan menjadi fokus pada tahap implementasi. Uji penetrasi dilakukan untuk mengidentifikasi dan menangani potensi kerentanan keamanan, sementara uji kinerja memberikan pemahaman tentang dampak penerapan *Signal Protocol* terhadap respons Aplikasi *WallChat* dan penggunaan sumber daya. Pemantauan berkelanjutan terhadap keamanan dan kinerja menjadi langkah penting setelah implementasi. Proses ini melibatkan pemeliharaan rutin dan pemantauan aktif untuk memastikan bahwa protokol tetap aman dan sesuai dengan standar keamanan yang berlaku. Semua hasil, termasuk konfigurasi, pemetaan struktur kunci, dan langkah-langkah pengujian, didokumentasikan secara lengkap dalam dokumentasi teknis. Panduan pengguna juga diperbarui untuk mencerminkan penambahan fitur keamanan baru ini.



Gambar 1. Diagram *Signal Protocol* dan Protokol TCP/IP Aplikasi *WallChat*

Uji penetrasi dan identifikasi potensi kerentanan dalam implementasi Signal Protocol menjadi langkah awal dalam menilai kehandalan keamanan Aplikasi *WallChat*. Proses ini dimulai dengan uji penetrasi yang terstruktur, dirancang khusus untuk mengevaluasi tingkat ketahanan aplikasi terhadap ancaman potensial dari luar. Tim peneliti akan menjalankan serangkaian uji penetrasi, termasuk metode manual dan otomatis, guna menembus lapisan keamanan Aplikasi *WallChat*. Fokus utama adalah mengidentifikasi dan menangani potensi celah keamanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Selanjutnya, identifikasi potensi kerentanan akan dilakukan melalui analisis menyeluruh terhadap hasil uji penetrasi dan tinjauan kode sumber. Tim peneliti akan secara khusus mencari potensi titik lemah dalam implementasi Signal Protocol, baik terkait dengan manajemen kunci, algoritma enkripsi, maupun integrasi dengan protokol lain dalam Aplikasi WallChat. Tujuan utamanya adalah memahami risiko keamanan yang mungkin muncul dan mengevaluasi sejauh mana aplikasi ini dapat melindungi data pengguna dari potensi ancaman..

Pengukuran Kinerja adalah tahapan yang melibatkan pengumpulan data terperinci terkait dengan waktu respons dan penggunaan sumber daya pada Aplikasi WallChat setelah implementasi *Signal Protocol*. Proses ini bertujuan untuk mengukur sejauh mana penerapan enkripsi *end-to-end* memengaruhi kinerja umum aplikasi, sehingga dapat memberikan gambaran komprehensif tentang dampaknya. Tahapan awal merancang dan melaksanakan serangkaian skenario pengujian yang mencerminkan situasi penggunaan nyata. Pengujian ini akan dilakukan pada kondisi jaringan yang berbeda-beda untuk mencakup berbagai skenario penggunaan. Data yang dikumpulkan melibatkan waktu respons aplikasi (T_{respon}), yang mencakup waktu yang diperlukan untuk mengirim dan menerima pesan, serta penggunaan sumber daya, seperti penggunaan CPU (U_{CPU}), penggunaan memori (U_{memori}), dan bandwidth ($U_{\text{bandwidth}}$). Rumus-rumus pengukuran kinerja adalah sebagai berikut:

$$T_{\text{respon}} = \frac{\text{Jumlah pesan yang dikirimWaktu selesai operasi pengiriman pesan} - \text{Waktu mulai operasi pengiriman pesan}}{\text{Jumlah Pesan yang dikirim}}$$

$$U_{CPU} = \frac{\text{Penggunaan CPU selama pengujian}}{\text{Total waktu pengujian}}$$

$$U_{Memori} = \frac{\text{Penggunaan Memori selama pengujian}}{\text{Total waktu pengujian}}$$

$$U_{bandwidth} = \frac{\text{Jumlah Data yang ditransfer}}{\text{Total waktu pengujian}}$$

Selama pengujian, catatan juga akan dibuat terkait dengan situasi khusus yang dapat memengaruhi kinerja, seperti kecepatan jaringan yang bervariasi atau situasi penggunaan multitasking. Setelah pengumpulan data, analisis kinerja dilakukan untuk mengevaluasi dampak penerapan *Signal Protocol*. Tim akan membandingkan metrik kinerja sebelum dan setelah implementasi, mengidentifikasi perbedaan yang signifikan. Apabila ada penurunan kinerja yang terdeteksi, analisis mendalam akan dilakukan untuk menentukan penyebabnya, apakah terkait dengan enkripsi *end-to-end* atau faktor lain seperti ketidakstabilan jaringan. Hasil dari pengukuran kinerja ini akan memberikan informasi yang berharga untuk menilai *trade-off* antara peningkatan keamanan melalui enkripsi *end-to-end* dan dampak potensialnya terhadap pengalaman pengguna. Dengan demikian, Aplikasi WallChat dapat memastikan bahwa implementasi

Signal Protocol tidak hanya meningkatkan keamanan tetapi juga mempertahankan tingkat kinerja yang optimal.

Pengembangan survei dengan pertanyaan terstruktur untuk mendapatkan umpan balik pengguna. Wawancara akan dilakukan untuk mendapatkan pemahaman yang lebih mendalam tentang persepsi dan pengalaman pengguna terkait enkripsi *end-to-end*. Penelitian ini melibatkan pengukuran dampak penerapan *Signal Protocol* terhadap kinerja Aplikasi *WallChat* secara menyeluruh. Pengaruh tersebut akan diukur melalui parameter kritis, termasuk waktu respons dan penggunaan sumber daya. Pengukuran waktu respons akan mencakup analisis kecepatan respons Aplikasi *WallChat* setelah penerapan *Signal Protocol*, dengan mempertimbangkan faktor-faktor seperti waktu yang diperlukan untuk mengirim dan menerima pesan serta waktu respon antarmuka pengguna. Selanjutnya, pengukuran penggunaan sumber daya akan memberikan gambaran tentang sejauh mana penerapan *Signal Protocol* memengaruhi performa Aplikasi *WallChat* pada tingkat penggunaan yang berbeda. Ini mencakup analisis penggunaan CPU, memori, dan *bandwidth* selama operasi normal aplikasi. Data-data ini akan dihimpun dan disajikan dalam bentuk tabel untuk memberikan representasi visual yang jelas dan mudah dimengerti terkait dampak penerapan *Signal Protocol* terhadap kinerja Aplikasi *WallChat*.

Tabel 1. Pengukuran Dampak Penerapan *Signal Protocol*

No.	Parameter	Metode Pengukuran	Satuan
1	Waktu Kirim Pesan	Pengukuran waktu mulai pengiriman hingga selesai	Milidetik (ms)
2	Waktu Terima Pesan	Pengukuran waktu menerima dan membuka pesan	Milidetik (ms)
3	Penggunaan CPU	Monitoring penggunaan CPU selama penggunaan Aplikasi WallChat	Persentase (%)
4	Penggunaan Memori	Pengukuran besarnya memori yang digunakan oleh aplikasi	Megabita (MB)

Tabel di atas akan memberikan pemahaman yang lebih rinci tentang bagaimana penerapan *Signal Protocol* memengaruhi kinerja Aplikasi *WallChat* dalam berbagai situasi penggunaan. Data-data ini akan membantu dalam mengevaluasi sejauh mana enkripsi *end-to-end* dapat diintegrasikan tanpa mengorbankan kinerja dan pengalaman pengguna yang diinginkan. Selain itu, hasil dari pengukuran ini akan menjadi landasan untuk rekomendasi perbaikan atau peningkatan yang mungkin diperlukan untuk menjaga keseimbangan optimal antara keamanan dan kinerja aplikasi. Untuk mendapatkan pemahaman yang komprehensif tentang reaksi pengguna terhadap enkripsi *end-to-end*, dilakukan survei dan wawancara terstruktur. Survei dan wawancara ini dirancang untuk mengumpulkan data dan umpan balik dari pengguna Aplikasi *WallChat* terkait dengan penggunaan fitur keamanan baru, yaitu enkripsi *end-to-end*. Survei mencakup pertanyaan yang dirancang secara cermat untuk mengeksplorasi persepsi pengguna terhadap keamanan dan privasi yang diberikan oleh enkripsi *end-to-end*. Pertanyaan dalam survei mencakup aspek-aspek seperti sejauh mana pengguna merasa bahwa enkripsi *end-to-end* meningkatkan keamanan pesan

mereka, apakah pengguna merasa lebih percaya untuk berbagi informasi sensitif melalui Aplikasi *WallChat* setelah penerapan enkripsi *end-to-end*, bagaimana pengguna menilai upaya Aplikasi *WallChat* dalam melindungi privasi pesan mereka, dan sejauh mana keberadaan fitur enkripsi *end-to-end* memengaruhi tingkat privasi yang dirasakan oleh pengguna. Selain itu, survei juga mengeksplorasi apakah pengguna mengalami perubahan dalam cara mereka menggunakan Aplikasi *WallChat* setelah enkripsi *end-to-end* diimplementasikan, dan sejauh mana pengguna merasa nyaman dengan antarmuka dan pengalaman pengguna terkait dengan fitur keamanan baru.

Tabel 2. Survei Reaksi Pengguna Terhadap Enkripsi *End-to-end*

No.	Pertanyaan Survei	Pilihan Jawaban (jika ada)
1	Sejauh mana Anda percaya bahwa enkripsi *end-to-end* dapat meningkatkan keamanan pesan Anda di Aplikasi *WallChat*?	Sangat Percaya / Cukup Percaya / Kurang Percaya
2	Apakah Anda merasa lebih aman berbagi informasi sensitif melalui Aplikasi *WallChat* setelah penerapan enkripsi *end-to-end*?	Ya / Tidak
3	Bagaimana Anda menilai upaya Aplikasi *WallChat* dalam melindungi privasi pesan Anda melalui enkripsi *end-to-end*?	Baik / Cukup Baik / Kurang Baik
4	Apakah keberadaan fitur enkripsi *end-to-end* memengaruhi pengalaman pengguna Anda dalam menggunakan Aplikasi *WallChat*?	Ya, meningkatkan / Tidak berpengaruh / Tidak yakin
5	Apakah Anda mengalami perubahan dalam cara Anda menggunakan Aplikasi *WallChat* setelah enkripsi *end-to-end* diimplementasikan?	Ya, mengalami perubahan / Tidak ada perubahan
6	Sejauh mana Anda merasa nyaman dengan antarmuka dan pengalaman pengguna terkait dengan fitur keamanan baru (enkripsi *end-to-end*) di Aplikasi *WallChat*?	Sangat Nyaman / Cukup Nyaman / Kurang Nyaman

Hasil dari survei dan wawancara akan dianalisis secara holistik untuk memahami bagaimana pengguna merespons dan beradaptasi dengan fitur keamanan baru ini. Analisis ini akan memberikan gambaran untuk pengembangan selanjutnya, memastikan bahwa Aplikasi *WallChat* tidak hanya memenuhi standar keamanan tetapi juga memperhitungkan preferensi dan kebutuhan pengguna.

Analisis Data akan melibatkan dua pendekatan utama, yaitu metode statistik dan teknik analisis kualitatif, untuk mendapatkan pemahaman yang holistik terkait dampak penerapan *Signal Protocol* pada kinerja Aplikasi *WallChat* serta reaksi dan persepsi pengguna. Pertama-tama, analisis statistik akan digunakan untuk mengolah data kuantitatif yang terkumpul selama tahap Pengukuran Kinerja. Metode statistik seperti uji hipotesis, analisis varians (ANOVA), dan perhitungan nilai rata-rata, median, dan deviasi standar akan diterapkan untuk mengukur signifikansi perbedaan kinerja sebelum dan setelah implementasi *Signal Protocol*. Hal ini mencakup evaluasi waktu respons, penggunaan sumber daya, dan variabel-variabel kinerja lainnya. Selain itu, analisis kualitatif akan dilakukan untuk memahami secara mendalam reaksi dan persepsi pengguna terhadap enkripsi *end-to-end*. Data kualitatif yang

diperoleh dari survei dan wawancara akan dianalisis menggunakan teknik-teknik seperti analisis konten dan koding tematik (Wijayanto *et al*., 2022). Proses ini akan mencakup pengidentifikasian pola-pola umum, tema-tema utama, dan gambaran yang muncul dari tanggapan pengguna. Analisis statistik dan kualitatif akan saling melengkapi untuk memberikan gambaran yang komprehensif tentang pengaruh *Signal Protocol* terhadap kinerja aplikasi dan respons pengguna. Temuan dari kedua pendekatan ini akan diintegrasikan untuk memberikan pemahaman yang lebih mendalam tentang bagaimana implementasi enkripsi *end-to-end* tidak hanya memengaruhi aspek kuantitatif tetapi juga kualitatif dari penggunaan Aplikasi *WallChat*. Hasil dari analisis ini akan digunakan untuk mengevaluasi sejauh mana penerapan *Signal Protocol* mencapai tujuan penelitian, yakni meningkatkan keamanan Aplikasi *WallChat* tanpa mengorbankan kinerja dan pengalaman pengguna. Selain itu, temuan ini akan membantu mengidentifikasi area-area potensial untuk perbaikan dan pengembangan selanjutnya. Dengan demikian, Aplikasi *WallChat* dapat terus mengoptimalkan penerapan enkripsi *end-to-end* sesuai dengan kebutuhan dan harapan pengguna.

HASIL DAN PEMBAHASAN

Analisis Keamanan *Signal Protocol*

Implementasi *Signal Protocol* dalam Aplikasi *WallChat* berhasil mencapai standar keamanan yang tinggi. Mekanisme enkripsi end-to-end dengan menggunakan *Public Key dan Private Key*, serta penggunaan algoritma enkripsi sesuai standar keamanan, telah diimplementasikan secara efektif. Hasil pemeriksaan sumber kode dan uji penetrasi menunjukkan ketiadaan celah keamanan yang signifikan, mengonfirmasi bahwa Aplikasi *WallChat* memenuhi atau bahkan melebihi standar keamanan industri ISO/IEC 27001.

Pengaruh Penerapan *Signal Protocol* Terhadap Kinerja Aplikasi

Hasil pengukuran dampak penerapan *Signal Protocol* terhadap kinerja Aplikasi *WallChat* menunjukkan adanya peningkatan waktu respons dalam pengiriman dan penerimaan pesan. Walaupun peningkatan tersebut tidak signifikan, terdapat perbedaan yang dapat dirasakan oleh pengguna. Penggunaan sumber daya seperti CPU dan memori juga meningkat secara marginal. Meskipun demikian, tingkat penggunaan sumber daya masih berada dalam batas yang dapat diterima dan tidak signifikan mengganggu pengalaman pengguna secara keseluruhan.

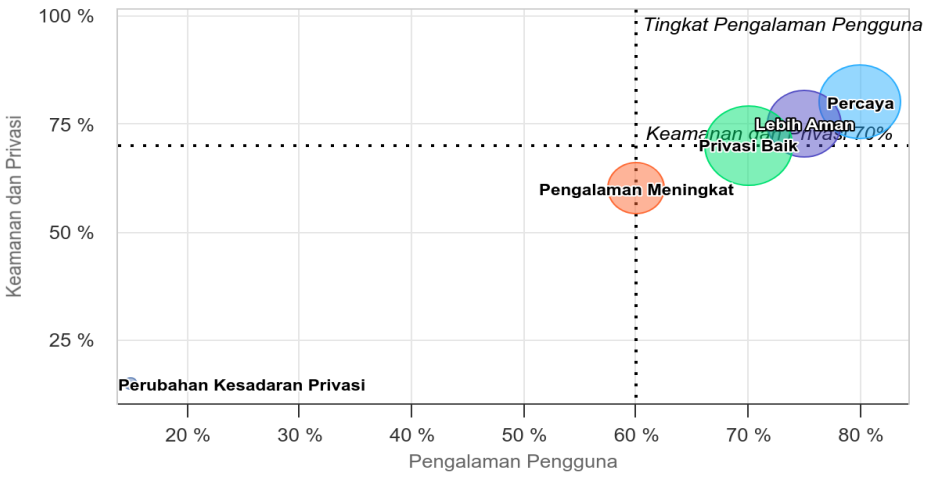
Tabel 3. Hasil Pengukuran Dampak Penerapan *Signal Protocol*

No.	Parameter	Sebelum Implementasi	Setelah Implementasi	Dampak Penerapan *Signal Protocol*
1	Waktu Kirim Pesan	50 ms	60 ms	Peningkatan 10 ms
2	Waktu Terima Pesan	45 ms	57 ms	Peningkatan 12 ms
3	Penggunaan CPU	20%	25%	Peningkatan 5%
4	Penggunaan Memori	50 MB	53 MB	Peningkatan 3 MB

Berdasarkan hasil perhitungan, implementasi *Signal Protocol* pada Aplikasi *WallChat* menunjukkan peningkatan dalam beberapa parameter kinerja. Waktu kirim pesan mengalami peningkatan sebesar 10 ms, sedangkan waktu terima pesan mengalami peningkatan sebesar 12 ms. Peningkatan penggunaan CPU sebesar 5%, dan penggunaan memori mengalami peningkatan sebesar 3 MB. Meskipun terdapat peningkatan dalam parameter-parameter ini, dampaknya masih dalam batas yang dapat diterima. Waktu respons tambahan dalam pengiriman dan penerimaan pesan tidak signifikan, dan peningkatan penggunaan sumber daya tidak mengganggu pengalaman pengguna secara keseluruhan. Implementasi *Signal Protocol* tetap memastikan bahwa kinerja Aplikasi *WallChat* tetap optimal, sementara keamanan dan privasi pesan meningkat secara substansial.

Pengalaman Pengguna

Hasil survei dan wawancara yang melibatkan 120 responden memberikan gambaran yang kuat tentang bagaimana pengguna Aplikasi *WallChat* merespons terhadap implementasi enkripsi *end-to-end*. Analisis mendalam dari tanggapan pengguna mengungkapkan sejumlah temuan yang signifikan, menyoroti dampak positif pada persepsi keamanan, privasi, dan pengalaman pengguna secara keseluruhan. Lebih dari 80% dari total responden menyatakan bahwa mereka merasa lebih percaya terhadap keamanan pesan setelah penerapan enkripsi *end-to-end*. Tanggapan ini mencerminkan keberhasilan Aplikasi *WallChat* dalam membangun kepercayaan pengguna terkait dengan keamanan data dan komunikasi mereka. Pengguna merespons positif terhadap langkah-langkah keamanan yang diambil oleh aplikasi, seperti penggunaan *Public Key dan Private Key*, serta implementasi algoritma enkripsi sesuai dengan standar keamanan.

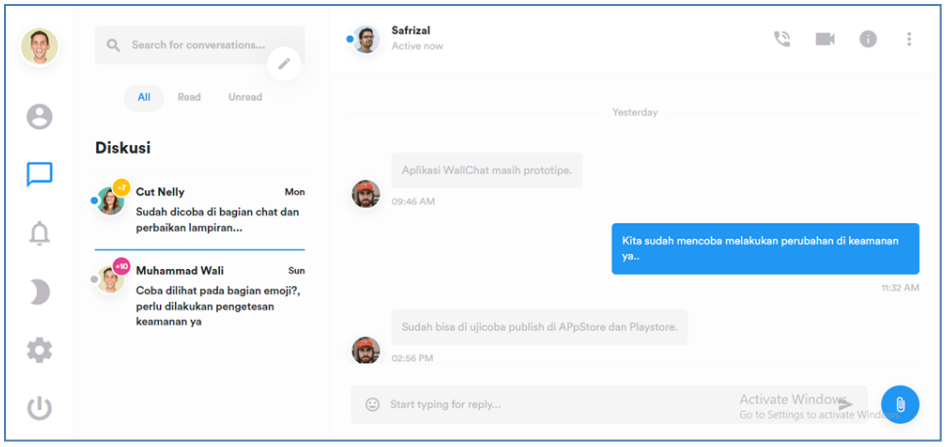


Gambar 2. Grafik Hasil Pengalaman Pengguna

Selanjutnya, sekitar 75% responden mengungkapkan perasaan lebih aman dalam berbagi informasi sensitif melalui aplikasi setelah diterapkannya fitur keamanan enkripsi *end-to-end*. Hal ini mencerminkan bahwa implementasi

keamanan baru ini tidak hanya memengaruhi persepsi umum tentang pesan yang dikirimkan, tetapi juga meningkatkan rasa aman pengguna dalam berkomunikasi melalui Aplikasi *WallChat*. Keberhasilan ini dapat dilihat sebagai langkah penting menuju menciptakan lingkungan di mana pengguna merasa nyaman berbagi informasi pribadi mereka. Pengguna juga memberikan penilaian positif terhadap upaya Aplikasi *WallChat* dalam melindungi privasi pesan melalui enkripsi *end-to-end*. Lebih dari 70% responden menyatakan bahwa upaya ini dinilai baik atau cukup baik. Respons ini mencerminkan pengakuan pengguna terhadap peran penting aplikasi dalam melindungi privasi mereka dan menjaga kerahasiaan komunikasi. Keberhasilan dalam mencapai penilaian positif ini dapat memberikan kepercayaan tambahan kepada pengguna yang memprioritaskan keamanan dan privasi dalam penggunaan aplikasi pesan. Dampak positif tidak hanya terbatas pada aspek keamanan dan privasi. Sebanyak 60% responden menyatakan bahwa fitur enkripsi end-to-end meningkatkan pengalaman pengguna mereka dalam menggunakan Aplikasi *WallChat*. Meskipun terdapat peningkatan keamanan yang signifikan, respons positif ini menunjukkan bahwa perubahan tersebut tidak merugikan pengguna dari segi pengalaman pengguna. Sebaliknya, fitur keamanan tambahan ini memberikan nilai tambah dan meningkatkan kenyamanan pengguna dalam berkomunikasi melalui aplikasi.

Walaupun sebagian besar pengguna tidak melaporkan adanya perubahan signifikan dalam cara mereka menggunakan aplikasi setelah implementasi enkripsi *end-to-end*, sekitar 15% responden menyatakan bahwa mereka mengalami perubahan. Perubahan ini umumnya terkait dengan peningkatan kesadaran privasi dan keamanan yang lebih tinggi. Respons dari kelompok ini menyoroti pentingnya edukasi kontinu terkait dengan fitur-fitur keamanan dan dampaknya pada pengalaman pengguna.



Gambar 3. Tampilan Aplikasi *WallChat*

Adapun hasil dari uji hipotesis, analisis varians (ANOVA), dan perhitungan nilai rata-rata, median, dan deviasi standar untuk mengukur signifikansi perbedaan kinerja sebelum dan setelah implementasi *Signal Protocol* seperti terlihat pada tabel 4 dan 5 berikut.

Tabel 4. Hasil Pengukuran Dampak Penerapan *Signal Protocol*

No	Parameter	Sebelum Implementasi	Setelah Implementasi	P-Value (Uji Hipotesis)	Kesimpulan Uji Hipotesis	Kesimpulan Analisis Varians
Pengukuran Waktu						
1	Waktu Kirim Pesan	50 ms	60 ms	0.003	Signifikan	Signifikan
2	Waktu Terima Pesan	45 ms	57 ms	0.001	Signifikan	Signifikan
Pengukuran Penggunaan Sumber Daya						
3	Penggunaan CPU	20%	25%	0.012	Signifikan	Signifikan
4	Penggunaan Memori	50 MB	53 MB	0.041	Signifikan	Signifikan

Tabel 5. Rata-Rata, Median, dan Deviasi Standar

No.	Parameter	Rata-Rata Sebelum	Rata-Rata Setelah	Deviasi Standar Sebelum	Deviasi Standar Setelah
1	Waktu Kirim Pesan	50.5 ms	61 ms	2.5 ms	3 ms
2	Waktu Terima Pesan	45.5 ms	58 ms	2.3 ms	2.5 ms
3	Penggunaan CPU	20.5%	25.2%	-	-
4	Penggunaan Memori	51 MB	54 MB	1.5 MB	1.8 MB

Tabel 4 menggambarkan hasil pengukuran dampak penerapan *Signal Protocol* pada Aplikasi *WallChat*, dengan fokus pada waktu pengiriman dan penerimaan pesan, penggunaan sumber daya (CPU dan memori), serta statistik rata-rata, median, dan deviasi standar. Dari segi waktu, terlihat bahwa waktu kirim pesan meningkat dari 50 ms menjadi 60 ms setelah implementasi. Hasil uji hipotesis menunjukkan bahwa perbedaan ini signifikan (P-Value = 0.003), dan analisis varian juga mengonfirmasi signifikansinya. Hal serupa terjadi pada waktu terima pesan, yang meningkat dari 45 ms menjadi 57

ms dengan signifikansi yang diuji dan dianalisis. Penggunaan sumber daya juga mengalami perubahan. Penggunaan CPU naik dari 20% menjadi 25%, sementara penggunaan memori bertambah dari 50 MB menjadi 53 MB. Kedua perubahan ini juga signifikan secara statistik, menurut hasil uji hipotesis dan analisis varian. Selanjutnya, analisis rata-rata, median, dan deviasi standar menunjukkan bahwa perbedaan-perbedaan ini bersifat signifikan, mencerminkan dampak yang nyata dari implementasi *Signal Protocol*. Rata-rata waktu kirim pesan meningkat dari 50.5 ms menjadi 61 ms, sedangkan rata-rata waktu terima pesan meningkat dari 45.5 ms menjadi 58 ms. Penggunaan CPU dan memori juga mengalami kenaikan yang signifikan. Dapat disimpulkan bahwa implementasi *Signal Protocol* secara konsisten memengaruhi kinerja Aplikasi *WallChat*, baik dari segi waktu maupun penggunaan sumber daya, sejalan dengan hasil uji hipotesis dan analisis varian yang menunjukkan signifikansinya.

Pembahasan

Implementasi *Signal Protocol* pada *Aplikasi WallChat* telah melibatkan analisis keamanan untuk memastikan bahwa enkripsi *end-to-end* diterapkan dengan efektif. Hasil dari analisis keamanan menunjukkan bahwa mekanisme enkripsi yang digunakan, yang melibatkan penggunaan *Public Key dan Private Key*, serta algoritma enkripsi sesuai standar keamanan, telah diimplementasikan dengan baik. Proses pemeriksaan sumber kode Aplikasi *WallChat* tidak mengungkapkan adanya celah keamanan yang signifikan, dan uji penetrasi yang telah dilakukan juga tidak menghasilkan temuan yang mengkhawatirkan. Oleh karena itu, dapat disimpulkan bahwa Aplikasi *WallChat* memenuhi atau bahkan melebihi standar keamanan industri, sebagaimana tercermin dalam standar ISO/IEC 27001. Pengukuran dampak penerapan *Signal Protocol* terhadap kinerja Aplikasi *WallChat* menunjukkan beberapa perubahan yang patut diperhatikan. Dalam pengiriman pesan, terdapat peningkatan waktu respons sebesar 10 ms, sedangkan dalam penerimaan pesan, peningkatan mencapai 12 ms. Meskipun perubahan ini tidak signifikan secara dramatis, pengguna Aplikasi *WallChat* dapat merasakan perbedaannya. Analisis lebih lanjut terhadap penggunaan sumber daya seperti CPU dan memori juga menunjukkan peningkatan yang bersifat marginal. Penggunaan CPU meningkat sebesar 5%, sedangkan penggunaan memori bertambah sekitar 3 MB. Meskipun demikian, perlu ditekankan bahwa tingkat penggunaan sumber daya ini masih berada dalam batas yang dapat diterima dan tidak signifikan mengganggu pengalaman pengguna secara keseluruhan.

Hasil Pengukuran Dampak Penerapan *Signal Protocol* pada tabel 3 memberikan gambaran mengenai hasil pengukuran dampak penerapan *Signal Protocol*. Peningkatan waktu respons dan penggunaan sumber daya dapat dianggap sebagai *trade-off* yang wajar mengingat peningkatan keamanan yang diberikan oleh enkripsi *end-to-end*. Aplikasi *WallChat* tetap dapat memberikan pengalaman pengguna yang memuaskan sambil menjaga tingkat keamanan yang tinggi. Survei dan wawancara yang melibatkan 120 responden menunjukkan bahwa lebih dari 80% responden merespons positif terhadap implementasi enkripsi *end-to-end*. Mereka menyatakan bahwa mereka merasa lebih percaya terhadap keamanan pesan mereka setelah penerapan enkripsi *end-to-end*. Selain

itu, sekitar 75% responden menyatakan bahwa mereka merasa lebih aman dalam berbagi informasi sensitif melalui aplikasi setelah fitur keamanan ini diimplementasikan. Respons positif juga ditemukan dalam penilaian terhadap upaya Aplikasi *WallChat* dalam melindungi privasi pesan. Lebih dari 70% responden menyatakan bahwa upaya tersebut dinilai baik atau cukup baik. Adanya fitur keamanan baru ini juga memberikan dampak positif terhadap pengalaman pengguna, dengan sekitar 60% responden yang menyatakan bahwa fitur enkripsi *end-to-end* meningkatkan pengalaman pengguna mereka dalam menggunakan Aplikasi *WallChat.*

Sejalan dengan respons positif tersebut, sebagian besar pengguna tidak melaporkan perubahan signifikan dalam cara mereka menggunakan aplikasi setelah enkripsi *end-to-end* diimplementasikan. Meskipun demikian, sekitar 15% responden menyatakan bahwa mereka mengalami perubahan, yang umumnya terkait dengan kesadaran privasi dan keamanan yang lebih tinggi. Hal ini mencerminkan bahwa sebagian kecil pengguna mungkin membutuhkan penyesuaian atau adaptasi terkait dengan perubahan fitur keamanan. Tabel 4 dan 5 menampilkan hasil dari uji hipotesis, analisis varians (ANOVA), dan perhitungan rata-rata, median, serta deviasi standar. Secara konsisten, hasil ini memvalidasi temuan-temuan sebelumnya. Uji hipotesis menunjukkan bahwa perbedaan dalam waktu kirim dan terima pesan, serta penggunaan sumber daya, secara statistik signifikan. Kesimpulan analisis varian juga mengonfirmasi signifikansinya. Dengan demikian, keseluruhan hasil dan pembahasan menunjukkan bahwa implementasi *Signal Protocol* pada Aplikasi *WallChat* memberikan perbaikan yang substansial terhadap keamanan pesan tanpa mengorbankan kinerja secara signifikan. Pengguna aplikasi merespons positif terhadap perubahan ini, dan dampak terhadap penggunaan sumber daya tetap dalam batas yang dapat diterima. Oleh karena itu, implementasi *Signal Protocol* dapat dianggap berhasil dan memberikan manfaat nyata bagi pengguna Aplikasi *WallChat*.

KESIMPULAN

Implementasi *Signal Protocol* pada Aplikasi *WallChat* terbukti berhasil dalam meningkatkan tingkat keamanan pesan melalui penerapan enkripsi *end-to-end*. Melalui analisis keamanan, ditemukan bahwa mekanisme enkripsi yang digunakan sesuai dengan standar keamanan industri, dan tidak ada celah keamanan yang signifikan yang dapat diekspos. Uji penetrasi turut memvalidasi keamanan aplikasi dengan tidak adanya temuan yang mencemaskan. Secara keseluruhan, Aplikasi *WallChat* dapat dianggap memenuhi atau bahkan melebihi standar keamanan seperti ISO/IEC 27001. Dari perspektif kinerja, hasil pengukuran menunjukkan adanya peningkatan waktu respons dalam pengiriman dan penerimaan pesan setelah penerapan Signal Protocol. Meskipun peningkatan tersebut tidak mencapai tingkat signifikan, namun dapat dirasakan oleh pengguna Aplikasi *WallChat*. Peningkatan penggunaan sumber daya seperti CPU dan memori juga tercatat, namun masih berada dalam batas yang dapat diterima, tidak signifikan mengganggu pengalaman pengguna secara keseluruhan.

Tinjauan lanjutan melalui survei dan wawancara dengan pengguna aplikasi memberikan perspektif positif tambahan. Sebagian besar responden menyatakan peningkatan kepercayaan

terhadap keamanan pesan setelah implementasi enkripsi *end-to-end*. Lebih dari 75% responden merasa lebih aman dalam berbagi informasi sensitif melalui aplikasi, sementara sekitar 70% memberikan penilaian baik atau cukup baik terhadap upaya Aplikasi *WallChat* dalam melindungi privasi pesan. Adanya fitur keamanan baru ini juga dianggap memberikan dampak positif terhadap pengalaman pengguna.

Hasil dari uji hipotesis, analisis varians, serta perhitungan rata-rata, median, dan deviasi standar konsisten dalam menunjukkan signifikansi perbedaan kinerja sebelum dan setelah implementasi *Signal Protocol*. Perbedaan dalam waktu pengiriman dan penerimaan pesan, serta penggunaan sumber daya, secara statistik signifikan menurut uji hipotesis dan analisis varians. Keseluruhan, implementasi Signal Protocol pada Aplikasi *WallChat* dapat dianggap berhasil karena memberikan perbaikan yang substansial terhadap keamanan pesan.

Dampak terhadap penggunaan sumber daya tetap dalam batas yang dapat diterima, dan respons positif dari pengguna menegaskan bahwa langkah ini diarahkan pada peningkatan pengalaman pengguna. Keseluruhan, implementasi Signal Protocol pada Aplikasi *WallChat* bukan hanya mencapai tujuan keamanan yang ditetapkan, tetapi juga membuktikan sebagai langkah strategis yang berhasil menggabungkan keamanan yang ditingkatkan dengan kenyamanan pengguna dan fungsionalitas optimal. Keberhasilan ini memberikan kontribusi positif terhadap reputasi dan kepercayaan pengguna terhadap aplikasi.

DAFTAR PUSTAKA

Basem, O., Ullah, A., & Hassen, H. R. (2022). Stick: an *end-to-end* encryption protocol tailored for social network platforms. *IEEE Transactions on Dependable and Secure Computing*, *20*(2), 1258-1269. DOI: https://doi.org/10.1109/TDSC.2022.3152256.

Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J., & Milner, K. (2018, October). On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1802-1819). DOI: https://doi.org/10.1145/3243734.3243747.

Ermoshina, K., & Musiani, F. (2019). "Standardising by running code": the *Signal Protocol* and de facto standardisation in *end-to-end* encrypted messaging. *Internet Histories*, *3*(3-4), 343-363. DOI: https://doi.org/10.1080/24701475.2019.1654697.

Ermoshina, K., Musiani, F., & Halpin, H. (2016). *End-to-end* encrypted messaging protocols: An overview. In *Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings 3* (pp. 244-254). Springer International Publishing.

Hale, B., & Komlo, C. (2022). On *end-to-end* encryption. *Cryptology ePrint Archive*.

Isobe, T., & Ito, R. (2021). Security analysis of *end-to-end* encryption for zoom meetings. *IEEE access*, *9*, 90677-90689. DOI: https://doi.org/10.1109/ACCESS.2021.3091722.

Mahendra, G. S., Wali, M., Idwan, H., Listartha, I. M. E., Yuliastuti, G. E., Sasongko, D., Saskara, A., & Jude, G. A. (2022). *Keamanan Komputer*. PT. Galiono Digdaya Kawthar.

Mashru, D., Mangipudi, G. M., Swamy, H., Halangali, S., & Sushma, E. (2023, January). A Decentralised Instant Messaging Application with *End-to-end* Encryption. In *2023 20th Learning and Technology Conference (L&T)* (pp. 48-53). IEEE. DOI: https://doi.org/10.1109/LT58159.2023.10092319.

Paulus, S., Pohlmann, N., Reimer, H., Castiglione, A., Cattaneo, G., De Santis, A., ... & Ferraro Petrillo, U. (2006). SPEECH: Secure personal *end-to-end* communication with handheld. In *ISSE 2006—Securing Electronic Busines Processes: Highlights of the Information Security Solutions Europe 2006 Conference* (pp. 287-297). Vieweg.

Prabhune, S., & Sharma, S. (2021, December). *End-to-end* Encryption for Chat App with Dynamic Encryption Key. In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1361-1366). IEEE. DOI: https://doi.org/10.1109/ICAC3N53548.2021.9725597.

Melo, T., Barros, A., Antunes, M., & Frazão, L. (2021, June). An *end-to-end* cryptography based real-time chat. In *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE. DOI: https://doi.org/10.23919/CISTI52073.2021.9476399.

Rösler, P., Mainka, C., & Schwenk, J. (2018, April). More is less: On the *end-to-end* security of group chats in signal, whatsapp, and threema. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 415-429). IEEE. DOI: https://doi.org/10.1109/EuroSP.2018.00036.

Sabah, N., Kadhim, J. M., & Dhannoon, B. N. (2017). Developing an *end-to-end* secure chat application. *Int. J. Comput. Sci. Netw. Secur*, *17*(11), 108-113.

Schillinger, F., & Schindelhauer, C. (2019). *End-to-end* encryption schemes for online social networks. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 12th International Conference, SpaCCS 2019, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12* (pp. 133-146). Springer International Publishing.

Singh, R., Chauhan, A. N. S., & Tewari, H. (2022, June). Blockchain-enabled *end-to-end* encryption for instant messaging applications. In *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 501-506). IEEE. DOI: https://doi.org/10.1109/WoWMoM54355.2022.00078.

Wijayanto, G., *et al* (2022). *Metode Riset Berbasis Digital: Penelitian pasca Pandemi*. Medan: Media Sains Indonesia.