PEMANFAATAN APACHE KAFKA DAN SPARK STRUCTURED STREAMING DALAM MONITORING JARINGAN: STUDI KASUS DETEKSI SERANGAN DDOS

SKRIPSI

Oleh:

FEBRIANTO KUDADIRI
NIM. 221113626

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

UTILIZING APACHE KAFKA AND SPARK STRUCTURED STREAMING IN NETWORK MONITORING: A CASE STUDY OF DDOS ATTACK DETECTION

UNDERGRADUATE THESIS

By:

FEBRIANTO KUDADIRI
ID NUMBER. 221113626

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

LEMBARAN PENGESAHAN

PEMANFAATAN APACHE KAFKA DAN SPARK STRUCTURED STREAMING DALAM MONITORING JARINGAN: STUDI KASUS DETEKSI SERANGAN DDOS

SKRIPSI

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

Oleh:

FEBRIANTO KUDADIRI
NIM. 221113626

Disetujui Oleh:

Dosen Pembimbing I,	Dosen Pembimbing II,
Dr. Kristian Telaumbanua, S.T., M.T.	Apriyanto Halim, S.Kom., M.Kom.

Medan, 17 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 : FEBRIANTO KUDADIRI
NIM : 221113626

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:
Judul Skripsi : Pemanfaatan Apache Kafka dan Spark Structured Streaming dalam Monitoring Jaringan: Studi Kasus Deteksi Serangan DDoS
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, 28 April 2026
Saya yang membuat pernyataan,

FEBRIANTO KUDADIRI

Pemanfaatan Apache Kafka dan Spark Structured Streaming dalam Monitoring Jaringan: Studi Kasus Deteksi Serangan DDoS

Abstrak

Serangan Distributed Denial of Service (DDoS) menghasilkan lalu lintas jaringan dalam jumlah besar sehingga memerlukan sistem deteksi yang mampu memproses data secara cepat dan berkelanjutan. Penelitian ini bertujuan membangun pipeline distributed stream processing berbasis Apache Kafka, Spark Structured Streaming, dan Random Forest untuk mendukung deteksi DDoS secara near real-time. Apache Kafka digunakan sebagai message broker, Spark Structured Streaming sebagai engine pemrosesan data streaming, dan Random Forest sebagai model klasifikasi serangan. Evaluasi dilakukan menggunakan variasi input rate sebesar 100, 200, dan 400 record per detik dengan mengukur performa Kafka Producer, Spark Structured Streaming, model Random Forest, serta pipeline end-to-end berdasarkan metrik latency, throughput, dan kualitas klasifikasi. Hasil penelitian menunjukkan bahwa pipeline mampu memberikan respon deteksi secara near real-time hingga input rate 200 record per detik dengan mayoritas latency pemrosesan berada di bawah SLA 5 detik setelah fase inisialisasi. Model Random Forest mempertahankan akurasi di atas 99% pada seluruh skenario pengujian. Penurunan performa pada input rate 400 record per detik disebabkan oleh overhead Spark Structured Streaming dan akumulasi antrean data. Hasil penelitian menunjukkan bahwa arsitektur yang dikembangkan layak diterapkan untuk deteksi DDoS pada beban rendah hingga menengah serta menjadi dasar pengembangan sistem stream processing yang lebih skalabel.

Kata kunci: *Apache Kafka, Spark Structured Streaming, Random Forest, DDoS, Distributed Stream Processing*

Abstract

Distributed Denial of Service (DDoS) attacks generate massive network traffic, requiring detection systems capable of processing data rapidly and continuously. This study develops a distributed stream processing pipeline using Apache Kafka, Spark Structured Streaming, and the Random Forest algorithm to support near real-time DDoS detection. Apache Kafka functions as the message broker, Spark Structured Streaming as the streaming processing engine, and Random Forest as the attack classification model. The pipeline is evaluated under input rates of 100, 200, and 400 records per second using latency, throughput, and classification performance as evaluation metrics. The results show that the proposed pipeline provides near real-time detection at input rates of up to 200 records per second, with most processing latency remaining below the 5-second Service Level Agreement (SLA) after initialization. In addition, the Random Forest model consistently achieves over 99% classification accuracy across all test scenarios. Performance degradation at 400 records per second is mainly caused by Spark Structured Streaming overhead and data queue accumulation. These findings demonstrate that the proposed architecture is suitable for low- to medium-load DDoS detection and provides a foundation for more scalable stream processing systems.

Keywords: *Apache Kafka, Spark Structured Streaming, Random Forest, DDoS, Distributed Stream Processing*

KATA PENGANTAR

Dengan memanjatkan puji syukur kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunia-Nya, sehingga tugas akhir ini dapat terselasaikan dengan baik, yang berjudul "PEMANFAATAN APACHE KAFKA DAN SPARK STRUCTURED STREAMING DALAM MONITORING JARINGAN: STUDI KASUS DETEKSI SERANGAN DDOS".

Adapun tujuan dari penulisan tugas akhir ini adalah sebagai bentuk salah satu persyaratan untuk menyelesaikan pendidikan guna mendapatkan gelar Sarjana Strata Satu Program Studi Teknik Informatika, Universitas Mikroskil Medan.

Dalam penyusunan tugas akhir ini, penulis menyampaikan rasa terima kasih kepada:

1. Bapak Dr. Kristian Telaumbanua, S.T., M.T., selaku Dosen Pembimbing I.
2. Bapak Apriyanto Halim, 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. Bapak dan Ibu Dosen yang telah mendidik dan membimbing penulis selama menempuh pendidikan di Universitas Mikroskil Medan.
7. Keluarga penulis, khususnya orang tua, yang senantiasa memberi dukurang moral dan materiil sepanjang awal masa studi hingga saat ini, sehingga penulis dapat menyelesaikan tugas akhir ini.

Penulis menyadari, bahwa penyusunan tugas akhir ini tidak luput dari keterbatasan dan kekurangan. Oleh karena itu, penulis sangat berharap atas kritik dan saran yang bersifat membangun demi penyempurnaan di masa mendatang. Akhir kata, semoga tugas akhir ini dapat memberikan manfaat bagi pembaca dan perkembangan ilmu pengetahuan.

Medan, 24 Juni 2026

Penulis,

FEBRIANTO KUDADIRI

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL