Kekuatan Enkripsi End-to-End: Kajian Literatur Mengenai Kerahasiaan Komunikasi Digital dalam Aplikasi Pesan Instan

Yeni Sri Maharani [1], ***Sausan Trisdiatin*** [2], ***Muhammad Rafli Ihsanuddin*** [3], ***Fayruz Rahma*** [4]
[1] *Jurusan Informatika, Universitas Islam Indonesia*, Sleman. Email: 21523262@students.uii.ac.id
[2] *Jurusan Informatika, Universitas Islam Indonesia*, Sleman. Email: 21523052@students.uii.ac.id
[3] *Jurusan Informatika, Universitas Islam Indonesia*, Sleman. Email: 21523132@students.uii.ac.id
[4] *Jurusan Informatika, Universitas Islam Indonesia*, Sleman. Email: fayruz.rahma@uii.ac.id

Abstract

Information and communication technology development has fundamentally changed the landscape of human communication, especially through instant messaging applications. However, concerns about privacy and security in digital communications are increasing. To solve this problem, end-to-end encryption has emerged as a powerful solution for maintaining the confidentiality of messages in digital communications. This scientific paper aims to discuss the strength of end-to-end encryption in instant messaging applications as an effective method for maintaining confidentiality in digital communications. With the increasing use of instant messaging applications, the need for privacy protection has become even more important. End-to-end encryption provides added security by ensuring only the sender and recipient can access the message content.

Keywords: encryption, end-to-end, privacy

Abstrak

Perkembangan teknologi informasi dan komunikasi telah mengubah lanskap komunikasi manusia secara fundamental, terutama melalui aplikasi pesan instan. Namun, kekhawatiran akan privasi dan keamanan dalam komunikasi digital semakin meningkat. Untuk mengatasi masalah ini, enkripsi end-to-end telah muncul sebagai solusi yang kuat untuk menjaga kerahasiaan pesan dalam komunikasi digital. Tujuan karya ilmiah ini adalah untuk membahas kekuatan enkripsi end-to-end dalam aplikasi pesan instan sebagai metode efektif untuk mempertahankan kerahasiaan dalam komunikasi digital. Dengan meningkatnya penggunaan aplikasi pesan instan, kebutuhan akan perlindungan privasi semakin penting. Enkripsi end-to-end memberikan keamanan tambahan dengan memastikan bahwa hanya pengirim dan penerima yang dapat mengakses konten pesan.

Kata Kunci: enkripsi, end-to-end, privasi

1. Pendahuluan

Dalam era digital yang semakin maju, penggunaan internet sebagai sarana komunikasi telah menjadi sangat penting dalam kehidupan pribadi maupun bisnis. Namun, dengan meningkatnya penggunaan internet, muncul ancaman terhadap keamanan dan privasi komunikasi *online* (Blaise, Awodele, & Yewande, 2021). Oleh karena itu, diperlukan solusi yang efektif untuk melindungi kerahasiaan dalam komunikasi digital.

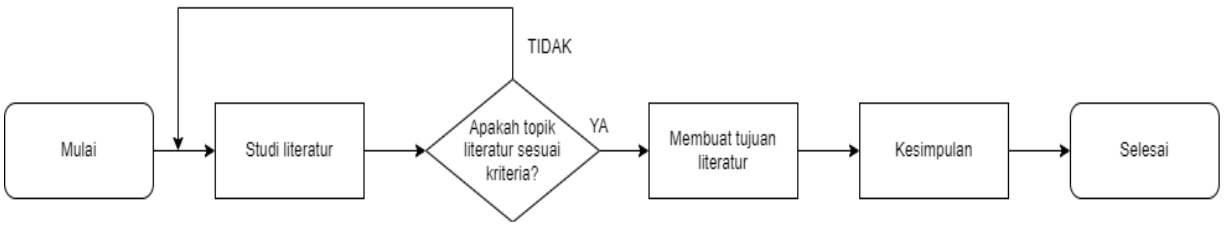
Salah satu solusi yang banyak digunakan untuk menjaga kerahasiaan komunikasi adalah enkripsi *end-to-end*. Enkripsi *end-to-end* adalah proses pertukaran data yang aman dari pengirim ke penerima, dengan mengenkripsi seluruh konten selama transmisi sehingga tidak dapat diakses atau dimodifikasi oleh pihak ketiga. Beberapa algoritma kriptografi digunakan untuk tujuan ini. Komponen-komponen seperti identitas pengguna, protokol pertukaran kunci, dan implementasi yang aman bekerja bersama-sama untuk memberikan keamanan yang terbaik kepada pengguna akhir (Blaise, Awodele, & Yewande, 2021).

Dalam konteks aplikasi pesan instan, keamanan dan privasi menjadi sangat penting (Ali & Alsaad, 2020). Jaringan sosial *online* dan aplikasi pesan instan seperti WhatsApp, Telegram, dan Facebook Messenger telah mengadopsi enkripsi *end-to-end* untuk melindungi komunikasi pengguna (S., 2022). Namun, dalam penggunaan sehari-hari, masih terdapat beberapa masalah keamanan dan privasi yang perlu diatasi guna melindungi informasi pribadi pengguna dan data yang dibagikan melalui aplikasi pesan instan ini (Ali & Alsaad, 2020).

Dalam mengimplementasikan enkripsi *end-to-end* dalam aplikasi pesan instan, penting untuk mempertimbangkan potensi dan batasan yang ada. Meskipun enkripsi *end-to-end* memberikan perlindungan yang kuat terhadap kerahasiaan pesan dan privasi pengguna, aspek-aspek lain seperti keamanan perangkat, pengelolaan kunci enkripsi, dan verifikasi identitas penerima pesan juga penting untuk diperhatikan. Selain itu, pengguna aplikasi pesan instan juga harus memperhatikan kebijakan privasi dan pernyataan keamanan dari penyedia layanan, serta terus memperbarui aplikasi mereka untuk mengatasi kerentanan keamanan yang mungkin muncul (Blaise, Awodele, & Yewande, 2021). Dengan memahami potensi dan batasan enkripsi *end-to-end*, serta melibatkan pengguna, pengembang, dan penyedia layanan, dapat dikembangkan teknologi keamanan dan privasi yang lebih kuat dan efektif di masa depan.

2. Metode

Dalam penelitian ini, diterapkan metodologi terstruktur. Digunakan pendekatan *Systematic Literature Review* dengan tujuan menjawab pertanyaan penelitian. Proses ini melibatkan tiga tahapan utama: identifikasi, penilaian, dan interpretasi topik penelitian dari temuan yang ada. Pendekatan ini dipilih karena menerapkan pendekatan yang sistematis, sehingga proses *literature review* dapat terhindar dari pemahaman subyektif. Proses pengerjaan seperti diperlihatkan pada Gambar 1.



Gambar 1: Diagram Alir Penelitian

2.1. Pertanyaan Penelitian

Pertanyaan penelitian digunakan sebagai panduan dalam mencari artikel dan jurnal terkait. Berikut merupakan beberapa pertanyaan yang diajukan sebagai acuan dalam pencarian literatur terkait:

1) Bagaimana mekanisme enkripsi *end-to-end* bekerja dalam aplikasi pesan instan?
2) Bagaimana kekuatan keamanan enkripsi *end-to-end* dalam melindungi kerahasiaan komunikasi digital dalam aplikasi pesan instan?
3) Bagaimana efektivitas penggunaan enkripsi *end-to- end* dalam melindungi komunikasi digital dalam konteks privasi pengguna dan perlindungan data?

2.2. Pengumpulan Literatur

Untuk mengumpulkan literatur, dilakukan pencarian terhadap sejumlah sumber yang relevan dengan topik penelitian, yaitu membahas tentang enkripsi *end-to-end*. Proses pencarian literatur dilakukan melalui *Google Scholar* dengan menggunakan kata kunci seperti: enkripsi *end-to- end*, cara kerja *end-to-end*, privasi, dan *instant message*.

2.3. Pemilihan Literatur

Pemilihan literatur dilakukan berdasarkan kriteria yang telah ditentukan. Sebanyak tujuh literatur dipilih berdasarkan kriteria seperti kesamaan topik yang membahas mekanisme enkripsi *end-to-end*, web dengan tahun penerbitan setidaknya tahun 2020, dan literatur dengan tahun penerbitan setidaknya tahun 2019. Kemudian, tujuh literatur tersebut dikelompokkan berdasarkan mekanisme, kekuatan, dan

efektivitas enkripsi *end-to-end*. Literatur yang relevan diorganisasikan dan dihitung berdasarkan kata kunci yang telah dicari, sebagaimana terdokumentasikan dalam Tabel 1.

Tabel 1: Jumlah Literatur Berdasarkan Kata Kunci

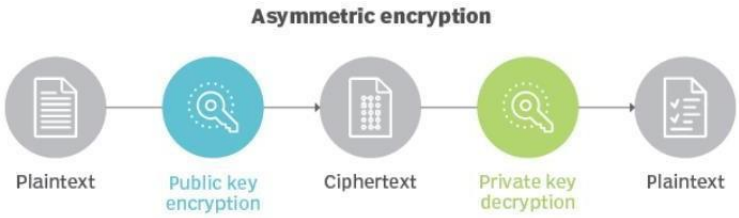
Kata Kunci	Literatur	Jumlah
Enkripsi *end-to-end*	(Blaise, Awodele, & Yewande, 2021) (Ali & Alsaad, 2020) (S., 2022) (Lutkevich, 2021) (Carpay & Lontorfos, 2019) (Rizal, 2021) (Simplilearn, 2021)	7
Cara kerja enkripsi	(Blaise, Awodele, & Yewande, 2021) (S., 2022) (Lutkevich, 2021) (Rizal, 2021) (Simplilearn, 2021)	5
Privasi	(Carpay & Lontorfos, 2019) (Simplilearn, 2021)	2
Pesan enkripsi	(Blaise, Awodele, & Yewande, 2021) (Simplilearn, 2021)	2

Berdasarkan data yang tertera dalam Tabel 1, dapat diamati bahwa literatur dari Simplilearn (2021) berhasil ditemukan dalam pencarian untuk semua kata kunci yang telah dicari.

3. Hasil dan Pembahasan

Hasil dan Pembahasan berisi data hasil tujuh literatur yang telah dikaji untuk dijadikan sebagai referensi penulis dalam menjawab pertanyaan ilmiah dan mencari tahu mengenai mekanisme enkripsi *end-to-end* bekerja dalam aplikasi pesan instan. Berdasarkan hasil analisis literatur, ditemukan bahwa enkripsi *end-to-end* mampu mencegah penyadapan pesan oleh pihak ketiga, menjaga privasi pengguna, dan mencegah penyalahgunaan data komunikasi. Enkripsi asimetris adalah salah satu teknik yang digunakan dalam enkripsi *end-to-end* untuk mencapai tingkat keamanan yang tinggi.

Tahapan kriptografi asimetris pada aplikasi pesan instan tertuang pada Gambar 2. Dalam enkripsi asimetris, pengguna memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi. Kunci publik digunakan untuk mengenkripsi pesan sebelum dikirimkan, sedangkan kunci pribadi digunakan untuk mendekripsinya saat pesan diterima. Keistimewaan dari enkripsi asimetris adalah bahwa siapa pun dapat memiliki kunci publik, yang dapat digunakan untuk mengirimkan pesan terenkripsi kepada pemilik kunci pribadi tanpa perlu mengungkapkan kunci pribadi itu sendiri. Ini menjadikan enkripsi asimetris sangat cocok untuk aplikasi keamanan data yang melibatkan komunikasi jarak jauh, seperti pesan instan.



Gambar 2: Enkripsi Asimetris
(Lutkevich, 2021)

Selain itu, ditemukan bahwa enkripsi *end-to-end* memiliki kekuatan keamanan seperti enkripsi *hybrid*, perlindungan dari penyadapan data, penghindaran pengiriman kunci, perlindungan terhadap perusakan pesan dan integritas data, serta kepatuhan terhadap peraturan perlindungan data. Penggunaan enkripsi *end-to-end* terbukti efektif dalam melindungi komunikasi digital, kerahasiaan pesan, perlindungan data, dan privasi pengguna dalam aplikasi pesan instan. Namun, penting juga untuk memperhatikan faktor lain seperti keamanan perangkat, identifikasi pengguna, pengelolaan kunci, verifikasi identitas, pembaruan keamanan, *transparansi* dan *auditabilitas*, serta edukasi pengguna guna meningkatkan keamanan komunikasi digital secara menyeluruh. Enkripsi asimetris menjadi salah satu pilar penting dalam rangkaian strategi keamanan ini, yang membantu memastikan pesan yang dikirimkan dan diterima tetap aman dan terlindungi.

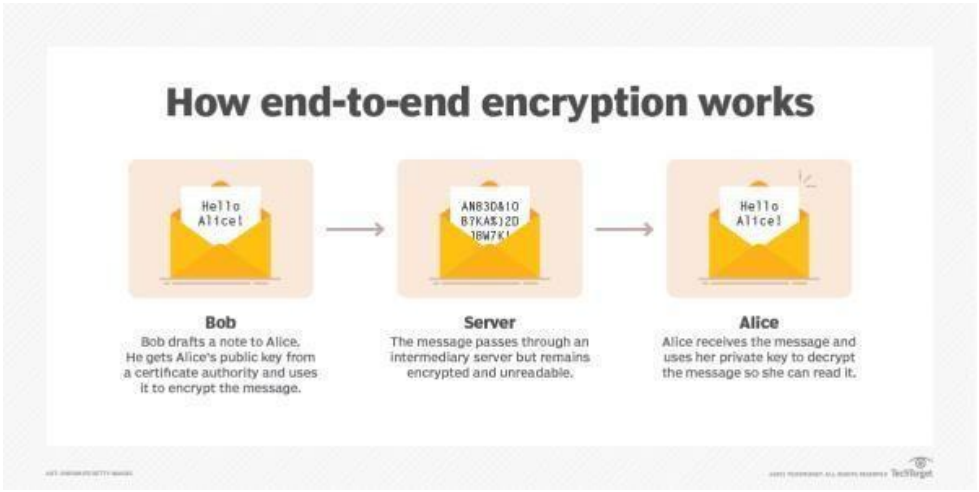
3.1. Mekanisme Enkripsi End-to-End dalam Aplikasi Pesan Instan

Dalam upaya menjawab pertanyaan mengenai mekanisme enkripsi *end-to-end* dalam aplikasi pesan instan, telah dilakukan analisis terhadap tujuh literatur yang relevan. Hasil analisis tersebut menunjukkan bahwa mekanisme enkripsi *end-to-end* dalam aplikasi pesan instan menggunakan kriptografi asimetris, simetris, maupun enkripsi *hybrid* dengan pasangan kunci publik dan kunci privat (S., 2022). Pada proses pengiriman pesan, kunci publik berfungsi untuk melakukan proses enkripsi terhadap pesan, sedangkan kunci privat digunakan untuk melakukan proses dekripsi terhadap pesan tersebut (Lutkevich, 2021).

Dalam proses ini, ketika pengguna mengirim pesan melalui aplikasi pesan instan, pesan tersebut dienkripsi menggunakan kunci publik penerima. Setelah melalui server aplikasi, pesan yang telah dienkripsi diterima dan kemudian didekripsi dengan kunci privat yang tersimpan di perangkat penerima. Hanya perangkat penerima yang memiliki kunci privat yang dapat mendekripsi dan memahami pesan dalam bentuk aslinya (Carpay & Lontorfos, 2019). Mekanisme enkripsi *end-to-end* ini secara efektif mencegah penyadapan pesan oleh pihak ketiga, termasuk penyedia layanan komunikasi dan penyerang yang mungkin ada di dalam jaringan (Rizal, 2021).

Kunci-kunci enkripsi yang menjamin keamanan pesan ini disimpan di perangkat yang saling berkomunikasi. Dengan sistem enkripsi *end-to-end* yang menggunakan kunci publik, server perantara, seperti ISP atau perusahaan lain, tidak mampu untuk menyadap isi pesan. Hal ini dikarenakan oleh mereka yang mungkin memiliki kunci publik, tapi mereka tidak memiliki kunci privat yang diperlukan untuk mendekripsi pesan (Lutkevich, 2021).

Kunci publik ini, untuk memastikan keotentikannya, biasanya disertai dengan sertifikat yang telah divalidasi oleh lembaga otoritas sertifikat (CA). Karena kunci publik CA sudah dikenal luas dan dipercayai, maka sertifikat yang dikeluarkan dan ditandatangani oleh CA dianggap otentik. Ini membantu memastikan bahwa kunci publik yang digunakan memang asli dan terkait dengan identitas yang benar. Dengan demikian, mekanisme enkripsi *end-to-end* memastikan bahwa pesan yang dikirim antar pengguna dalam aplikasi pesan instan dilindungi dengan ketat dari potensi ancaman penyadapan (Lutkevich, 2021). Tahapan kerja enkripsi *end-to-end* tersebut tertuang pada Gambar 3.



Gambar 3: Prosedur enkripsi end-to-end
(Lutkevich, 2021)

Dengan menggunakan enkripsi *end-to-end*, pesan yang dikirim melalui aplikasi pesan instan tetap terenkripsi selama perpindahannya dari perangkat pengirim ke perangkat penerima (Rizal, 2021). Dalam mekanisme ini, server perantara (seperti server WhatsApp) tidak memiliki kemampuan untuk membaca atau memahami isi pesan sehingga menjaga privasi pengguna dan mencegah pihak ketiga mengintip komunikasi tersebut (S., 2022).

3.2. Keamanan Enkripsi End-to-End dalam Aplikasi Pesan Instan

Analisis literatur juga bertujuan untuk menjawab pertanyaan mengenai keamanan enkripsi *end-to-end* dalam melindungi kerahasiaan komunikasi digital dalam aplikasi pesan instan. Berdasarkan analisis tersebut, ditemukan beberapa keamanan yang melibatkan enkripsi *end-to-end*:

1) Enkripsi *Hybrid*: Enkripsi ini digunakan dalam beberapa aplikasi pesan instan, merupakan pendekatan yang menggabungkan kekuatan enkripsi simetris dan asimetris. Dalam enkripsi *hybrid*, pesan pertama-tama dienkripsi menggunakan kunci simetris yang dihasilkan secara acak, yang efisien dalam mengenkripsi data. Selanjutnya, kunci simetris ini dienkripsi lagi menggunakan kunci publik penerima pesan, yang merupakan kunci asimetris. Pendekatan ini meningkatkan efektivitas enkripsi karena kunci simetris digunakan hanya untuk pesan tertentu, sementara kunci asimetris menjaga keamanan kunci simetris. Dengan demikian, enkripsi *hybrid* memberikan tingkat keamanan yang kuat dalam komunikasi digital, menjaga privasi pengguna, dan mencegah penyadapan pesan oleh pihak ketiga (Blaise, Awodele, & Yewande, 2021).
2) Perlindungan dari Penyadapan Data: Enkripsi *end-to-end* memastikan bahwa pesan yang dikirim melalui jaringan tidak dapat dibaca oleh pihak yang tidak berwenang. Hal ini melindungi komunikasi digital dari serangan penyadapan data dan menjaga kerahasiaan pesan (Simplilearn, 2021).
3) Terbatasnya Akses Dekripsi Pesan: Pada Enkripsi *end-to-end* ini hanya titik awal dan titik akhir yaitu pengirim dan penerima yang diperbolehkan untuk mendekripsi dan membaca pesan (Lutkevich, 2021).
4) Perlindungan Terhadap Perusakan Pesan dan Integritas Data: Enkripsi *end-to-end* tidak hanya melindungi kerahasiaan pesan, tetapi juga memastikan integritas data. Pesan yang dienkripsi dengan enkripsi *end-to-end* dapat dideteksi jika terjadi perubahan atau perusakan saat dalam perjalanan, sehingga memastikan bahwa pesan tidak diubah oleh pihak yang tidak berwenang (Simplilearn, 2021).
5) Kepatuhan Terhadap Peraturan Perlindungan Data: Enkripsi *end-to-end* mematuhi peraturan tentang penanganan data pribadi yang sensitif. Dalam beberapa yurisdiksi, seperti *General Data Protection Regulation* (GDPR) di Uni Eropa, enkripsi *end-to-end* dianggap sebagai langkah yang kuat untuk melindungi privasi pengguna dan perlindungan data (S., 2022).

Melalui keamanan-keamanan ini, enkripsi *end-to-end* memberikan keamanan yang diperlukan untuk melindungi komunikasi digital dalam aplikasi pesan instan.

3.3. Efektivitas Penggunaan Enkripsi End-to-End dalam Melindungi Komunikasi Digital dalam Konteks Privasi Pengguna dan Perlindungan Data

Analisis literatur juga melibatkan pertanyaan mengenai efektivitas penggunaan enkripsi *end-to-end* dalam melindungi komunikasi digital dalam konteks privasi pengguna dan perlindungan data. Berdasarkan analisis tersebut, penggunaan enkripsi *end-to-end* terbukti sangat efektif dalam melindungi komunikasi digital dalam aplikasi pesan instan. Beberapa efektivitas penggunaan enkripsi *end-to-end* yang diidentifikasi adalah sebagai berikut (Simplilearn, 2021):

1) Kerahasiaan pesan pada enkripsi *end-to-end* memastikan bahwa pesan hanya dapat dibaca oleh pengirim dan penerima yang dituju. Informasi sensitif dalam pesan tetap terlindungi dari akses oleh penyedia layanan atau pihak ketiga yang mungkin memiliki akses ke data komunikasi.
2) Perlindungan data dengan menggunakan enkripsi *end-to-end*, data komunikasi yang dikirimkan melalui jaringan tetap terlindungi dari potensi serangan dan intersepsi oleh pihak yang tidak berwenang. Hal ini mengurangi risiko penyalahgunaan data dan kebocoran informasi.
3) Privasi pengguna disebabkan oleh enkripsi *end-to-end* yang memainkan peran penting dalam menjaga privasi pengguna. Pesan yang dienkripsi tidak dapat dibaca oleh penyedia layanan atau pihak ketiga lainnya, sehingga mengurangi kemungkinan penggunaan data pribadi untuk tujuan yang tidak diinginkan.

Penggunaan enkripsi *end-to-end* dalam aplikasi pesan instan memberikan perlindungan yang kuat terhadap komunikasi digital, memastikan privasi pengguna, dan menjaga keamanan data yang dikirim melalui platform tersebut. Namun, penting juga untuk menyadari bahwa enkripsi *end-to-end* hanyalah salah satu aspek dari keamanan komunikasi digital. Selain enkripsi *end-to-end*, terdapat faktor lain yang dapat mempengaruhi keamanan komunikasi digital, seperti ancaman *malware*, serangan *phishing*, dan praktik keamanan yang buruk dari pengguna sendiri. Oleh karena itu, penting bagi pengguna untuk tetap waspada dan mengambil tindakan pencegahan yang sesuai untuk menjaga keamanan komunikasi digital mereka.

Dalam rangka melindungi komunikasi digital dengan efektif, kombinasi dari enkripsi *end-to-end* dan praktik keamanan yang baik harus diimplementasikan. Ini melibatkan kombinasi teknologi yang kuat, seperti penggunaan enkripsi *end-to-end*, kebijakan keamanan yang ketat, dan pembaruan sistem yang teratur. Selain itu, kesadaran pengguna tentang praktik keamanan yang tepat juga penting, seperti menggunakan kata sandi yang kuat, tidak membagikan informasi pribadi dengan sembarangan, dan tidak mengklik tautan yang mencurigakan.

Dengan menggabungkan enkripsi *end-to-end* dan praktik keamanan yang baik, pengguna aplikasi pesan instan dapat meningkatkan privasi mereka, melindungi data pribadi, dan memastikan komunikasi digital yang aman. Selain itu, pengembang aplikasi pesan instan juga memiliki peran penting dalam meningkatkan keamanan aplikasi mereka dengan memperbarui sistem, menangani kerentanan keamanan, dan meningkatkan transparansi terkait praktik keamanan yang diterapkan. Dengan kerja sama antara pengguna dan pengembang, kita dapat menciptakan ekosistem komunikasi digital yang lebih aman dan terlindungi di masa yang akan datang.

4. Kesimpulan

Berdasarkan analisis literatur, enkripsi *end-to-end* terbukti sangat efektif dalam melindungi privasi dan data pengguna dalam komunikasi digital, khususnya dalam konteks aplikasi pesan instan. Keuntungannya meliputi kerahasiaan pesan dan perlindungan data, memberikan lapisan keamanan yang kuat. Namun, penting untuk diingat bahwa enkripsi *end-to-end* hanya sebagian dari upaya keamanan yang diperlukan. Upaya tambahan seperti menjaga keamanan perangkat, identifikasi pengguna yang kuat, pengelolaan kunci enkripsi yang aman, serta pembaruan rutin aplikasi dan pemahaman terhadap kebijakan privasi penyedia layanan juga penting untuk memastikan komunikasi digital yang aman dan privasi pengguna terjaga.

Selain itu, pengembang aplikasi pesan instan juga harus aktif dalam meningkatkan keamanan aplikasi mereka dengan pembaruan sistem, menangani kerentanan keamanan, dan melibatkan auditor independen. Dengan memperhatikan aspek-aspek keamanan ini, pengguna aplikasi pesan instan dapat memastikan privasi, melindungi data pribadi, dan menjaga komunikasi digital yang aman di era digital yang terus berkembang ini. Langkah-langkah ini menjadi semakin penting dalam menghadapi ancaman keamanan yang terus muncul.

Referensi

Ali, R. M., & Alsaad, S. N. (2020). Instant messaging security and privacy secure instant messenger design. *3rd International Conference on Sustainable Engineering Techniques (ICSET 2020).* Baghdad: IOP Conference Series. doi:10.1088/1757-899X/881/1/012117

Blaise, O. O., Awodele, O., & Yewande, O. (2021, April). An Understanding and Perspectives of End-To-End Encryption. *International Research Journal of Engineering and Technology (IRJET), 8*(4), 1086-1094. Retrieved from https://www.irjet.net/archives/V8/i4/IRJET-V8I4210.pdf

Carpay, T., & Lontorfos, P. (2019, Februari 5). *WhatsApp End-to-End Encryption: Are Our Messages Private?* Retrieved from SNE Master Research Projects 2018-2019: https://rp.os3.nl/2018-2019/p25/report.pdf

Lutkevich, B. (2021, Juni). *end-to-end encryption (E2EE).* Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE

Rizal, A. (2021, Oktober 19). *Apa itu dan Bagaimana Cara Kerja Enkripsi End-to-end WhatsApp?* Retrieved from InfoKomputer: https://infokomputer.grid.id/read/122949582/apa-itu-dan-bagaimana-cara-kerja-enkripsi-end-to-end-whatsapp

S., A. (2022, Juni 28). *End-to-End Encryption and its Benefits for your Messenger App*. Retrieved from Quickblox: https://quickblox.com/blog/end-to-end-encryption-and-its-benefits-for-your-messenger-app/

Simplilearn. (2021, November 18). *What is End-to-End Encryption? How It Works, and Why We Need It.* Retrieved from Simplilearn: https://www.simplilearn.com/what-is-end-to-end-encryption-article