201910370311084
Sadewa
Prodi Informatika

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Internet of Things (IoT) adalah konsep yang menggabungkan berbagai sensor dan perangkat elektronik yang terhubung oleh internet. Hal ini memungkinkan perangkat-perangkat tersebut untuk berkomunikasi, mengendalikan, menghubungkan, dan bertukar data[1]. Pengumpulan, analisis, dan berbagi data secara real-time memungkinkan teknologi ini membangun sistem yang lebih cerdas dan efektif[2]. Dari aplikasi industri yang canggih hingga otomatisasi rumah dan pemantauan lingkungan, Internet of Things telah berdampak besar pada banyak aspek masyarakat. IoT adalah komponen kunci dalam transformasi digital banyak industri, termasuk perawatan kesehatan, transportasi, dan pertanian, karena kapasitasnya untuk merampingkan prosedur dan meningkatkan produksi[3].

Meningkatnya jumlah perangkat IoT yang terhubung pada jaringan internet, banyak perangkat IoT dirancang tanpa mempertimbangkan aspek keamanan, sehingga rentan terhadap serangan siber seperti firmware yang tidak diperbarui, sistem keamanan yang lemah, dan data yang tidak terenkripsi dengan baik[4]. Celah keamanan membuat perangkat IoT rentan terhadapat serangan siber, seperti serangan malware, Denial of Service (DoS) yang memanfaatkan perangkat tidak aman untuk membentuk botnet, dan pencurian data melalui Man in-the-Middle[5]. Serangan tersebut memiliki risiko yang terjadi ke jaringan IoT yang dapat menyebabkan berbagai kerusakan, mulai dari pencurian data pribadi, gangguan layanan, hingga pelanggaran privasi yang serius . Oleh karena itu, deteksi dini dan akurat sangat penting untuk menjaga integritas dan keamanan jaringan IoT[4].

Penanganan celah keamanan pada Internet of Things (IoT) memerlukan pendekatan komprehensif dan berlapis untuk melindungi perangkat dan jaringan dari ancaman. Langkah-langkah penting mencakup penerapan enkripsi

data dengan protokol seperti AES untuk melindungi informasi sensitif dengan bentuk data bukan lagi plain teks melainkan cipher teks, serta AES dirancang untuk mengoptimalkan kinerja pada perangkat dengan sumber daya terbatas[6]. Firewall, sistem deteksi intrusi, dan pemantauan lalu lintas jaringan yang dalam waktu bersamaan juga mencegah lalu lintas data yang tidak aman untuk masuk di dalam jaringan[7]. sementara pembaruan perangkat lunak secara rutin menjadi kunci dalam menutup celah keamanan akibat patch yang belum diterapkan. Kebijakan kata sandi ketat, kontrol akses yang memadai, dan edukasi pengguna juga penting untuk menangkal serangan siber dan pencurian data[8]. Dengan langkah-langkah ini, ekosistem IoT dapat lebih terlindungi dari ancaman siber yang terus berkembang.

Berbagai solusi telah dikembangkan untuk meningkatkan keamanan IoT, seperti metode untuk memastikan kerahasiaan dan autentikasi data, kontrol akses dalam jaringan, serta perlindungan privasi dan kepercayaan antara pengguna dan perangkat. Namun, meskipun mekanisme ini sudah diterapkan, jaringan IoT tetap rentan terhadap berbagai jenis serangan. Oleh karena itu, diperlukan sistem keamanan yang lebih spesifik, seperti Intrusion Detection System (IDS), yang dirancang untuk mendeteksi dan merespons ancaman secara lebih efektif dalam ekosistem IoT[9]. Model proses IDS memiliki tiga fungsi dasar, yaitu: pemantauan dan pengumpulan data, analisis untuk mendeteksi ancaman, serta memberikan respon atau notifikasi kepada administrator[10]. Secara umum, IDS terbagi menjadi dua kelompok utama, yaitu *Signature-based* dan *Anomaly based*[11]. Intrusi yang dilakukan oleh pihak yang tidak memiliki otorisasi (cracker) atau penyalahgunaan hak akses oleh pengguna internal (insider threat) dapat dideteksi oleh IDS. Meskipun IDS tidak berfungsi untuk mencegah serangan, sistem ini membantu meminimalkan dampak serangan dan gangguan pada jaringan dengan memberikan alert/peringatan kepada administrator, yang memungkinkan untuk segera mengambil langkah mitigasi[12].

Berdasarkan pada latar belakang tersebut maka dalam penelitian ini berfokus pada penerapan Intrusion Detection System (IDS) berbasis signature

untuk meningkatkan keamanan jaringan perangkat Internet of Things (IoT). Dalam penelitian ini, digunakan Snort, salah satu IDS paling populer yang menerapkan metode deteksi berbasis *Signature-based*, untuk mengidentifikasi serangan yang dikenal, Snort dapat menganalisis lalu lintas jaringan dan mendeteksi pola-pola serangan secara real-time. serta memberikan respons cepat terhadap aktivitas mencurigakan. Penelitian ini menekankan pentingnya pembaruan database secara berkala untuk menjaga efektivitas deteksi dan merekomendasikan integrasi Snort dengan sistem pemantauan lainnya untuk meningkatkan keamanan secara keseluruhan dalam ekosistem IoT.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Teknik apa yang dapat diterapkan untuk meningkatkan keamanan jaringan IoT dari ancaman siber?
2. Bagaimana implementasi sistem pendeteksi intrusi berbasis signature pada jaringan IoT menggunakan Snort?
3. Sejauh mana sistem pendeteksi intrusi dapat mendeteksi dan merespon ancaman pada jaringan IoT?

## 1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menganalisis celah keamanan dalam jaringan Internet of Things (IoT) serta bagaimana sistem pendeteksi intrusi dapat membantu mengatasinya.
2. Mengimplementasikan sistem pendeteksi intrusi berbasis signature menggunakan Snort untuk meningkatkan keamanan jaringan IoT.
3. Menganalisis sistem pendeteksi intrusi dari tingkat akurasi deteksi, mengamati penggunaan CPU dan Memori pada *gateway*, dan efektivitas dalam mengurangi false positive.

## 1.4 Batasan Masalah

Dalam penelitian ini, untuk menjaga fokus dan kejelasan, beberapa batasan masalah ditetapkan sebagai berikut:

1. Penelitian hanya membahas sistem pendeteksi intrusi menggunakan metode signature-based detection. Tidak membahas metode lain seperti anomaly based detection secara mendalam.
2. Penerapan sistem pendeteksi intrusi hanya dibatasi pada penggunaan ESP32 sebagai node sensor yang terhubung pada raspberry sebagai gateway-nya. Tidak mencakup seluruh jenis IoT secara luas, melainkan hanya pada beberapa skenario spesifik.
3. Penelitian ini mengamati berdasarkan tingkat akurasi deteksi, penggunaan CPU dan Memory pada *gateway* saat kondisi normal, dan pada saat terjadi penyerangan, efektivitas dalam mengurangi false positive. Tidak membahas aspek keamanan IoT secara keseluruhan.

## 1.5 Sistematik Penulisan

Sub bab ini menjelaskan mengenai struktur penulisan laporan tugas akhir yang akan dilakukan jika proposal diterima oleh Dewan Penguji.

Sistematika penulisan laporan penelitian ini disusun menjadi beberapa bab sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi pendahuluan yang menjelaskan latar belakang, perumusan masalah, tujuan, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi mengenai kajian pustaka sebagai parameter rujukan untuk dilaksanakannya penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang tahapan desain penelitian, kerangka, dan konsep penelitian yang digunakan untuk menyelesaikan permasalahan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai implementasi, pengujian, hasil penelitian serta pembahasan mengenai hasil penelitian. pengujian membuat implementasi meliputi implementasi sistem dan implementasi aplikasi, hasil pengujian aplikasi.

BAB V PENUTUP

Bab ini berisikan kesimpulan dari sistem yang dibuat serta saran untuk kepentingan lebih lanjut.