ANALISIS PERBANDINGAN *AUTOENCODER-RANDOM FOREST* DAN *AUTOENCODER-MULTI LAYER PERCEPTRON* UNTUK DETEKSI SERANGAN *ZERO-DAY*

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

BRYANTNATA IMAM SAFI'I

22.11.4763

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

ANALISIS PERBANDINGAN *AUTOENCODER-RANDOM FOREST* DAN *AUTOENCODER-MULTI LAYER PERCEPTRON* UNTUK DETEKSI SERANGAN *ZERO-DAY*

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

BRYANTNATA IMAM SAFI'I

22.11.4763

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN *AUTOENCODER-RANDOM FOREST* DAN *AUTOENCODER-MULTI LAYER PERCEPTRON* UNTUK DETEKSI SERANGAN *ZERO-DAY*

yang disusun dan diajukan oleh

Bryantnata Imam Safi'i

22.11.4763

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Januari 2026

Dosen Pembimbing,

Subektiningsih, S.Kom., M.Kom.
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN *AUTOENCODER-RANDOM FOREST* DAN *AUTOENCODER-MULTI LAYER PERCEPTRON* UNTUK DETEKSI SERANGAN *ZERO-DAY*

yang disusun dan diajukan oleh

Bryantnata Imam Safi'i

22.11.4763

Telah dipertahankan di depan Dewan Penguji
pada tanggal 27 Januari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ferian Fauzi Abdulloh, S.Kom., M.Kom. NIK. 190302276	
Riu Andriani, S.Kom., M.Kom. NIK. 190302458	
Subektiningsih, S.Kom., M.Kom. NIK. 190302413	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 27 Januari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Bryantnata Imam Safi'i
NIM : 22.11.4763

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Perbandingan *Autoencoder-Random Forest* dan *Autoencoder-Multi Layer Perceptron* Untuk Deteksi Serangan *Zero-Day*

Dosen Pembimbing : Subektiningsih, S.Kom., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 27 Januari 2026

Yang Menyatakan,

Bryantnata Imam Safi'i

Sembah sujud serta syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi ini penulis persembahkan kepada:

1. Kedua orang tua tercinta, yang senantiasa memberikan doa, kasih sayang, dukungan moral, serta pengorbanan yang tak terhingga dalam setiap langkah perjalanan hidup dan pendidikan penulis.
2. Keluarga besar, yang selalu memberikan semangat, motivasi, dan dukungan kepada penulis selama menempuh pendidikan.
3. Ibu Subektiningsih, S.Kom., M.Kom., selaku dosen pembimbing, yang telah memberikan arahan, ilmu, serta bimbingan dengan penuh kesabaran sehingga penelitian ini dapat terselesaikan dengan baik.
4. Kak Ifada Nurrohmaniah, M.Psi., Psikolog, dan dr. Lucia Puspita Dewi, Sp.KJ., atas dukungan profesional dalam menjaga kesehatan saya selama proses penyusunan karya ini.
5. Teman-teman seperjuangan, yang telah memberikan dukungan, kebersamaan, dan semangat selama proses perkuliahan hingga penyusunan skripsi ini.
6. Almamater tercinta, Universitas AMIKOM Yogyakarta, yang telah menjadi tempat penulis menimba ilmu dan mengembangkan diri untuk menjadi lebih baik.
7. Semua pihak yang tidak dapat disebutkan satu per satu yang telah memberikan bantuan secara langsung maupun tidak langsung selama proses penyusunan skripsi.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga skripsi ini dapat diselesaikan dengan baik sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika, Universitas AMIKOM Yogyakarta. Dalam proses penyusunan skripsi ini, penulis memperoleh bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM., selaku Rektor Universitas Amikom Yogyakarta.
2. Prof. Dr. Kusrini, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Ibu Eli Pujastuti, M.Kom, selaku Ketua Program Studi Informatika Universitas Amikom Yogyakarta.
4. Ibu Subektiningsih, M.Kom., selaku dosen pembimbing yang telah memberikan arahan dan bimbingan selama penyusunan skripsi.
5. Bapak Ferian Fauzi Abdulloh, M.Kom., selaku dosen wali yang telah membimbing penulis selama masa perkuliahan.
6. Seluruh dosen dan civitas akademika Universitas Amikom Yogyakarta, yang telah memberikan ilmu, pengalaman, dan wawasan selama kuliah

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan, sehingga kritik dan saran sangat diharapkan demi penyempurnaan karya ini. Semoga skripsi ini dapat memberikan manfaat, khususnya dalam bidang keamanan jaringan dan deteksi serangan Zero-Day.

Yogyakarta, 1 Januari 2026

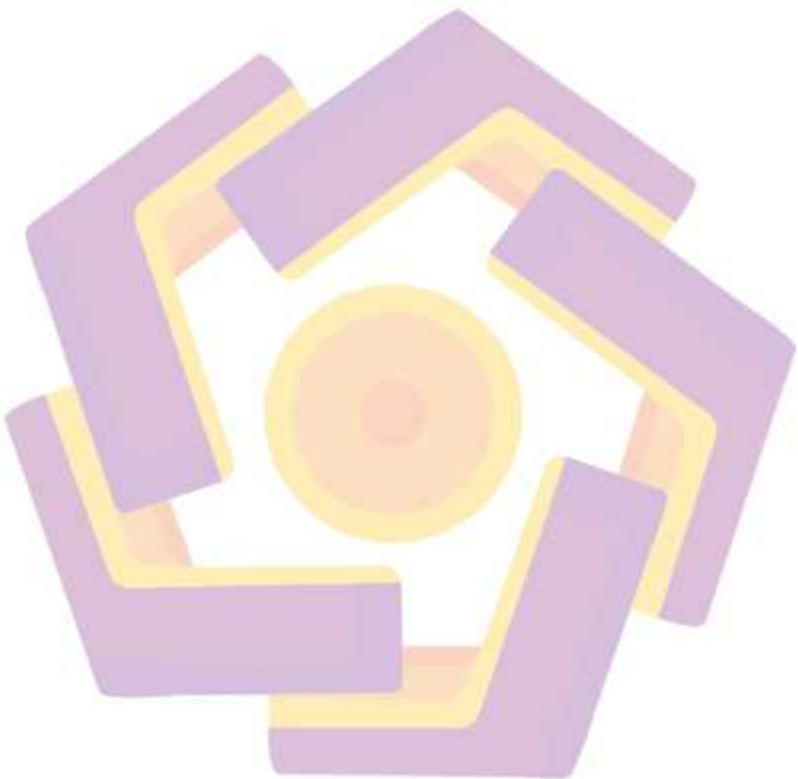
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN



DAFTAR LAMBANG DAN SINGKATAN

x	Vektor *input* atau data asli.
$\hat{x}$	Vektor *output* atau hasil rekonstruksi data.
h	*Hidden layer* atau representasi laten.
W	Matriks bobot *(Weight)* pada jaringan saraf tiruan
b	Vektor bias pada jaringan saraf tiruan
f(.)	Fungsi aktivasi pada *encoder*
g(.)	Fungsi aktivasi pada *decoder*
L	Fungsi kerugian *(Loss Function)*
θ	Parameter model
AE	*Autoencoder*
ANN	*Artificial Neural Network*
CNN	*Convolutional Neural Network*
DL	*Deep Learning*
FN	*False Negative*
FP	*False Positive*
FPR	*False Positive Rate*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
ML	*Machine Learning*
MLP	*Multi-Layer Perceptron*
MSE	*Mean Squared Error*
NIDS	*Network Intrusion Detection System*
RE	*Reconstruction Error*
ReLU	*Rectified Linear Unit*
RF	*Random Forest*
SGD	*Stochastic Gradient Descent*
TN	*True Negative*
TP	*True Positive*
TPR	*True Positive Rate*

DAFTAR ISTILAH

Anomaly Detection	Sistem yang digunakan untuk mendeteksi dan menganalisis ancaman atau aktivitas mencurigakan dalam jaringan atau sistem komputer dengan tujuan menemukan serangan atau pelanggaran keamanan.
Benign	Istilah yang digunakan untuk melabeli lalu lintas jaringan yang normal, aman, dan bukan merupakan serangan.
Bottleneck	Lapisan tengah pada arsitektur *Autoencoder* yang memiliki dimensi paling kecil, berfungsi untuk memaksa model mempelajari representasi data yang paling penting (fitur laten).
Class Imbalance	Kondisi dalam *dataset* di mana jumlah sampel antar kelas tidak seimbang secara signifikan, misalnya jumlah data normal jauh lebih banyak daripada data serangan.
Confusion Matrix	Tabel yang digunakan untuk mengevaluasi kinerja model klasifikasi dengan membandingkan nilai prediksi model terhadap nilai sebenarnya *(ground truth)*.
Epoch	Satu putaran penuh di mana seluruh *dataset* pelatihan telah melewati proses pembelajaran oleh algoritma *machine learning*.
Feature Extraction	Proses transformasi data mentah menjadi format numerik yang dapat diproses oleh model, dalam penelitian ini dilakukan menggunakan *Autoencoder*.
Hyperparameter	Parameter eksternal yang nilainya ditetapkan sebelum proses pelatihan dimulai (misalnya: *learning rate, batch size*, jumlah *tree*) dan tidak berubah selama pelatihan.

Latent Space	Representasi data yang terkompresi pada lapisan *bottleneck* di dalam *Autoencoder*, yang memuat fitur-fitur esensial dari data *input*.
Loss Function	Fungsi matematis yang mengukur selisih antara prediksi model dengan target yang sebenarnya; dalam *Autoencoder* sering menggunakan MSE.
Overfitting	Kondisi di mana model terlalu baik dalam mempelajari data latih (termasuk noise) sehingga performanya buruk saat diuji pada data baru yang belum pernah dilihat.
Parquet	Format penyimpanan data berbasis kolom *(columnar storage)* yang efisien dalam hal kompresi dan kecepatan pembacaan, digunakan untuk menangani *dataset* besar.
Reconstruction Error	Nilai selisih atau kesalahan antara data *input* asli dengan data hasil rekonstruksi *output* pada *Autoencoder*; digunakan sebagai indikator anomali.
Throughput	Ukuran kecepatan sistem dalam memproses data, dalam penelitian ini dihitung berdasarkan jumlah baris data yang dapat diklasifikasikan per detik.
Unseen Data	Data yang tidak pernah dilibatkan selama proses pelatihan model, digunakan untuk menguji kemampuan generalisasi model terhadap serangan baru.

INTISARI

Serangan Zero-Day merupakan ancaman keamanan jaringan yang sulit dideteksi karena karakteristiknya yang tidak terdaftar dalam pangkalan data tanda tangan ancaman tradisional. Penelitian ini bertujuan untuk menganalisis dan membandingkan performa dua arsitektur *hybrid* berbasis deteksi anomali, yaitu *Autoencoder - Random Forest* (AE-RF) dan *Autoencoder - Multi Layer Perceptron* (AE-MLP), dalam mendeteksi serangan Zero-Day menggunakan *dataset* CSE-CIC-IDS2018. Metode yang diusulkan memanfaatkan *Autoencoder* untuk mereduksi 78 fitur asli menjadi 16 fitur laten serta mengintegrasikan fitur *Reconstruction Error* (RE) guna memperkuat sinyal anomali. Hasil pengujian menunjukkan bahwa model *baseline* tanpa *Autoencoder* gagal mendeteksi serangan *Zero-Day* dengan tingkat keberhasilan 0%. Pada arsitektur *hybrid*, model *Autoencoder - Multi Layer Perceptron* dengan *Reconstruction Error* menunjukkan performa terbaik dengan tingkat deteksi serangan *Zero-Day* keseluruhan mencapai 99,84% serta efisiensi komputasi tertinggi sebesar 178.917 baris per detik melalui akselerasi GPU. Meskipun memiliki *False Positive Rate* yang lebih tinggi (18,00%) sebagai konsekuensi sensitivitas tinggi terhadap anomali, model ini jauh mengungguli model *Autoencoder - Random Forest* dengan *Reconstruction Error* yang hanya menghasilkan tingkat deteksi 51,22% akibat kegagalan mendeteksi pola serangan terenkripsi (SSH) serta memiliki *throughput* yang lebih rendah. Berdasarkan hasil tersebut, dapat disimpulkan bahwa arsitektur *Autoencoder - Multi Layer Perceptron* dengan integrasi fitur *Reconstruction Error* merupakan pendekatan yang paling optimal untuk deteksi serangan Zero-Day pada lingkungan jaringan berskala besar.

Kata kunci: *Intrusion Detection System*, Serangan *Zero-Day*, *Autoencoder*, *Reconstruction Error*, *Multi-Layer Perceptron*.

ABSTRACT

Zero-Day attacks pose a serious threat to network security due to their characteristics that are not recorded in traditional signature-based threat databases. This study aims to analyze and compare the performance of two hybrid anomaly-based detection architectures, namely Autoencoder-Random Forest (AE-RF) and Autoencoder-Multi Layer Perceptron (AE-MLP), for detecting Zero-Day attacks using the CSE-CIC-IDS2018 dataset. The proposed method employs an Autoencoder to reduce the original 78 features into 16 latent features and integrates the Reconstruction Error (RE) as an additional indicator to enhance anomaly detection. Experimental results show that the baseline model without Autoencoder completely fails to detect Zero-Day attacks, achieving a detection rate of 0%. In contrast, the hybrid Autoencoder-Multi Layer Perceptron with Reconstruction Error model demonstrates the best performance, achieving an overall Zero-Day detection rate of 99.84% and the highest computational efficiency with a throughput of 178,917 records per second through GPU acceleration. Although it exhibits a higher False Positive Rate (18.00%) as a consequence of high sensitivity to anomalies, this model significantly outperforms the Autoencoder - Random Forest with Reconstruction Error model, which only yields a detection rate of 51.22% due to its failure in detecting encrypted attack patterns (SSH) and has a lower throughput. Based on these results, it can be concluded that the Autoencoder - Multi Layer Perceptron architecture integrated with Reconstruction Error is the most optimal approach for Zero-Day attack detection in large-scale network environments.

Keywords: Intrusion Detection System, Zero-Day Attack, Autoencoder, Reconstruction Error, Multi-Layer Perceptron.