PERANCANGAN SISTEM KEAMANAN SIBER BERBASIS *HYBRID ENSEMBLE* UNTUK DETEKSI ANOMALI JARINGAN

SKRIPSI

Diajukan Guna Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S. Kom.)
Pada Program Studi Teknik Informatika

Oleh :

Nico Adi Saputra
NPM : 2113020119

FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS NUSANTARA PGRI KEDIRI
2025

Skripsi oleh:

Nico Adi Saputra
NPM : 2113020119

Judul :

PERANCANGAN SISTEM KEAMANAN SIBER BERBASIS HYBRID ENSEMBLE UNTUK DETEKSI ANOMALI JARINGAN

Telah Disetujui Untuk Diajukan Kepada Panitia Ujian/Sidang Skripsi
Program Studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer
Universitas Nusantara PGRI Kediri

Tanggal : 20 Juni 2025

Pembimbing I	Pembimbing II
Rony Heri Irawan, M.Kom.	Umi Mahdiyah, S.Pd., M.Si.
NIDN. 0711018102	NIDN. 0729098903

Skripsi oleh:

Nico Adi Saputra
NPM : 2113020119

Judul :

PERANCANGAN SISTEM KEAMANAN SIBER BERBASIS HYBRID ENSEMBLE UNTUK DETEKSI ANOMALI JARINGAN

Telah dipertahankan di depan Panitia Ujian/Sidang Skripsi
Program Studi Teknik Informatika Fakultas Teknik dan Ilmu Komputer
Universitas Nusantara PGRI Kediri
Pada tanggal : 10 Juli 2025
Dan Dinyatakan telah Memenuhi Syarat

Panitia Penguji :

1. Ketua : Rony Heri Irawan, M.Kom.
2. Penguji I : Ratih Kumalasari N, S.ST, M.Kom.
3. Penguji II : Umi Mahdiyah, S.Pd., M.Si.

Mengetahui,
Dekan FTIK

Dr. Sulistiono, M.Si.
NIDN. 0007076801

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini saya,

Nama	: Nico Adi Saputra
Jenis Kelamin	: Laki-laki
Tempat/Tgl Lahir	: Kediri / 4 April 2001
NPM	: 2113020119
Fakultas/Prodi	: Teknik dan Ilmu Komputer / Teknik Informatika

Menyatakan dengan sebenarnya, bahwa dalam Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi, dan sepanjang pengetahuan saya tidak dapat karya tulis atau pendapat yang pernah diterbitkan oleh orang lain, kecuali yang secara sengaja dan tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Kediri, 10 Juli 2025
Yang Menyatakan

Nico Adi Saputra
NPM : 2113020119

HALAMAN PERSEMBAHAN

Penulisan skripsi ini dengan tulus saya dedikasikan kepada:

1. Kedua orang tua saya, yang dengan penuh kesabaran senantiasa mendoakan, memberikan dukungan terbaik, serta menjadi sumber motivasi tak henti-hentinya dalam perjalanan menyelesaikan skripsi ini.
2. Dea Avrillia Arba'a pemilik NPM 2113020125, yang selalu memberikan semangat dan dukungan moral, sehingga saya dapat menyelesaikan proses ini dengan baik.
3. Seluruh dosen Universitas Nusantara PGRI Kediri, yang telah memberikan bimbingan, ilmu, dan pelajaran berharga, baik dalam ranah akademik maupun kehidupan sehari-hari.
4. Teman-teman seperjuangan di kampus, yang menjadi tempat berbagi suka dan duka, serta saling menyemangati selama menjalani masa perkuliahan hingga tahap akhir ini.
5. Almamater tercinta, Universitas Nusantara PGRI Kediri, yang telah menjadi tempat saya tumbuh, belajar, dan mengembangkan diri selama masa perkuliahan.
6. Semua pihak yang tidak dapat saya sebutkan satu per satu, yang telah memberikan kontribusi dalam berbagai bentuk dukungan selama proses penyusunan skripsi ini.

Semoga dedikasi ini dapat menjadi penghormatan atas semua dukungan, doa, dan kebersamaan yang telah diberikan.

HALAMAN MOTTO

"Keutamaan ilmu lebih baik daripada keutamaan ibadah, karena ilmu adalah cahaya, sedangkan ibadah adalah jalan menuju cahaya." **— Imam Syafi'i**

"Jangan berhenti belajar, karena kehidupan tidak pernah berhenti mengajarkan."

— Albert Einstein

"Ilmu adalah harta yang tidak akan pernah habis, maka carilah ilmu sebanyak mungkin sebelum waktumu habis."

— Ali bin Abi Thalib RA

"Hidup itu bukan sekadar mencari kebahagiaan, tetapi menemukan tujuan dan memberi makna pada kehidupan." **— Albert Einstein**

RINGKASAN

Nico Adi Saputra Perancangan Sistem Keamanan Siber Berbasis Hybrid Ensemble untuk Deteksi Anomali Jaringan, Skripsi, Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Nusantara PGRI Kediri, 2025

Kata Kunci : Deteksi Anomali, *Hybrid Ensemble*, Keamanan Siber, Serangan Siber, *Network Intrusion Detection System*.

Penelitian ini bertujuan untuk mengembangkan sistem deteksi anomali jaringan berbasis *Hybrid Ensemble Learning* yang menggabungkan algoritma *Isolation Forest*, *K-Means*, dan *Random Forest* dengan menggunakan metode *majority voting.* Tujuan utama dari sistem ini adalah untuk meningkatkan performa deteksi anomali pada serangan siber, khususnya serangan zero-day dan *Advanced Persistent Threats* (APT), yang sering sulit dideteksi menggunakan metode tradisional berbasis tanda tangan.

Sistem ini menggunakan dataset CSE-CIC-IDS2018 untuk pelatihan dan pengujian, serta mengevaluasi hasil dengan menggunakan metrik seperti akurasi, p*recision*, *recall*, *F1-score*, dan AUC. Hasil penelitian menunjukkan bahwa pendekatan *hybrid* ini mampu mencapai akurasi 99,9% dan mengurangi tingkat *false positive* secara signifikan, lebih baik dibandingkan dengan penggunaan algoritma tunggal.

Metode ini membuktikan efektivitasnya dalam meningkatkan keandalan sistem deteksi anomali dengan menggabungkan kekuatan berbagai algoritma, serta memberikan kontribusi terhadap pengembangan teknologi keamanan jaringan yang lebih efisien dan adaptif.

PRAKATA

Puji Syukur dipanjatkan kepada Tuhan Yang Maha Esa, karena atas ridha dan karunianya peneliti dapat menyelesaikan penyusunan laporan penelitian ini. Penulisan ini juga tak lepas dari dukungan pihak yang selalu membantu dalam penulisan penelitian ini. Oleh karenanya peneliti ingin mengucapkan terima kasih kepada:

1. Bapak Dr. Zainal Afandi, M.Pd. selaku Rektor Universitas Nusantara PGRI Kediri.
2. Bapak Dr. Sulistiono, M. Si. selaku Dekan Fakultas Teknik dan Ilmu Komputer Universitas Nusantara PGRI Kediri.
3. Ibu Risa Helilintar, M. Kom. selaku Ketua Program Studi Teknik Informatika Universitas Nusantara PGRI Kediri.
4. Bapak Rony Heri Irawan, M. Kom. dan Ibu Umi Mahdiyah, S. Pd., M. Si. selaku Dosen Pembimbing Skripsi yang telah dan mengarahkan kami selama mengerjakan skripsi.
5. Kedua Orang Tua saya dan Keluarga atas doa dan dukungannya.
6. Ucapan terimakasih juga disampaikan kepada pihak-pihak lain yang tidak dapat disebutkan satu persatu, yang telah banyak membantu menyelesaikan penulisan penelitian ini.

Disadari penelitian ini masih banyak kekurangan, maka diharapkan kritik dan saran dari berbagai pihak sangat diharapkan. Semoga penelitian ini bermanfaat bagi semua pihak.

Kediri, 10 Juli 2025

Nico Adi Saputra
NPM : 2113020119

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan era digital telah menjadikan keamanan siber sebagai aspek yang sangat penting dalam melindungi data dan sistem informasi. Berbagai sektor, seperti pemerintahan, kesehatan, dan bisnis, semakin bergantung pada jaringan komputer untuk menjalankan operasi sehari-hari. Ketergantungan ini, meskipun meningkatkan efisiensi dan produktivitas, juga membuka peluang bagi penyerang untuk mengeksploitasi kelemahan sistem melalui serangan siber yang canggih, seperti *zero day attacks* dan *Advanced Persistent Threats* (APT) (Goswami, 2024; Alserhani & Aljared, 2023).

Untuk mengatasi ancaman tersebut, *Network Intrusion Detection Systems* (NIDS) telah menjadi salah satu alat penting dalam sistem keamanan jaringan. NIDS dirancang untuk memantau lalu lintas jaringan dan mengidentifikasi aktivitas mencurigakan yang dapat mengindikasikan adanya serangan. Namun, pendekatan tradisional berbasis tanda tangan (*signature-based detection*) memiliki keterbatasan signifikan karena hanya mampu mendeteksi serangan yang telah dikenali sebelumnya, sehingga kurang efektif dalam menghadapi serangan baru yang belum memiliki tanda tangan (Alserhani & Aljared, 2023).

Sebagai alternatif, pendekatan berbasis deteksi anomali (*anomaly-based detection*) menawarkan solusi yang lebih adaptif dengan menggunakan model pembelajaran untuk mengenali pola lalu lintas jaringan normal dan mengidentifikasi anomali sebagai indikasi serangan. Meskipun metode ini menjanjikan, sering kali menghasilkan tingkat *false positive* yang tinggi, yang membebani pengguna dalam melakukan analisis manual dan mengurangi kepercayaan terhadap sistem deteksi (Elmahalwy dkk., 2023).

Berbagai penelitian telah mengkaji pendekatan deteksi anomali dalam sistem keamanan jaringan. (Santoso dkk., 2024) menggunakan algoritma *Naive Bayes* yang mencapai akurasi 86%, namun masih menghadapi masalah *false positive*. (Agustina dkk, 2024) menerapkan algoritma *Random Forest* dengan metode pemilihan fitur *wrapper*, menghasilkan akurasi lebih tinggi yaitu 91,51% dibandingkan metode *filter*. (Bakhare, 2024) mengevaluasi beberapa algoritma dan menemukan bahwa *Random Forest* mencapai akurasi terbaik sebesar 87%. Meskipun demikian, pendekatan-pendekatan ini masih memiliki keterbatasan, seperti ketergantungan pada algoritma tunggal dan tingkat *false positive* yang tinggi. Hal ini menunjukkan kebutuhan untuk pendekatan yang lebih komprehensif, seperti penggunaan *hybrid ensemble learning*, yang dapat mengatasi keterbatasan tersebut.

Untuk mengatasi keterbatasan tersebut, penelitian ini mengusulkan penggunaan teknik *hybrid ensemble learning* yang menggabungkan kekuatan beberapa algoritma *machine learning*, seperti *IForest-K-Means*, *Random Forest* dan penerapan *Majority Voting*. Kombinasi algoritma ini diharapkan dapat meningkatkan peforma model, agar dapat membantu memperkuat keputusan deteksi, sehingga menghasilkan sistem deteksi yang lebih andal dan efisien. Dengan demikian, penelitian ini bertujuan untuk merancang dan mengevaluasi metode *hybrid ensemble learning* yang lebih efektif dalam mendeteksi ancaman siber, khususnya *zero day attacks* dan APT.

B. Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, berikut adalah identifikasi masalah yang ditemukan:

1. Sistem deteksi berbasis *signature-based detection* tidak mampu mendeteksi ancaman canggih seperti *zero-day attacks* dan APT, sehingga menciptakan celah keamanan yang signifikan dalam sistem jaringan.

2. Tingginya tingkat *false positives* pada sistem deteksi anomali menyebabkan pengguna kehilangan kepercayaan terhadap hasil deteksi.
3. Kurangnya integrasi algoritma yang optimal dalam sistem deteksi intrusi jaringan mengakibatkan rendahnya akurasi dalam mendeteksi ancaman anomali, khususnya pada data jaringan berskala besar.

C. Rumusan Masalah

Berdasarkan identifikasi masalah yang telah diuraikan, rumusan masalah dalam penelitian ini adalah bagaimana penerapan kombinasi algoritma *IForest-KMeans* dan *Random Forest* dengan integrasi teknik *Majority Voting* dapat meningkatkan performa sistem dalam mendeteksi anomali pada jaringan?

D. Batasan Masalah

Agar penelitian ini terarah dan fokus pada pencapaian tujuan, batasan masalah yang diterapkan adalah sebagai berikut:

1. Penelitian ini merancang dan mengevaluasi metode *hybrid ensemble learning* yang mengintegrasikan algoritma *Isolation Forest, K-Means*, dan *Random Forest*, serta menggunakan teknik *Majority Voting* untuk meningkatkan peforma sistem.
2. Penelitian menggunakan *dataset* publik yang relevan, yang berfokus pada serangan yang lebih terkini. *Dataset* ini berisi data jaringan yang dapat digunakan untuk melatih model deteksi serangan.
3. Sistem dirancang berbasis *web* dengan menggunakan *framework flask* dari *python* sebagai *backend*. Visualisasi data dan hasil deteksi anomali akan disajikan dalam *dashboard web*.
4. Evaluasi performa model akan dibatasi pada *evaluation metrics* dan AUC tanpa mempertimbangkan aspek implementasi langsung pada sistem keamanan *real-time*.

E. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disampaikan, penelitian ini bertujuan untuk merancang dan mengevaluasi kombinasi algoritma *IForest-KMeans* dan *Random Forest* dengan integrasi teknik *Majority*

Voting, guna meningkatkan performa sistem deteksi anomali pada jaringan, yang meliputi peningkatan akurasi deteksi serta pengurangan tingkat *false positives*.

F. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat dalam berbagai aspek, baik secara akademis, praktis, maupun teknologi. Berikut adalah manfaat penelitian yang diharapkan:

1. Manfaat Akademis**:**
    a. Penelitian ini berkontribusi pada pengembangan teori dan praktik dalam bidang keamanan siber, khususnya dalam penerapan *hybrid ensemble learning* untuk deteksi ancaman.
    b. Menyediakan referensi dan temuan terbaru yang dapat digunakan oleh peneliti lain dalam studi lanjutan mengenai deteksi ancaman siber dan teknik *machine learning*.
    c. Memperkenalkan pendekatan baru dalam kombinasi algoritma *machine learning* yang dapat menjadi dasar bagi penelitian selanjutnya dalam pengembangan metode deteksi yang lebih efektif.
2. Manfaat Praktis:
    a. Memberikan solusi yang lebih akurat dan efisien dalam mendeteksi ancaman siber, sehingga organisasi dapat meningkatkan tingkat keamanan jaringan mereka dan mengurangi risiko serangan.
    b. Menurunkan tingkat *false positives* organisasi dapat mengurangi biaya yang terkait dengan analisis ancaman manual dan pemulihan dari serangan yang berhasil.
    c. Sistem deteksi yang lebih andal meningkatkan kepercayaan pengguna dan pemangku kepentingan terhadap sistem keamanan informasi yang diterapkan.
3. Manfaat Teknologi:
    a. Mengembangkan dan mengimplementasikan metode *hybrid ensemble learning* yang dapat diterapkan dalam berbagai sistem

deteksi intrusi, meningkatkan kemampuan teknologi dalam menghadapi ancaman siber yang terus berkembang.

b. Menyediakan pendekatan yang tidak hanya meningkatkan akurasi deteksi tetapi juga mempertimbangkan efisiensi penggunaan sumber daya komputasi, memungkinkan penerapan di lingkungan dengan keterbatasan infrastruktur.