BAB II

TINJAUAN PUSTAKA

2.1 Internet of Things (IoT)

Internet of Things (IoT) adalah sistem untuk menghubungkan perangkat komputer, mesin mekanik dan digital, objek, atau individu dengan sistem identifikasi unik (UID) untuk mengirimkan data tanpa memerlukan interaksi manusia-ke-manusia atau komputer-ke-manusia. Intinya, IoT menghubungkan manusia dan komputer dengan objek yang dapat diberi alamat IP dan mengirimkan data melalui jaringan[13].

1. Konektivitas: IoT terdiri dari berbagai jaringan perangkat yang terhubung, yang mengumpulkan data dan berbagi informasi tentang cara mereka beroperasi dan melakukan tugas.
2. Sensor: Sensor tertanam di perangkat, termasuk ponsel dan perangkat elektronik lainnya, dan mengirimkan data ke jaringan IoT.
3. Otomatisasi: Perangkat IoT melakukan sebagian besar pekerjaan tanpa campur tangan manusia, meskipun manusia dapat berinteraksi dengan perangkat untuk konfigurasi, instruksi, atau akses data.
4. Analisis Data: Data sensor dikirim ke cloud atau dianalisis di tempat untuk analisis data.

2.2 Keamanan IoT dan Tantanganya

Meskipun IoT memberikan banyak manfaat dan berbagai kemudahan, perangkat IoT juga memiliki tantangan besara dalam hal sistem keamanan. Menurut jurnal “Keamanan dan Keselamatan Implementasi Internet of Things (IoT): Tantangan pada Sektor Industri dan Rumah Tangga” Perangkat IoT memiliki beberapa tantangan utama meliputi[14] :

1. Kerentanan terhadap Serangan Siber: Perangkat IoT rentan terhadap serangan siber seperti peretasan, pencurian data, atau pemanfaatan perangkat sebagai bagian dari serangan botnet.

2. Penyalahgunaan Data Pribadi: Banyak perangkat IoT mengumpulkan data pribadi yang sensitif, yang dapat dengan mudah diekspos jika tidak dilindungi dengan baik.
3. Kurangnya Kesadaran Pengguna: Pengguna perlu lebih berhati-hati dalam mengamankan perangkat mereka, seperti penggunaan kata sandi yang kuat, pengaturan jaringan yang aman, dan pembaruan perangkat lunak yang rutin.

2.3 Ancaman Keamanan pada Jaringan IoT

Internet of Things (IoT) membawa manfaat besar dalam berbagai bidang, namun juga menghadirkan ancaman keamanan pada jaringan IoT yang menjadi perhatian serius seiring dengan meningkatnya kompleksitas dan kerentanan sistem. Berdasarkan tinjauan literatur komparatif, jaringan IoT rentan terhadap berbagai serangan, seperti Denial-of-Service (DoS), Man-in-the-Middle (MITM), phishing, dan malware. Serangan-serangan ini dapat mengancam privasi dan keamanan pengguna dengan memanfaatkan kerentanan pada jaringan IoT, yang meliputi data, protokol, ukuran, komunikasi, dan standar yang beragam[15].

2.4 Sistem Deteksi Intrusi

Intrusion Detection System (IDS) adalah sistem deteksi dini jika terjadi serangan jaringan komputer. IDS akan memberitahu administrator jaringan komputer jika terjadi serangan pada jaringan komputer. IDS juga mencatat semua upaya dan aktivitas yang bertujuan mengganggu jaringan komputer dan serangan jaringan komputer lainnya[16]. Ada dua jenis IDS yaitu:

1. Network-Based IDS (NIDS): Network Intrusion Detection Systems (NIDS) adalah alat penting untuk mendeteksi dan mengurangi serangan siber berbasis jaringan. NIDS ditempatkan pada titik-titik strategis di dalam jaringan IoT untuk memantau lalu lintas[17].
2. Host-Based IDS (HIDS): Host-Based Intrusion Detection Systems (HIDS) merupakan sistem deteksi serangan yang dipasang langsung pada server untuk memantau aktivitas jaringan dan keamanan file[17], [18].

2.5 Teknik dan Metode Deteksi Intrusi

Sistem Deteksi Intrusi (Intrusion Detection System- IDS) digunakan untuk mengidentifikasi aktivitas mencurigakan atau serangan terhadap jaringan dan perangkat IoT. IDS dapat mendeteksi pola serangan yang telah dikenal maupun anomali yang tidak biasa dalam lalu lintas jaringan. Terdapat dua pendekatan utama dalam deteksi intrusi, yaitu Signature-Based Detection, dan Anomaly Based Detection[19].

1. Signature-Based: Teknik signature-based mengandalkan pola-pola serangan yang telah diketahui untuk mengidentifikasi aktivitas yang tidak diinginkan, membuatnya efektif dalam mendeteksi ancaman yang sudah dikenal dan terklasifikasi.
2. Anomaly-Based: Teknik anomaly-based menggunakan aturan-aturan untuk mengidentifikasi aktivitas yang tidak sesuai dengan pola normal yang telah ditentukan, sehingga lebih unggul dalam menangani intrusi yang tidak terdeteksi oleh signature-based, meskipun sering menghasilkan lebih banyak false positive.

2.6 Snort

Snort adalah aplikasi keamanan jaringan open *source* yang digunakan untuk mendeteksi adanya percobaan serangan atau aktivitas mencurigakan pada jaringan komputer. Snort bekerja dengan cara melihat lalu lintas jaringan secara *real time* dan paket log untuk melakukan analisis Snort mampu mengidentifikasi berbagai jenis ancaman seperti DoS, hingga percobaan eksploitasi. Informasi yang terkumpul kemudian digunakan untuk memberikan alert kepada administrator serta mendukung proses evaluasi keamanan dan autentikasi pada sistem[20].

2.7 Penelitian Terdahulu

Penelitian ini mengacu pada studi sebelumnya, tentang pembahasan implementasi pendeteksi intrusi pada IoT dengan tujuan untuk mengumpulkan informasi, data, temuan, serta konsep yang telah dikembangkan dan

dipublikasikan dalam literatur ilmiah. Maka dari itu penulis melakukan *review* untuk dijadikan acuan dalam penelitian seperti pada tabel 1 berikut.

Tabel 1 *Penelitian Terdahulu*

No	Judul Penelitian	Peneliti	Pembahasan Utama	Hasil
1.	Pemanfaatan Kerangka Kerja Investigasi Forensik Jaringanuntuk Identifikasi Serangan Jaringan Menggunakan Sistem DeteksiIntrusi (2022)	Abdul Khalid,Sri Novida Sari	Jurnal tersebut membahas tentang pemanfaatan kerangka kerja investigasi forensik jaringan untuk mengidentifikasi serangan jaringan menggunakan Sistem Deteksi Intrusi (IDS). Penelitian ini menggunakan Network Forensic Investigation Framework yang diusulkan untuk melakukan simulasi jaringan, analisis, dan investigasi dalam menentukan jenis serangan jaringan komputer.	Hasil penelitian menunjukkan bahwa kerangka kerja ini memfasilitasi proses investigasi ketika terjadi serangan jaringan dan efektif digunakan ketika jaringan komputer memiliki aplikasi dukungan keamanan jaringan seperti IDS. IDS juga efektif dalam mendeteksi aktivitas pemindaian jaringan dan serangan DOS.

No	Judul Penelitian	Peneliti	Pembahasan Utama	Hasil
2	Penggunaan Metode Signature Based Dalam Pengenalan Pola Serangan di Jaringan Komputer (2021)	Herri Setiawan, M.Agus Munandar, Lastri Widya Astuti	Pengenalan pola serangan jaringan penting untuk administrator dalam penanganan gangguan. Intrusion Detection System (IDS) adalah solusi yang dapat digunakan karena kemampuannya mendeteksi serangan secara real-time. Penelitian ini menerapkan metode signature based dalam simulasi untuk mengidentifikasi paket data berbahaya dan menguji akurasi deteksi dengan berbagai rule.	penelitian ini menunjukkan bahwa metode signatured based efektif dalam mengenali pola serangan jaringan dan dapat diimplementasikan dalam sistem IDS dengan tampilan monitoring berbasis web untuk membantu administrator dalam mendeteksi dan menangani serangan.
3	Implementation of signature	Pahala Bima	Jurnal tersebut membahas tentang	Penelitian ini membuktikan

No	Judul Penelitian	Peneliti	Pembahasan Utama	Hasil
	based intrusion detection system using SNORT to prevent threats in network servers(2022)	Pramudya, Alamsyah	implementasi sistem deteksi intrusi (IDS) berbasis tsignature based menggunakan SNORT untuk mencegah ancaman pada server jaringan. Penelitian ini menggunakan dataset MIT-DARPA 1999 untuk menguji sistem dalam mendeteksi serangan seperti Network Scanning dan DoS (Denial of Services).	kinerja tinggi SNORT dengan kecepatan 83,494 paket/detik, true positive 100%, dan akurasi 98.10%. Pengujian menggunakan dataset MIT-DARPA 1999 menunjukkan keandalannya dalam mendeteksi Network Scanning dan DoS dalam jaringan kompleks.
4	Meningkatkan Keamanan Siber dalam Lingkungan Internetof Things (IoT) dengan	Richard Parlindungan Simanjuntak,Ramson Rikson Maruwahal	Jurnal tersebut membahas tentang peningkatan keamanan siber dalam lingkungan Internet of Things (IoT) dengan	Hasil penelitian jurnal tersebut menunjukkan bahwa sistem deteksi intrusi berbasis machine learning mampu

No	Judul Penelitian	Peneliti	Pembahasan Utama	Hasil
	Menggunakan Sistem Deteksi Intrusi Berbasis Pembelajaran Mesin	Sijabat (2024)	menggunakan Sistem Deteksi Intrusi (IDS) berbasis pembelajaran mesin. Penelitian ini bertujuan untuk mengembangkan IDS yang adaptif dan efisien untuk mengidentifikasi dan mencegah serangan siber di lingkungan IoTyang kompleks dan dinamis.	mengenali serangan siber dengan tingkat akurasi yang tinggi dan meminimalkan kerugian yang disebabkan oleh serangan tersebut.
5	Generation for Signature Based Detection Systems of Cyber Attacks in IoT Environments (2019)	YanNaung Soe,Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto, Kouichi Sakurai	Jurnal ini membahas tentang pembuatan aturan (rule generation) untuk sistem deteksi berbasis tanda tangan (signature-based) yang ringan untuk mendeteksi serangan siber di	Hasil penelitian ini menunjukkan bahwa model yang diusulkan berhasil menghasilkan 16 aturan deteksi yang efektif dari 659.015 pola serangan, memungkinkan perangkat IoT

No	Judul Penelitian	Peneliti	Pembahasan Utama	Hasil
			lingkungan IoT yang rentan terhadap serangan botnet. Metode yang diusulkan menggunakan dataset serangan botnet IoT modern dan algoritma machine learning J48 untuk menghasilkan aturan deteksi yang efektif dengan sumber daya terbatas, bertujuan untuk meningkatkan keamanan perangkat IoT dan memperluas kemampuan deteksi pada sistem IDS publik seperti Snort dan Suricata. Penelitian ini berkontribusi pada keamanan IoT	dengan sumber daya terbatas untuk memproses deteksi serangan secara efisien. Aturan yang dihasilkan tidak hanya berguna untuk mengamankan perangkat IoT tetapi juga dapat diperluas untuk meningkatkan kemampuan deteksi pada sistem IDS publik seperti Snort dan Suricata, sehingga memberikan kontribusi signifikan dalam melindungi ekosistem IoT dari ancaman siber.

No	Judul Penelitian	Peneliti	Pembahasan Utama	Hasil
			dengan menyediakan pendekatan untuk menghasilkan aturan deteksi yang efektif dan ringan, yang penting untuk melindungi perangkat IoT dari ancaman siber modern.	

Pada tabel 1, dari jurnal penelitian terdahulu, dapat disimpulkan bahwa sistem deteksi intrusi yang diimplementasikan pada IoT mampu meningkatkan keamanan jaringan dengan mengidentifikasi dan merespons ancaman secara efektif. implementasi *Intrusion Detection System* (IDS) pada gateway jaringan dinilai efektif karena seluruh lalu lintas data dari dan menuju perangkat IoT melewati satu titik terpusat. Gateway berperan sebagai penghubung antara jaringan lokal IoT dan jaringan eksternal, sehingga penempatan IDS pada gateway memungkinkan proses pemantauan, inspeksi paket, dan deteksi serangan dilakukan secara menyeluruh tanpa perlu memasang IDS pada setiap perangkat IoT yang memiliki keterbatasan sumber daya. Pendekatan ini juga mampu mengurangi beban komputasi pada end-device serta meningkatkan efisiensi pengelolaan keamanan jaringan.