BAB I
PENDAHULUAN

Bab I berisikan pendahuluan yang membahas tentang latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian dan luaran dari penelitian. Pendahuluan yang disampaikan pada bab ini menjelaskan secara rinci gambaran umum terkait penelitian yang akan dilakukan.

1.1 Latar Belakang Masalah

Kehadiran konsep *Smart City* yang memanfaatkan teknologi informasi untuk mendukung kehidupan masyarakat semakin mempercepat perkembangan teknologi informasi (Sharif & Pokharel, 2022). Berbagai istilah berkaitan dengan *smart city* yang menggunakan perangkat teknologi informasi muncul, seperti *smart agriculture*, *smart medical*, *smart farming*, *smart home, smart campus* dan lain-lain. Beberapa perangkat yang digunakan pada smart *city* terhubung secara langsung ke Internet digunakan istilah *Internet of Things* (IoT).

Seiring dengan perkembangan teknologi informasi global, ancaman terhadap keamanan sistem informasi juga terus meningkat. Kerugian yang diakibatkan oleh serangan terhadap sistem IoT dan perangkatnya berbeda dengan jaringan tradisional. Apabila kelemahan sistem IoT dieksploitasi, maka dapat menyebabkan kerusakan serius. Akibat yang ditimbulkan tidak hanya merusak sistem informasinya namun juga akan merusak secara fisik (D. Li et al., 2019). Salah satu contoh kasus adalah pada tahun 2017, ketika Maersk, salah satu perusahaan pelayaran terkemuka di dunia, dirusak secara besar-besaran oleh *malware* NotPetya, merugikan bisnis perusahaan tersebut sebesar $250 juta–$300 juta. Pada tahun 2021, JBS, pemasok daging terbesar di dunia, menjadi sasaran serangan ransomware yang memaksanya menutup operasi beberapa layanannya di beberapa negara dan memengaruhi ribuan pekerja (Friha et al., 2022). Laporan Kaspersky menunjukkan lebih dari 100 juta serangan pada perangkat IoT dalam enam bulan pertama tahun 2019, dan sebagian besar adalah serangan Botnet IoT (Nguyen et al., 2022). Salah satu perangkat yang digunakan sebagai botnet oleh penyerang adalah

kamera pintar. Perangkat ini bisa mengirimkan DDoS ke *server* situs web (S. K. Gupta et al., 2022) (De Donno et al., 2018).

Keamanan sistem informasi dibuat agar kerugian yang dialami menjadi berkurang. Salah satu sistem yang dibuat adalah mekanisme peringatan untuk mengetahui adanya pelanggaran keamanan sistem informasi yang dinamakan dengan deteksi intrusi. Deteksi Intrusi adalah proses pemantauan peristiwa yang terjadi dalam sistem komputer atau jaringan dan menganalisisnya untuk pertanda kemungkinan insiden (Scarfone & Mell, 2007). Deteksi intrusi melakukan proses identifikasi perilaku yang mencoba menyerang, menyerang atau telah menyerang sistem (Tidjon et al., 2019).

Deteksi intrusi pada IoT dapat dikelompokkan dalam dua cara yaitu dengan menggunakan statistik dan menggunakan pendekatan *Machine Learning* (ML). Perkembangan kemampuan mesin dibidang kecerdasan buatan kemudian diusulkan menjadi penyelesaian masalah yang lebih baik dalam mendeteksi serangan (Alzahrani et al., 2020). Berbagai metode ML kemudian digunakan untuk meningkatkan kemampuan IDS dalam mendeteksi adanya serangan yang dikenal dan juga yang belum dikenal sebelumnya (H. Liu & Lang, 2019). Namun, dengan meningkatnya kompleksitas struktur jaringan dan keragaman perilaku intrusi, sistem deteksi intrusi yang ada secara bertahap menunjukkan beberapa kelemahan, seperti tingkat positif palsu dan negatif palsu yang tinggi, ekstraksi fitur data yang sulit, dan efisiensi pemrosesan data yang rendah (Wang et al., 2021). Positif palsu terjadi ketika model menyatakan suatu data sebagai positif, padahal sebenarnya negatif. Sementara pada negatif palsu terjadi sebaliknya, model menyatakan suatu data sebagai negatif, padahal sebenarnya positif. Kelemahan ini menjadikan model yang dibangun tidak mendeteksi dengan tepat sesuai yang diharapkan.

Menurut penelitian (Aleesa et al., 2020), teknik deteksi intrusi pada jaringan IoT masih mengalami berbagai kesulitan dan masalah sehingga menghalangi teknik tersebut untuk mendeteksi serangan secara efisien. Di antara masalah tersebut adalah peningkatan volume serangan yang stabil dan ancaman tingkat lanjut yang menyebabkan alarm palsu yang tinggi pada sistem deteksi intrusi jaringan (NIDS). Metode ML klasik juga mengalami berbagai kesulitan di antaranya adalah

kurangnya *dataset* pelatihan berlabel dan keragaman lalu lintas jaringan. Kesulitan yang dihadapi dalam deteksi intrusi tersebut membuat penerapan ML tradisional pada lalu lintas yang besar dan implementasi di jaringan sebenarnya menjadi sulit.

Penelitian (Wang et al., 2021) mengemukakan bahwa untuk mengatasi kekurangan yang dimiliki oleh ML, dapat digunakan metode *Deep Learning* (DL). Perkembangan metode DL kemudian menjadi solusi dalam menangani kendala yang dihadapi oleh ML tradisional. Paling tidak ada dua persoalan yang kemudian dapat diselesaikan dengan menggunakan DL. Pertama DL digunakan sebagai teknik ekstraksi fitur dan kedua sebagai pengklasifikasi serangan. Pada teknik ekstraksi, DL digunakan untuk mempelajari atau melakukan ekstraksi fitur berharga secara otomatis dari data mentah yaitu data yang belum dilakukan proses prapengolahan. Sedangkan pada tahap klasifikasi, DL digunakan dalam membedakan serangan atau tidak serangan (Aleesa et al., 2020).

Penggunaan algoritma *Deep Feedforward Neural Network* (DFNN) sebagai salah satu pengembangan DL dalam menyelesaikan persoalan deteksi intrusi jaringan dapat dilihat pada penelitian (Vigneswaran et al., 2018), DFNN dengan menggunakan 3 lapisan lebih baik dibandingkan dengan algoritma ML. Penelitian (Diro & Chilamkurti, 2018) juga memperlihatkan bahwa DL lebih unggul dibandingkan ML saat digunakan mengevaluasi intrusi pada jaringan dengan nilai akurasi 99.2% sedangkan ML hanya 95.22%. Hasil penelitian (Gamage & Samarabandu, 2020) juga menunjukkan bahwa jaringan *neural feed-forward* (ANN) yang dilatih secara terawasi menunjukkan kinerja baik pada semua metrik (akurasi, *F1-score*, *false negatives*) dan memiliki waktu pelatihan serta inferensi yang efisien dibandingkan dengan model semi-supervised seperti *Autoencoders* dan *Deep Belief Networks*.

Berdasarkan berbagai penelitian yang telah dikaji, DFNN memiliki potensi yang besar untuk dikembangkan sebagai metode deteksi intrusi pada keamanan siber. Penelitian ini memfokuskan pada perangkat kamera IP karena merupakan salah satu perangkat multimedia IoT yang menghasilkan lalu lintas jaringan dalam jumlah besar dan beroperasi secara terus-menerus. Dibandingkan dengan perangkat IoT berbasis sensor, kamera IP memiliki karakteristik komunikasi yang lebih

kompleks akibat proses *streaming* video, penggunaan berbagai protokol jaringan, serta kebutuhan transfer data yang tinggi. Kondisi tersebut menjadikan kamera IP lebih rentan terhadap serangan siber, baik sebagai target serangan maupun sebagai perangkat yang dapat dimanfaatkan sebagai bagian dari botnet untuk menyerang sistem lain (Nguyen et al., 2022). Oleh karena itu, kamera IP dipilih sebagai objek penelitian karena mampu merepresentasikan tantangan keamanan pada lingkungan multimedia IoT yang lebih realistis, kompleks, dan relevan untuk mengevaluasi efektivitas metode DFNN yang diusulkan. Penelitian ini mengusulkan metode *Selective Predictive Attack Detection using Ensemble Hybridization* (SPADEH) sebagai pendekatan *ensemble feature selection* yang dirancang untuk meningkatkan kualitas fitur masukan dan kinerja model DFNN dalam mendeteksi intrusi pada jaringan kamera IP.

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang dan hasil kajian literatur, penelitian ini mengidentifikasi tiga permasalahan utama. Pertama, meningkatnya ancaman siber pada perangkat multimedia IoT, khususnya kamera IP, yang berpotensi mengganggu operasional dan layanan organisasi. Kedua, karakteristik data lalu lintas jaringan yang berdimensi tinggi dan tidak seimbang menyebabkan proses deteksi intrusi menjadi lebih kompleks dan berpotensi menurunkan performa model klasifikasi. Ketiga, sebagian besar penelitian terdahulu masih menggunakan metode seleksi fitur tunggal sehingga belum mampu menangkap berbagai bentuk hubungan yang terdapat dalam data, baik hubungan linear, monotonik, maupun non-linear. Kondisi tersebut menunjukkan perlunya pengembangan pendekatan seleksi fitur yang lebih komprehensif untuk menghasilkan fitur yang lebih representatif dalam mendukung proses deteksi intrusi berbasis *deep learning*. Pengembangan penelitian akan menjawab permasalahan yang akan dicarikan solusinya pada penelitian ini. Permasalahan tersebut adalah :

1. Bagaimana meningkatkan kemampuan DFNN dalam mendeteksi intrusi pada jaringan kamera IP yang memiliki karakteristik data berdimensi tinggi dan tidak seimbang?

2. Bagaimana efektivitas metode SPADEH dalam menghasilkan subset fitur yang representatif untuk meningkatkan performa DFNN pada deteksi intrusi jaringan kamera IP?
3. Bagaimana efektivitas pendekatan *ensemble feature selection* dalam meningkatkan generalisasi model pada dataset publik dan *real-world*?
4. Bagaimana merancang prototipe sistem informasi berbasis web yang dapat mengintegrasikan hasil deteksi intrusi untuk mendukung kebutuhan operasional, manajerial, dan pengambilan keputusan strategis?

1.3 Tujuan Penelitian

Penelitian ini mengembangkan dan mengevaluasi model DFNN dalam mendeteksi intrusi pada jaringan kamera IP, dengan harapan dapat meningkatkan akurasi deteksi, mengurangi *false* alarm, serta mampu mengenali pola serangan baru yang belum teridentifikasi sebelumnya. Adapun tujuan dari penelitian adalah:

1. Menerapkan algoritma *Deep Feedforward Neural Network* (DFNN) untuk mendeteksi intrusi pada lalu lintas jaringan kamera IP serta menganalisis karakteristiknya guna membedakan pola normal dari pola serangan.
2. Mengevaluasi performa model deteksi menggunakan berbagai metrik evaluasi.
3. Mengembangkan metode SPADEH sebagai pendekatan *ensemble feature selection* untuk menghasilkan fitur yang lebih representatif pada deteksi intrusi jaringan kamera IP.
4. Mengembangkan prototipe sistem informasi berbasis web yang mengintegrasikan model deteksi intrusi sebagai sarana pemantauan dan pendukung pengambilan keputusan keamanan jaringan.

1.4 Kebaruan (*Novelty*)

Penelitian ini memiliki kebaruan (*novelty*) pada beberapa aspek penting yang belum banyak dieksplorasi secara terpadu dalam penelitian sebelumnya, yaitu:

1. Integrasi Multi-Metode Seleksi Fitur

   Penelitian ini mengembangkan metode SPADEH yang mengintegrasikan tiga metode statistik dan informasi, yaitu korelasi Pearson, korelasi

Spearman, dan Mutual Information. Pendekatan ini tidak sekadar menggabungkan fitur terpilih, tetapi membangun mekanisme seleksi fitur berbasis keragaman statistik (*statistical diversity*), di mana setiap metode merepresentasikan karakteristik hubungan data yang berbeda.

Berbeda dengan penelitian terdahulu yang umumnya menggunakan satu metode filter atau kombinasi terbatas pada karakteristik statistik tertentu, penelitian ini mengembangkan kerangka *ensemble feature selection* yang mengintegrasikan tiga perspektif hubungan data, yaitu hubungan linear melalui korelasi Pearson, hubungan monotonik melalui korelasi Spearman, dan hubungan non-linear melalui Mutual Information. Pendekatan ini memungkinkan proses seleksi fitur menangkap informasi yang lebih beragam dibandingkan penggunaan satu metode tunggal.

2. Aplikasi pada Jaringan kamera IP

   Penelitian difokuskan pada deteksi intrusi dalam jaringan IoT yang digunakan untuk layanan multimedia, khususnya perangkat kamera IP. Fokus ini masih relatif jarang dibahas secara mendalam, padahal perangkat multimedia memiliki karakteristik lalu lintas data yang berbeda dari sensor IoT biasa, sehingga memerlukan pendekatan deteksi khusus.

3. Optimasi Deteksi Menggunakan DFNN

   Model DFNN digunakan secara spesifik dan di optimasi untuk meningkatkan performa deteksi intrusi. Berbeda dari pendekatan umum, penelitian ini menunjukkan bahwa arsitektur DFNN yang disederhanakan dan difokuskan dengan pemilihan fitur yang tepat mampu memberikan hasil yang kompetitif.

4. Prototipe sistem informasi keamanan siber

   Integrasi model deteksi intrusi berbasis SPADEH-DFNN ke dalam prototipe sistem informasi keamanan siber yang mendukung level operasional, manajerial, dan strategis.

1.5 Manfaat Penelitian

Manfaat yang didapatkan dari penelitian ini adalah sebagai berikut :

1. Penelitian ini diharapkan mampu menjadi rujukan bagi penelitian berikutnya terkait model terbaik yang dapat digunakan pada jaringan kamera IP.
2. Praktisi pertahanan dan keamanan siber dapat memilih model deteksi intrusi terbaik dalam melindungi perangkat dan jaringannya.
3. Pengambil kebijakan di bidang keamanan informasi dapat menggunakan hasil penelitian ini sebagai dasar dalam merumuskan regulasi, standar, atau kebijakan yang mendukung keamanan jaringan kamera IP..
4. Bagi organisasi, penelitian ini menyediakan mekanisme pendukung keputusan *(decision support*) dalam pengelolaan keamanan jaringan kamera IP melalui penyediaan informasi ancaman secara cepat dan akurat. Informasi tersebut dapat digunakan sebagai dasar dalam pengambilan keputusan operasional, taktis, maupun strategis terkait mitigasi risiko keamanan siber.

1.6 Pembatasan Masalah

Penetapan batasan masalah dalam penelitian ini bertujuan untuk mempersempit ruang lingkup pembahasan agar tetap terfokus pada bidang yang diteliti. Berikut ini adalah batasan masalah yang digunakan:

1. Penelitian ini dibatasi pada pengembangan dan evaluasi deteksi intrusi pada jaringan khususnya pada jaringan IoT yang menggunakan layanan kamera IP.
2. Fokus penelitian adalah pada serangan yang umum terjadi dalam konteks jaringan IoT, seperti *denial-of-service* (DoS), *spoofing*, dan *injection*.
3. Data yang digunakan merupakan data eksperimen dan dataset publik yang merepresentasikan lalu lintas jaringan. Data diklasifikasikan sebagai lalu lintas normal dan lalu lintas yang mengandung serangan.

4. Data lalu lintas normal adalah data lalu lintas alami perangkat yang digunakan sementara data lalu lintas yang mengandung serangan diklasifikasikan sebagai intrusi.
5. Dalam disertasi ini, istilah serangan (*attack*) merujuk pada setiap upaya yang bertujuan merusak atau mengakses sistem secara tidak sah, baik berhasil maupun tidak. Sementara itu, intrusi (*intrusion*) merujuk pada kondisi ketika serangan tersebut berhasil sehingga terjadi pelanggaran kebijakan keamanan sistem.
6. Arsitektur jaringan syaraf tiruan yang digunakan dalam penelitian ini adalah *Deep Feedforward Neural Network* (DFNN), perbandingan terhadap arsitektur lainnya dilakukan pada tahap awal untuk menentukan *baseline* model terbaik.
7. Pengukuran performa deteksi intrusi dilakukan dengan metrik akurasi, *false alarm rate*, presisi, *recall*, dan *F1-score*
8. Penelitian ini tidak membahas aspek implementasi keamanan secara menyeluruh di perangkat IoT maupun protokol enkripsi yang digunakan, tetapi hanya fokus pada deteksi dini terhadap anomali atau serangan berdasarkan data jaringan yang masuk.