# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang Masalah

Kemajuan teknologi komputer dan informasi telah mengubah cara komunikasi massa dengan dampak sosial dan politik yang signifikan. Di era *modern*, orang bergantung pada perangkat digital yang memungkinkan siaran terpadu berbasis teks, audio, dan video melalui berbagai aplikasi. Ketergantungan ini menimbulkan risiko baru bagi keamanan siber individu, kelompok, dan negara [1]. Ketika teknologi informasi berkembang, perlu memahami komunikasi data, yang terjadi ketika data digital dikirim dan diterima antara perangkat melalui media komunikasi data [2].

Banyak industri, termasuk pemerintahan, telah terkena dampak teknologi, terutama internet, dalam hal ini. Keberadaan sistem dan kemampuan untuk mencegah serangan siber sangat penting untuk keamanan negara karena orang-orang yang ingin menyalahgunakan data digital [3]. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) trafik anomali serangan siber Indonesia tahun 2023 mencapai 403.990.813 anomali. Trafik anomali dapat mengakibatkan penurunan kinerja perangkat dan jaringan, pencurian informasi sensitif, serta merusak reputasi dan kepercayaan terhadap suatu organisasi [4].


Gambar 1. 1 Grafik Trafik Anomali Serangan Siber di Indonesia Tahun 2023

Gambar 1.1 menunjukkan anomali trafik Indonesia sepanjang tahun 2023 akibat serangan siber. Grafik mengalami kenaikan dan penurunan setiap bulan.

Namun, pada bulan Agustus 2023, terjadi peningkatan signifikan dengan 78.464.385 anomali, dan pada bulan November, terjadi penurunan signifikan dengan 19.296.439 anomali[4].

Keamanan siber harus diprioritaskan karena ketergantungan manusia pada teknologi, khususnya internet, menciptakan celah baru bagi ancaman keamanan negara[3]. Kejahatan siber adalah serangkaian kejahatan terorganisir yang menyerang dunia maya dan keamanan siber. Kejahatan siber mencakup aktivitas kriminal yang dilakukan menggunakan komputer dan Internet, seperti mengakses komputer secara ilegal, mengakses sistem komputer yang mengirimkan data komputer, atau mengakses komputer melalui cara lain yang memungkinkan orang mengakses data komputer[5].

Contoh kasus *Distributed Denial of Service* (DDoS) yang pernah terjadi yaitu adalah serangan Mirai Botnet yang terjadi pada tahun 2016. Serangan DDoS ini menargetkan ke DNS *Dyn* yang menyebabkan gangguan besar pada layanan seperti *Twitter, Spotify dan Netflix*. Serangan ini memanfaatkan perangkat *Internet of Things* (IoT) yang memiliki keamanan lemah sebagai sumber lalu lintas serangan *[6]*. Kemudian serangan DDoS juga melakukan penyerangan kepada *GitHub* pada tahun 2018 dengan lalu lintas serangan mencapai 1,35 *terabit* per detik (Tbps) [7]. Serangan terbesar lainnya terjadi pada tahun 2020, di mana *Amazon Web Services* (AWS) mengalami serangan DDoS dengan puncak mencapai 2,3 Tbps, menjadikannya serangan terbesar dalam sejarah layanan AWS. Serangan DDoS yang dialami oleh AWS menggunakan *server web Connection-less Lightweight Directory Access Protocol* (CLDAP) [8].

Berdasarkan masalah keamanan siber diatas, diperlukan pemanfaatan *integrasi antara Software Defined Network* dan *Intrusion Detection Prevention System* (IDPS). Dengan menggabungkan keduanya, diharapkan dapat memperkuat keamanan jaringan terhadap ancaman siber. SDN mengatur jaringan melalui pengontrol terpusat yang berada di bidang kontrol, sementara bidang data yang terdiri dari *switch* akan meneruskan paket ke titik keluar yang ditentukan[9]. Untuk memastikan keamanan jaringan yang optimal, IDPS bertugas untuk memantau, mendeteksi, dan menghentikan ancaman serangan secara *real-time* serta memberikan peringatan kepada administrator tentang potensi serangan[10].

Salah satu ancaman siber yang umum terjadi yaitu *Distributed Denial of Service* (DDoS) yaitu serangan yang menghentikan layanan *server* secara terus-menerus secara permanen maupun sementara pada aplikasi atau *website* dengan cara membanjiri permintaan melalui *botnet* secara bersama yang dapat merusak sistem. Serangan ini menyebabkan layanan tidak dapat diakses oleh pengguna dan menimbulkan kerugian. Dua bentuk umum dari serangan ini adalah *ICMP Flood* dan *SYN Flood* yang menyerang pada *network layer* dan *transport layer*. Oleh karena itu, kedua jenis serangan ini dipilih dalam penelitian sebagai skenario pengujian untuk dianalisis efektivitas integrasi SDN dan IDPS dalam mendeteksi serta mitigasi serangan[11] .

Penelitian ini berfokus pada analisis efektivitas integrasi SDN dan IDPS dalam meningkatkan keamanan jaringan terhadap serangan DDoS. Dengan melakukan simulasi serangan *ICMP Flood* dan *SYN Flood* menggunakan *OpenDayLight* sebagai *SDN Controller* dan *Suricata* sebagai IDPS, penelitian ini bertujuan untuk mengevaluasi sejauh mana sistem dapat mendeteksi dan mencegah serangan yang terjadi. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan strategi mitigasi serangan DDoS yang lebih optimal

Berdasarkan latar belakang masalah diatas, maka peneliti akan melakukan penelitian yang berfokus pada efektivitas SDN dengan integrasi IDPS dengan judul penelitian **"Analisis Efektivitas Integrasi *Intrusion Detection Prevention System* (IDPS) Dan *Software-Defined Networking* (SDN) Dalam Keamanan Jaringan"**.

## 1.2. Rumusan Penelitian

Berdasarkan latar belakang diatas, maka rumusan masalah pada penelitian ini yaitu pada penelitian ini akan mengukur dampak penggunaan IDPS dan SDN melalui pendekatan *Quality of Service* (QoS) yang terdiri dari *throughput, delay*, *jitter* dan *packet loss* ketika dilakukan serangan *Distributed Denial of Service* (DDoS) antara lain ICMP *Flood* dan SYN *Flood.*

## 1.3. Pertanyaan Penelitian

Pertanyaan dari penelitian ini antara lain:

1. Bagaimana efektivitas SDN dan IDPS dalam mencegah Serangan DDoS yang meliputi ICMP *Flood* dan SYN *Flood* dengan analisis yang mencakup *Quality of Service* (QoS)?

## 1.4. Batasan Masalah

Berdasarkan rumusan masalah dan tujuan dari penelitian, maka terdapat beberapa batasan masalah pada penelitian ini adalah sebagai berikut:

1. Penelitian ini berfokus pada analisis keamanan jaringan dengan menggunakan integrasi SDN dan IDPS.
2. Penelitian ini menggunakan *tools Suricata* untuk mendeteksi serangan jaringan.
3. Jenis Serangan DDoS yang digunakan yaitu serangan *ICMP Flood* dan *SYN Flood.*
4. Penelitian dilakukan secara virtual yang menggunakan simulasi komputer dan kemudian akan diujikan dengan serangan *DDoS.*
5. Sistem operasi yang digunakan dalam penelitian ini menggunakan *Linux Ubuntu* dan Windows untuk menjalankan *tools* dan simulasi.
6. Penilaian analisis dengan menggunakan *Quality of Service* (QoS) yang meliputi *throughput, delay*, *jitter* dan *packet loss.*

## 1.5. Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain:

1. Menerapkan intergrasi antara *Intrusion Detection Prevention* (IDPS) dan *Software-Defined Network* (SDN) untuk mendeteksi dan mencegah ancaman siber dalam keamanan jaringan.
2. Menilai efektivitas integrasi SDN dan IDPS dalam meningkatkan keamanan jaringan dengan melakukan analisis terhadap parameter *QoS* yang terdiri dari penilaian *throughput, delay*, *jitter* dan *packet loss.*

## 1.6. Manfaat Penelitian

Adapun manfaat dari penelitian adalah sebagai berikut:

a. Menambah wawasan dan pengetahuan dibidang keamanan jaringan khususnya integrasi SDN serta IDPS.
b. Menambah pengalaman peneliti dalam melakukan penelitian eksperimental dan simulasi di bidang keamanan jaringan.
c. Menyediakan hasil penelitian yang dapat digunakan untuk referensi penelitian selanjutnya.