UNIVERSITAS
GADJAH MADA
**COMPARATIVE ANALYSIS OF HANDSHAKE LATENCY: STANDARD TLS 1.3 VS. TLS 1.3 WITH ENCRYPTED CLIENTHELLO (ECH)**
Milenika Iqbal Khawarits, Dr. Mardhani Riasetiawan, SE Ak, MT
**Universitas Gadjah Mada, 2024 | Diunduh dari http://etd.repository.ugm.ac.id/**

# ABSTRACT

The rapid growth of computer networks has woven digital interactions into everyday life, heightening the demand for strong data security protocols to protect sensitive information from interception. While Transport Layer Security (TLS) 1.3 has advanced significantly, it still transmits metadata like the Server Name Indication (SNI) in plaintext, which poses privacy risks. To address this, the TLS working group introduced the Encrypted ClientHello (ECH) extension to mitigate such vulnerabilities. This study examines the impact of ECH on handshake latency, comparing standard TLS 1.3 with TLS 1.3 augmented by ECH, focusing on the balance between performance and enhanced privacy for secure communication.

The research employs a controlled testbed environment with client and server configurations optimized for precise data collection using Wireshark and other network tools. Each configuration, standard TLS 1.3 and TLS 1.3 with ECH, is tested with a series of 100 automated requests to capture handshake latency, resulting in a total of 200 queries. Comprehensive statistical analysis, including descriptive statistics, visualization, and inferential statistical tests, ensures the reliability of the performance comparison between the two configurations.

The results reveal that the implementation of ECH in TLS 1.3 introduces a minor increase in handshake latency, with TLS 1.3 with ECH averaging 7.38 ms compared to 6.81 ms for standard TLS 1.3. However, this difference is not statistically significant ($p = 0.5850$), and the effect size is small (rank-biserial correlation = -0.0448). The bootstrap confidence interval for the latency difference, calculated as [-0.5829, 0.5747], further indicates that the true latency difference is likely negligible. Despite this minimal latency impact, ECH provides enhanced privacy by encrypting sensitive handshake metadata, allowing network administrators and developers to prioritize user privacy without significantly affecting performance

UNIVERSITAS
GADJAH MADA
**COMPARATIVE ANALYSIS OF HANDSHAKE LATENCY: STANDARD TLS 1.3 VS. TLS 1.3 WITH ENCRYPTED CLIENTHELLO (ECH)**
Milenika Iqbal Khawarits, Dr. Mardhani Riasetiawan, SE Ak, MT
**Universitas Gadjah Mada, 2024 | Diunduh dari http://etd.repository.ugm.ac.id/**

# ABSTRAK

Pertumbuhan pesat jaringan komputer telah mengintegrasikan interaksi digital ke dalam kehidupan sehari-hari, meningkatkan kebutuhan akan protokol keamanan data yang kuat untuk melindungi informasi sensitif dari penyadapan. Meskipun Transport Layer Security (TLS) 1.3 telah mengalami kemajuan signifikan, protocol tersebut masih mengirimkan metadata seperti Server Name Indication (SNI) dalam plaintext, yang menimbulkan risiko privasi. Untuk mengatasi hal ini, kelompok kerja TLS memperkenalkan ekstensi Encrypted ClientHello (ECH) untuk mengurangi kerentanan tersebut. Studi ini meneliti dampak ECH pada latensi handshake, dengan membandingkan TLS 1.3 Standar dengan TLS 1.3 yang ditingkatkan oleh ECH, berfokus pada keseimbangan antara performa dan peningkatan privasi untuk komunikasi yang lebih aman.

Penelitian ini menggunakan testbed terkontrol dengan konfigurasi klien dan server yang dioptimalkan untuk pengumpulan data yang presisi menggunakan Wireshark dan alat jaringan lainnya. Setiap konfigurasi, baik TLS 1.3 Standar maupun TLS 1.3 dengan ECH, diuji dengan serangkaian 100 kueri otomatis untuk menangkap latensi handshake, menghasilkan total 200 kueri. Analisis statistik yang komprehensif, termasuk statistik deskriptif, visualisasi, dan uji statistik inferensial, mendukung validitas keakuratan perbandingan kinerja antara kedua konfigurasi tersebut.

Hasil penelitian menunjukkan bahwa implementasi ECH dalam TLS 1.3 memperkenalkan peningkatan kecil dalam latensi handshake, dengan rata-rata TLS 1.3 dengan ECH sebesar 7,38 ms dibandingkan dengan 6,81 ms untuk TLS 1.3 standar. Namun, perbedaan ini tidak signifikan secara statistik ($p = 0,5850$), dan ukuran efeknya kecil (korelasi rank-biserial = -0,0448). Metode bootstrap yang digunakan menghasilkan interval kepercayaan untuk perbedaan latensi [-0,5829, 0,5747], angka tersebut menunjukkan bahwa perbedaan latensi yang sebenarnya kemungkinan dapat diabaikan. Meskipun ada dampak latensi yang minimal, ECH memberikan peningkatan privasi dengan mengenkripsi metadata handshake yang sensitif, memungkinkan administrator jaringan dan pengembang untuk memprioritaskan privasi pengguna tanpa secara signifikan mempengaruhi kinerja.