BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan *Internet of Things* (IoT) membawa perubahan dalam kehidupan manusia sehari-hari, contohnya dalam penerapan sistem Rumah pintar *(Smart Home)*. Implementasi teknologi IoT pada sistem *Smart Home* memungkinkan berbagai perangkat seperti kamera pengawas, sensor pintu, dan lampu pintar, untuk saling terhubung dan dapat dikendalikan melalui jaringan internet. Dengan adanya teknologi ini, pengguna dapat mengontrol dan memantau kondisi rumah mereka dari jarak jauh, sehingga meningkatkan kenyamanan dan efisiensi dalam kehidupan sehari-hari.

Namun, penggunaan sistem IoT juga menghadapi tantangan besar dalam keamanan jaringan. Dalam hal ancaman, serangan jaringan dan ancaman *malware* merupakan risiko utama yang dihadapi oleh perangkat IoT. Penyerang dapat memanfaatkan kerentanan keamanan di atas untuk mengendalikan perangkat secara jarak jauh, mencuri data, atau melancarkan serangan penolakan layanan [1].

Perangkat keamanan pintar memperkenalkan kelas baru komputer ke lingkungan kerja dan rumah, namun tampaknya tidak ada tingkat pemahaman yang serupa terkait ancaman yang terkandung di dalamnya [2]. Serangan umum pada IoT seperti *DDoS Attack*, di mana server atau perangkat ditargetkan dengan lalu lintas data berlebihan sehingga menyebabkan gangguan layanan. Ancaman keamanan terhadap IoT tidak hanya terjadi pada lingkungan rumah, tetapi juga telah menjadi perhatian serius pada sektor publik. Hal ini diperkuat oleh hasil tinjauan komprehensif terhadap 16 artikel ilmiah terkait ancaman IoT dari tahun 2020 hingga 2024. Data menunjukkan bahwa sekitar 37% studi penelitian berfokus pada serangan *Denial-of-Service* (DoS), 31% membahas serangan *Malware*, dan 19% fokus pada *Phishing*. Tingginya persentase serangan DoS (37%) mengonfirmasi bahwa upaya pelumpuhan layanan merupakan ancaman paling dominan yang dapat menyebabkan gangguan fatal pada operasional perangkat IoT [3]. Untuk mengatasi masalah ini, diperlukan sistem keamanan yang mampu mendeteksi dan merespons ancaman secara real-time. *Intrusion Detection System* (IDS) berbasis *Snort* adalah salah satu solusi yang dapat digunakan untuk memantau lalu lintas jaringan IoT dan

mendeteksi aktivitas mencurigakan. IDS akan bekerja dengan menganalisis paket data yang masuk ke server, mendeteksi pola serangan, dan memberikan peringatan jika terjadi aktivitas anomali.

Dalam penelitian ini, IDS *Snort* akan diterapkan pada *Virtual Private Server* (VPS) untuk mengamankan jaringan IoT *Smart Home*. Server VPS dipilih karena memberikan fleksibilitas dalam pengelolaan keamanan jaringan dibandingkan perangkat fisik seperti Raspberry Pi. Dengan kombinasi IDS *Snort*, sistem IoT berbasis NodeMCU ESP32-CAM, Sensor PIR, dan Bot Telegram, penelitian ini bertujuan untuk membangun sistem keamanan yang tangguh, mampu mendeteksi serangan, serta memberikan peringatan dini terhadap ancaman yang terjadi pada lalu lintas jaringan IoT *Smart Home*.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, rumusan masalah yang diangkat pada penelitian ini adalah :

1. Bagaimana cara mengimplementasikan dan mengonfigurasi *Snort* sebagai *Intrusion Detection System* (IDS) untuk memantau lalu lintas data dari perangkat IoT menuju server VPS?
2. Bagaimana kemampuan Snort dalam mendeteksi serangan DDoS yang ditujukan pada *endpoint* API VPS?.
3. Bagaimana dampak serangan DDoS terhadap performa pengiriman data dan transmisi gambar dari NodeMCU ESP32-CAM menuju server?.

1.3. Batasan Penelitian

Agar masalah yang dibahas lebih terarah dan mencapai pemecahan masalah yang optimal, maka perlu dibuat suatu pembatasan masalah, di antaranya :

1. IDS yang digunakan dalam penelitian ini hanya berbasis *Snort* sebagai mesin deteksi utama dalam memantau lalu lintas jaringan.
2. Perangkat keras yang digunakan dalam penelitian ini terbatas pada NodeMCU ESP32-CAM dan Sensor PIR (*Passive* Infrared) sebagai perangkat pengambilan data.
3. Pengujian keamanan difokuskan pada serangan *DDoS (Distributed Denial*

of Service) Attack terhadap endpoint API *Virtual Private Server* (VPS).

4. Sistem akan diuji dalam lingkungan terbatas dengan jumlah perangkat dan lalu lintas jaringan yang dikontrol.
5. Evaluasi sistem akan berfokus pada deteksi IDS *Snort* dan efektivitas mitigasi serangan, tanpa membahas aspek konsumsi daya atau efisiensi energi perangkat IoT.

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dikemukakan, maka tujuan penelitian ini adalah sebagai berikut :

1. Mengimplementasikan IDS berbasis *Snort* pada VPS, untuk memonitor dan menganalisis lalu lintas jaringan IoT.
2. Menganalisis kemampuan IDS *Snort* dalam mendeteksi dan memberikan peringatan terhadap aktivitas dan serangan jaringan yang terjadi secara real-time berdasarkan log *alert* yang dihasilkan.
3. Mengevaluasi efektivitas IDS dalam mendeteksi dan merespons ancaman keamanan terhadap jaringan IoT, yang diukur ketika berada dalam kondisi lalu lintas normal maupun saat terjadi serangan berdasarkan log *alert* dan notifikasi integrasi bot telegram yang dihasilkan.

Dengan demikian, hasil penelitian ini diharapkan dapat menjadi kontribusi nyata dalam peningkatan keamanan jaringan IoT.

1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat menjadi manfaat dari berbagai aspek, antara lain :

1. Manfaat Bagi Penulis
   - Menambah wawasan dan keahlian praktis dalam mengkonfigurasi sistem keamanan jaringan menggunakan snort
   - Memahami korelasi antara kerentanan jaringan pada sisi server (*Cloud*) dengan fungsionalitas perangkat keras (IoT)
2. Manfaat Bagi Akademis
   - Menjadi referensi bagi penelitian selanjutnya dibidang keamanan

Internet of Things (IoT) dan pertahanan server terhadap serangan *DDoS*.

- Memberikan data empiris mengenai dampak serangan *DDoS* terhadap transmisi data gambar pada perangkat mikrokontroler dengan sumber daya terbatas.

3. Manfaat Bagi Umum
    - Memberikan gambaran mengenai solusi keamanan yang relatif terjangkau untuk melindungi sistem monitoring berbasis IoT.
    - Membantu pengembangan sistem IoT dalam membangun infrastruktur yang lebih tahan banting terhadap serangan yang bertujuan melumpuhkan layanan.