IMPLEMENTASI SISTEM KEAMANAN JARINGAN UNTUK MITIGASI SERANGAN *DDoS* BERBASIS ENSEMBLE *MACHINE LEARNING* MENGGUNAKAN MIKROTIK DAN IDS

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Terapan Teknik Komputer dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Ujung Pandang

GUIDO SEPTIVIANUS PRASETIO VENTURA
425 21 011

PROGRAM STUDI S1 TERAPAN TEKNIK KOMPUTER DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI UJUNG PANDANG
MAKASSAR
2025

HALAMAN PENGESAHAN

Skripsi dengan judul IMPLEMENTASI SISTEM KEAMANAN JARINGAN UNTUK MITIGASI SERANGAN *DDoS* BERBASIS *ENSEMBLE MACHINE LEARNING* MENGGUNAKAN MIKROTIK DAN IDS oleh GUIDO SEPTIVIANUS PRASETIO VENTURA NIM 42521011 telah diterima dan disahkan sebagai salah satu syarat untuk memperoleh gelar Sarjana Terapan pada Program Studi Teknik Komputer dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Ujung Pandang.

Makassar, 26 Agustus 2025

Mengesahkan,

Dosen Pembimbing I	Dosen Pembimbing II
Prof. Irfan Syamsuddin S.T., M.Com.ISM., Ph.D.	**Fadli Tamrin, S.Kom., M.Cs**
NIP. 197312202000031008	NIP. 198912232022031006

Mengetahui,
Ketua Program Studi

Meylanie Olivya, S.T., M.T.
NIP. 198205032014042002

HALAMAN PENERIMAAN

Pada hari ini, tanggal 26 Agustus 2025 Tim Penguji Ujian Sidang Skripsi telah menerima dengan baik Skripsi oleh mahasiswa GUIDO SEPTIVIANUS PRASETIO VENTURA nomor induk mahasiswa 42521011 dengan judul "IMPLEMENTASI SISTEM KEAMANAN JARINGAN UNTUK MITIGASI SERANGAN *DDoS* BERBASIS *ENSAMBLE MACHINE LEARNING* MENGGUNAKNAN MIKROTIK DAN IDS"

Makassar, 26 Agustus 2025

Tim Penguji Ujian Sidang Skripsi:

1	Muhammad Nur Yasir Utomo, S.ST., M.Eng	Ketua	(.....)
2	Budy Santoso, S.Kom., M.Eng.	Sekretaris	(.....)
3	Ir.Dahlia,M.T.	Anggota	(.....)
4	Rini Nur,S.T., M.T.	Anggota	(.....)
5	Prof. Irfan Syamsuddin S.T., M.Com.ISM., Ph.D.	Anggota	(.....)
6	Fadli Tamrin, S.Kom., M.Cs	Anggota	(.....)

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena berkat dan juga Rahmat-Nya yang telah memberikan kesehatan kepada penulis sehingga penulis dapat menyelesaikan skripsi-Nya yang berjudul "Perancangan Sistem Keamanan Jaringan Untuk Mitigasi Serangan *DDoS* Berbasis Ensamble *Machine learning* Menggunakan Mikrotik Dan IDS" dengan baik dan lancar.

Skripsi ini disusun sebagai salah satu syarat untuk dapat menyelesaikan studi dan juga dalam rangka memperoleh gelar diploma IV (D-4 / S1 Terapan) pada Program Studi Teknik Komputer dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Ujung Pandang.

Penulis menyadari bahwa keberhasilan dari skripsi ini tidak terlepas dari bantuan berbagai pihak baik secara langsung maupun secara tidak langsung. oleh karena itu, penulis menyampaikan bentuk apresiasi dengan mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Kepada Tuhan Yang Maha Esa yang telah memberikan kesehatan dan juga kesempatan sehingga penulis bisa menyelesaikan penelitian ini dengan baik dan lancar.
2. Orang tua dari penulis yakni Bapak Bonefasius Tura dan Ibu Aurelia Suen serta saudara penulis dan keluarga besar yang telah memberikan semangat, motivasi, doa dan bimbingan kepada penulis.
3. Bapak Prof. Dr. Jamal, S.T., M.T. selaku Direktur Politeknik Negeri Ujung Pandang.
4. Ibu Irmawati, S.T., M.T. selaku Ketua Jurusan Teknik Informatika dan Komputer Politeknik Negeri Ujung Pandang.
5. Ibu Meylanie Olivya, S.T., M.T. sebagai Ketua Program Studi D4 Teknik Komputer dan Jaringan, atas segala fasilitas dan kesempatan yang telah diberikan kepada penulis.

6. Bapak Prof. Irfan Syamsuddin, S.T., M.Com.ISM., Ph.D sebagai Dosen Pembimbing I, atas segala arahan, bimbingan, dan juga dukungan yang tidak pernah lelah diberikan.
7. Bapak Fadli Tamrin, S.Kom., M.Cs sebagai Dosen Pembimbing II, atas segala motivasi, saran, dan juga dukungan selama proses penelitian ini hingga penulisan skripsi ini selesai dengan lancar.
8. Bapak / Ibu Dosen dan staf jurusan Teknik Informatika dan Komputer khususnya Program Studi Teknik Komputer dan Jaringan yang telah memberikan ilmu yang sangat berharga selama mengikuti perkuliahan di Politeknik Negeri Ujung Pandang.
9. Teman-teman seperjuangan di Program Studi TKJ angkatan 2021 yang telah berjuang bersama selama 4 tahun dan banyak memberikan berbagai hal baik dari segi akademik maupun non akademik dan banyak hal tentang kebersamaan dan juga kekompakan selama menyelesaikan studi di Politeknik Negeri Ujung Pandang.

Penulis berharap semoga Tuhan Yang Maha Esa berkenan membalas segala kebaikan oleh semua pihak yang telah membantu. Penulis menyadari bahwa penyusunan skripsi masih terdapat banyak kekurangan, sehingga penulis mengharapkan untuk diberikan kritik maupun saran yang bersifat membangun untuk dapat membangun untuk diperbaiki di masa yang akan datang. Semoga apa yang penulis telah lakukan bisa bermanfaat bagi pembaca sehingga dapat menghasilkan sumber daya manusia yang berkualitas dan juga berguna bagi bangsa dan negara.

Makassar,26 Agsutus 2025

Penulis

DAFTAR ISI

SURAT PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama Lengkap	: Guido Septivianus Prasetio Ventura
NIM	: 42521011
Program Studi	: Teknik Komputer dan Jaringan
Tempat / Tgl. Lahir	: Makassar, 12 September 2003
Alamat	: Jalan Gassing Dg Tiro

Dengan ini menyatakan :

A. Tugas Akhir / Skripsi yang berjudul :

Implementasi Sistem Keamanan Jaringan Untuk Mitigasi Serangan DDoS Berbasis Ensamble Machine Learning Menggunakan Mikrotik Dan IDS

Adalah benar disusun / dibuat oleh saya sendiri dan jika dikemudian hari diketahui berdasarkan bukti-bukti yang kuat ternyata Tugas Akhir / Skripsi tersebut dibuatkan oleh orang lain atau diketahui bahwa Tugas Akhir / Skripsi tersebut merupakan plagiat/mencontek/menjiplak hasil karya ilmiah orang lain, maka dengan ini saya siap menerima segala yang ditimbulkan berupa pembatalan/pencabutan Gelar Akademik dan siap mengulang kembali dari awal.

B. Bahwa seluruh dokumen (copy ijazah, copy transkrip nilai) dan lain-lain sebagai persyaratan sidang adalah asli milik saya pribadi dan dapat saya pertanggung jawabkan keasliannya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Makassar, 26 Agustus 2025

Hormat Saya,

Guido Septivianus Prasetio Ventura

IMPLEMENTASI SISTEM KEAMANAN JARINGAN UNTUK MITIGASI SERANGAN *DDoS* BERBASIS ENSEMBLE *MACHINE LEARNING* MENGGUNAKAN MIKROTIK DAN IDS

RINGKASAN

Serangan Distributed Denial of Service (*DDoS*) merupakan ancaman siber yang terus berkembang, mampu melumpuhkan layanan jaringan dan menyebabkan kerugian signifikan. Sistem keamanan konvensional seringkali tidak cukup fleksibel untuk menghadapi serangan yang dinamis dan canggih. Penelitian ini bertujuan untuk merancang dan membangun sebuah sistem keamanan jaringan yang cerdas dan otomatis untuk mitigasi serangan *DDoS*. Sistem ini mengintegrasikan *Intrusion Detection System* (IDS) Zeek, model *ensemble machine learning*, dan router MikroTik dalam satu alur kerja yang kohesif. Metode yang digunakan melibatkan analisis lalu lintas jaringan secara real-time oleh Zeek, yang kemudian log-nya diklasifikasikan oleh model ensemble learning yang telah dilatih menggunakan dataset CIC*DDoS*2019. Hasil pengujian menunjukkan bahwa model yang dikembangkan, dengan seleksi fitur menggunakan metode *SelectKBest*, mampu mencapai akurasi deteksi sebesar 94.98%. Sistem secara keseluruhan menunjukkan responsivitas yang tinggi, mampu mendeteksi dan mengeksekusi blokir otomatis pada IP penyerang di MikroTik dalam waktu rata-rata 38 detik. Implementasi sistem terbukti efektif dalam melindungi *server* target, yang ditunjukkan dengan normalisasi penggunaan *CPU* dari 97.1% saat serangan menjadi 4.7% setelah mitigasi, serta pemulihan parameter Quality of Service (*Qos*) jaringan. Penelitian ini berhasil menghasilkan sebuah arsitektur pertahanan siber yang otonom, cepat, dan akurat, serta menyediakan cetak biru praktis untuk mengamankan infrastruktur jaringan yang ada dari ancaman *DDoS*.

Kata Kunci: Keamanan Jaringan, Mitigasi *DDoS*, Ensemble *Machine learning*, MikroTik, Zeek IDS, Otomatisasi Keamanan.

BAB I PENDAHULUAN

1.1 Latar Belakang

Seiring dengan pesatnya perkembangan teknologi digital, situs web telah menjadi bagian penting dalam berbagai sektor, mulai dari bisnis, layanan publik, hingga interaksi sosial. Ketergantungan yang tinggi terhadap situs web dan infrastruktur digital ini berbanding lurus dengan meningkatnya ancaman keamanan siber, termasuk serangan *Distributed Denial of Service* (*DDoS*). Menurut laporan terbaru dari NETSCOUT (2023), jumlah serangan *DDoS* global meningkat lebih dari 30% dalam lima tahun terakhir, dengan skala dan kompleksitas yang semakin berkembang.

Serangan *DDoS* bertujuan untuk membuat layanan web tidak tersedia bagi pengguna yang sah dengan cara membanjiri infrastruktur *server* atau jaringan dengan lalu lintas data dalam jumlah besar. Hal ini menyebabkan *server* menjadi kewalahan dan gagal memproses permintaan pengguna normal, yang berujung pada kegagalan layanan secara keseluruhan. Seperti yang dijelaskan oleh Kaur et al. (2016) bahwa "serangan *DDoS* tidak hanya berdampak pada ketersediaan layanan tetapi juga dapat menyebabkan kerugian finansial dan reputasi yang signifikan bagi organisasi yang terdampak".

Router merupakan salah satu komponen utama dalam infrastruktur jaringan yang berfungsi mengatur lalu lintas data berdasarkan tabel routing yang tersedia. Perangkat ini menjadi titik krusial dalam jaringan karena bertanggung jawab dalam meneruskan paket data ke tujuan yang benar. Namun, router juga menjadi sasaran utama dalam serangan *DDoS*, di mana penyerang mengirimkan lalu lintas berlebih secara terus-menerus untuk membebani kapasitas pemrosesan router. (Jaya, Yuhandri, & Sumijan, 2020) menjelaskan bahwa metode serangan seperti manipulasi ukuran paket yang dikirimkan ke router dapat menyebabkan peningkatan konsumsi daya dan lonjakan penggunaan *CPU*, yang pada akhirnya mengakibatkan penurunan kinerja jaringan, bahkan sebelum serangan mencapai *server* utama..

Sistem keamanan jaringan pada *Firewall* dan *Intrusion Detection System (*IDS) telah digunakan untuk memitigasi serangan *DDoS*. Namun, pendekatan ini memiliki keterbatasan dalam menghadapi serangan yang semakin canggih dan dinamis. *Firewall* hanya dapat memblokir lalu lintas berdasarkan aturan yang telah ditentukan sebelumnya, sehingga kurang fleksibel dalam menyesuaikan diri dengan ancaman yang belum teridentifikasi. Sementara itu, IDS memiliki keterbatasan dalam melakukan analisis mendalam terhadap konten data, yang sangat krusial untuk mengidentifikasi karakteristik spesifik dari serangan *DDoS* (Syujak., dkk 2024). IDS berperan dalam mendeteksi aktivitas mencurigakan di dalam jaringan, tetapi umumnya hanya berfungsi sebagai sistem pemantauan tanpa mekanisme pencegahan otomatis.

Salah satu solusi yang menjanjikan dalam menghadapi serangan *DDoS* adalah penerapan *Machine learning* (ML) dalam sistem keamanan jaringan. (Yu, Li, dan Li 2020) menunjukkan bahwa penggunaan *machine learning* dapat meningkatkan akurasi dalam mendeteksi serangan jaringan, terutama ketika menggunakan teknik *ensemble learning. Ensemble learning* menggabungkan beberapa model *machine learning* untuk meningkatkan ketahanan terhadap variasi serangan yang lebih kompleks (Sagi & Rokach, 2018).

Namun, meskipun pendekatan *ensemble learning* telah terbukti meningkatkan efektivitas deteksi serangan *DDoS*, masih terdapat beberapa aspek yang perlu diperhatikan dalam implementasinya. Salah satu aspek utama adalah integrasi model *ensemble learning* dengan perangkat jaringan seperti MikroTik dan IDS agar dapat berfungsi secara optimal. Hingga saat ini, penelitian yang membahas integrasi langsung antara model *ensemble learning* dan MikroTik masih terbatas, terutama dalam hal bagaimana aturan *Firewall* dapat dikendalikan secara otomatis berdasarkan prediksi yang diberikan oleh model *machine learning.*

Selain itu, proses otomatisasi dalam penerapan kebijakan *Firewall* berdasarkan hasil prediksi model *machine learning* juga masih menjadi tantangan. Saat ini, sebagian besar solusi IDS berbasis *machine learning* hanya berfungsi sebagai sistem deteksi dan belum terintegrasi secara langsung dengan *Firewall* untuk melakukan mitigasi serangan secara otomatis. Beberapa penelitian menunjukkan

bahwa meskipun model *machine learning* dapat meningkatkan akurasi deteksi, mekanisme otomatisasi dalam merespons ancaman secara langsung melalui perangkat seperti MikroTik masih belum banyak dieksplorasi. Dalam konteks efisiensi penggunaan sumber daya komputasi dan skalabilitas, implementasi *ensemble learning* sering kali memerlukan daya komputasi yang tinggi, yang dapat menjadi kendala saat diterapkan pada perangkat jaringan dengan sumber daya terbatas. Oleh karena itu, diperlukan pendekatan yang tidak hanya efektif dalam mendeteksi serangan, tetapi juga efisien dalam konsumsi sumber daya dan kompatibel dengan infrastruktur jaringan yang ada.

Dengan mempertimbangkan tantangan tersebut, penelitian ini bertujuan untuk merancang sistem keamanan jaringan berbasis *ensemble learning* yang terintegrasi dengan MikroTik dan IDS. Sistem ini diharapkan dapat mendeteksi dan memitigasi serangan *DDoS* secara efektif dengan pendekatan berbasis kecerdasan buatan yang lebih fleksibel dan cepat dalam merespons ancaman. Dengan demikian, penelitian ini akan memberikan kontribusi dalam meningkatkan keamanan jaringan, khususnya dalam menghadapi ancaman *DDoS* yang semakin kompleks.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini, Bagaimana cara mengintegrasikan model *ensemble machine learning* dengan perangkat jaringan MikroTik dan IDS untuk mendeteksi dalam mitigasi serangan *DDoS* ?

1.3 Ruang Lingkup Penelitian

Penelitian ini berfokus pada perancangan dan implementasi sistem keamanan jaringan untuk mitigasi serangan *DDoS* dengan menggunakan pendekatan *ensemble machine learning*. Ruang lingkup penelitian ini mencakup:

1. Integrasi model *machine learning* dengan MikroTik dan IDS sebagai sistem keamanan jaringan.

2. Pengujian performa sistem dalam mendeteksi dan memitigasi serangan *DDoS* pada jaringan simulasi, khususnya serangan *SYN Flood* sebagai salah satu jenis serangan yang akan digunakan dalam pengujian.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk, Membangun sistem keamanan jaringan berbasis *ensemble machine learning* dengan mengintegrasikan MikroTik dan IDS untuk mendeteksi serta memitigasi serangan *DDoS* dalam lingkungan jaringan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Menghasilkan sistem keamanan jaringan yang mampu mendeteksi dan memitigasi serangan *DDoS* dengan tingkat akurasi yang lebih baik.
2. Menyediakan solusi keamanan jaringan yang dapat diintegrasikan dengan MikroTik dan IDS, sehingga dapat diterapkan secara praktis oleh administrator jaringan
3. Menghasilkan sistem keamanan jaringan yang otomatis dan efisien dalam mendeteksi serta merespons serangan *DDoS*, sehingga mengurangi penanganan secara manual.