IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATTING MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING

SKRIPSI

Oleh:

CHARLES
NIM. 221110156
CECILIA ONGSO
NIM. 221111729
JASON WILBERT
NIM. 221111572

PROGRAM STUDI S-1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
UNIVERSITAS MIKROSKIL
MEDAN
2026

IMPLEMENTATION AND EVALUATION OF CHATTING SECURITY PROTOCOLS USING CHACHA20 AND ECDHE TO PREVENT EAVESDROPPING

UNDERGRADUATE THESIS

By:

CHARLES
ID NUMBER. 221110156
CECILIA ONGSO
ID NUMBER. 221111729
JASON WILBERT
ID NUMBER. 221111572

UNDERGRADUATE PROGRAM OF S-1 INFORMATICS ENGINEERING
FACULTY OF INFORMATICS
UNIVERSITAS MIKROSKIL
MEDAN
2026

LEMBARAN PENGESAHAN

IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATTING MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING

SKRIPSI

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Sarjana
Program Studi S-1 Teknik Informatika

Oleh:

CHARLES
NIM. 221110156
CECILIA ONGSO
NIM. 221111729
JASON WILBERT
NIM. 221111572

Disetujui Oleh:

Dosen Pembimbing,

Dosen Pembimbing I,	Dosen Pembimbing II,
Syanti Irviantina, S.Kom., M.Kom.	Darwin, S.Kom., M.Kom.

Medan, 22 Juli 2026
Diketahui dan Disahkan Oleh:

Ketua Program Studi
S-1 Teknik Informatika,

Carles Juliandy, S.Kom., M Kom

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Cecilia Ongso
NIM : 221111729

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:

Judul Skripsi : Implementasi dan Evaluasi Protokol Keamanan Chatting Menggunakan ChaCha20 dan ECDHE untuk Pencegahan Eavesdropping
Tempat Penelitian : -
Alamat Tempat Penelitian : -
No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 6 Juli 2026
Saya yang membuat pernyataan,

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Charles
NIM : 221110156

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:

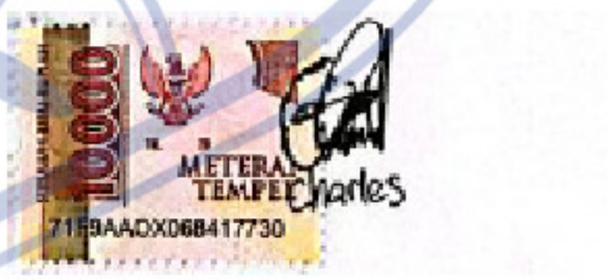
Judul Skripsi : Implementasi dan Evaluasi Protokol Keamanan Chatting Menggunakan ChaCha20 dan ECDHE untuk Pencegahan Eavesdropping
Tempat Penelitian : -
Alamat Tempat Penelitian : -
No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 6 Juli 2026
Saya yang membuat pernyataan,



HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Jason Wilbert
NIM : 221111572

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:

Judul Skripsi : Implementasi dan Evaluasi Protokol Keamanan Chatting Menggunakan ChaCha20 dan ECDHE untuk Pencegahan Eavesdropping
Tempat Penelitian : -
Alamat Tempat Penelitian : -
No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 6 Juli 2026
Saya yang membuat pernyataan,

Jason Wilbert

IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATTING MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING

Abstrak

Aplikasi chatting berbasis web menghadapi tantangan serius terkait keamanan komunikasi, yaitu serangan eavesdropping. Untuk melindungi kerahasiaan komunikasi, berbagai aplikasi chatting modern telah menerapkan konsep End-to-End Encryption (E2EE), di mana proses enkripsi dan dekripsi pesan dilakukan langsung pada sisi pengirim dan penerima. Pada penelitian ini, akan dievaluasi efektivitas kombinasi algoritma ChaCha20 dan Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) dalam mencegah serangan eavesdropping pada skenario komunikasi chatting berbasis web. Metode yang digunakan dalam penelitian ini adalah metode Waterfall. Hasil evaluasi menunjukkan bahwa metode ChaCha20 dapat diterapkan secara praktikal dalam aplikasi chatting karena memilik waktu eksekusi yang cepat. Selain itu, metode ECDHE juga mampu mendeteksi adanya perubahan baik terhadap nilai kunci publik ataupun nilai hash dari user penerima, sehingga proses komunikasi akan langsung dihentikan apabila terdeteksi adanya perubahan data tersebut. Percobaan dekripsi dengan menyadap data kunci publik dan beberapa ciphertext juga akan sulit berhasil, karena tidak adanya korelasi antara beberapa ciphertext yang dihasilkan tersebut, walaupun ciphertext dihasilkan dengan menggunakan pesan dan shared key yang sama. Dari hasil pengujian juga terbukti bahwa aplikasi chatting dengan menggunakan metode ChaCha20 dan ECDHE mampu melakukan pencegahan terhadap eavesdropping.

Kata Kunci: *chatting, protokol keamanan, metode ChaCha20, metode ECDHE, eavesdropping*

Abstract

Web-based chat applications face a significant security challenge in the form of eavesdropping attacks. To protect communication confidentiality, many modern messaging applications implement End-to-End Encryption (E2EE), where message encryption and decryption are performed only on the sender's and receiver's devices. This study evaluates the effectiveness of combining the ChaCha20 algorithm and Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) in preventing eavesdropping in a web-based chat application. The research adopts the Waterfall development methodology. The evaluation results show that ChaCha20 is practical for chat applications due to its fast execution time. In addition, ECDHE can detect any modification to the recipient's public key or hash value, causing the communication process to terminate immediately if such changes are detected. Decryption attempts through intercepted public keys and ciphertexts are also unlikely to succeed because no correlation exists among the generated ciphertexts, even when they are produced from the same plaintext and shared key. The experimental results demonstrate that the integration of ChaCha20 and ECDHE effectively prevents eavesdropping attacks in web-based chat applications.

Keywords: *chatting, security protocol, ChaCha20 method, ECDHE method, eavesdropping*

KATA PENGANTAR

Ucapan syukur kepada Tuhan Yang Maha Esa, penulis ingin mengucapkan terima kasih atas berkat dan karunia-Nya yang telah memungkinkan penulis menyelesaikan Tugas Akhir ini dengan judul "**IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATTING MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING**".

Tugas Akhir ini disusun sebagai bagian dari persyaratan untuk meraih gelar Sarjana Strata Satu (S1) pada Program Studi Teknik Informatika Universitas Mikroskil Medan.

Dalam proses penulisan Tugas Akhir ini, penulis telah berupaya untuk mencapai hasil yang terbaik. Keberhasilan ini tidak lepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih kepada:

1. Ibu Syanti Irviantina, S.Kom., M.Kom., selaku Dosen Pembimbing I.
2. Bapak Darwin, S.Kom., M.Kom., selaku Dosen Pembimbing II.
3. Bapak Hardy, S.Kom., M.Sc., Ph.D., selaku Rektor Universitas Mikroskil Medan.
4. Bapak Sunaryo Winardi, S.Kom., M.T., selaku Dekan Fakultas Informatika Universitas Mikroskil Medan.
5. Bapak Carles Juliandy, S.Kom., M.Kom., selaku Ketua Program Studi S-1 Teknik Informatika Fakultas Informatika Universitas Mikroskil Medan.
6. Orang tua dan keluarga yang selalu memberikan doa, dukungan, motivasi pada penulis selama penyusunan Tugas Akhir.
7. Seluruh teman-teman seperjuangan yang telah membantu penulis dalam bentuk doa dan dukungan, serta pihak-pihak yang memberi masukan dalam Tugas Akhir.

Penulis menyadari Tugas Akhir ini tidak lepas dari kekurangan dan jauh dari kesempurnaan karena keterbatasan pengetahuan dan pengalaman penulis. Oleh karena itu, kritik dan saran dari pembaca sangat diharapkan agar Tugas Akhir ini dapat memberikan manfaat untuk pembaca dan bagi pihak-pihak yang membutuhkan.

Medan, 01 Juli 2026

Penulis,

Charles

Cecilia Ongso

Jason Wilbert

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL