

# Bab I

## Pendahuluan

### 1.1 Latar Belakang

Pada zaman teknologi sekarang ini, *Intrusion Detection System* (IDS) merupakan hal penting untuk melindungi komputer dan jaringan dari berbagai jenis serangan dan virus yang dapat menimbulkan kerugian, seperti hilangnya suatu data [20]. IDS digunakan oleh *Network Administrator* untuk memantau kondisi jaringan, sehingga dapat mencegah terjadi serangan pada jaringan.

Dikarenakan intrusi dan serangan pada jaringan semakin berkembang setiap tahunnya, maka IDS yang pintar harus digunakan untuk menjaga jaringan tetap aman. Salah satu faktor yang mempengaruhi performa dari IDS adalah klasifikasi serangan yang cepat dan akurat. Metode klasifikasi yang sudah ada saat ini, masih memiliki kelebihan dan kekurangan masing-masing, oleh karena itu, pengembangan metodologi untuk mengatasi kekurangan dari metode klasifikasi yang ada masih terbuka [3].

Pada penelitian sebelumnya, terdapat beberapa metode klasifikasi yang telah melakukan klasifikasi pada data IDS, seperti *Support Vector Machine* (SVM), *Genetic Algorithm* (GA), *K-Nearest Neighbour* (KNN), *Artificial Neural Network* (ANN), *Bayesian Method*, *Decision Tree* dan *Fuzzy Logic* [20].

Menurut [20],[15], dan [2], lambatnya waktu *testing* masih menjadi tantangan untuk penelitian mengenai metode klasifikasi pada IDS. Berdasarkan jurnal tersebut, salah satu metode klasifikasi yang sudah ada pada IDS seperti SVM memiliki kendala pada saat melakukan *training* dan *testing* yang dinilai lambat. Setelah dilakukan studi literatur pada klasifikasi non IDS, ditemukan metode pengembangan dari *Kernel Logistic Regresion* dan mirip dengan metode SVM, yaitu *Import Vector Machine* (IVM). Menurut [13], IVM memiliki waktu komputasi dalam klasifikasi yang lebih cepat dibandingkan SVM. Sehingga metode tersebut patut dianalisis performanya dalam klasifikasi data IDS sehingga dapat mengatasi kekurangan metode sebelumnya.

Penelitian ini dilakukan untuk menguji performa metode IVM dalam klasifikasi data IDS dengan membandingkan metode IVM dengan metode yang umum digunakan dalam klasifikasi. Diharapkan peneltian ini dapat menghasilkan tingkat akurasi yang baik dan waktu *Testing* yang cepat dengan menguji

parameter yang dapat mempengaruhi performa IVM.

## 1.2 Pernyataan Masalah

Performa dari IDS dipengaruhi oleh proses klasifikasi serangan yang cepat dan akurat. Akan tetapi, metode klasifikasi yang sudah ada saat ini masih memiliki kekurangan dalam waktu proses klasifikasi yang lama.

## 1.3 Perumusan Masalah

Berikut rumusan masalah yang ingin saya angkat adalah

1. Bagaimana melakukan studi terhadap metode klasifikasi yang belum diuji pada IDS?
2. Bagaimana mengimplementasikan metode IVM pada IDS dengan menggunakan parameter terbaik?
3. Bagaimana melakukan analisis perbandingan metode klasifikasi IVM dengan metode yang sudah ada?

## 1.4 Objektif

Berikut adalah tujuan yang ingin dicapai pada penulisan proposal/TA.

1. Melakukan studi terhadap metode klasifikasi yang belum diuji pada IDS;
2. Melngimplementasikan metode IVM pada IDS dengan menggunakan parameter terbaik;
3. Melakukan analisis perbandingan metode klasifikasi IVM dengan metode yang sudah ada;

;

## 1.5 Hipotesa

1. Pengujian metode klasifikasi IVM pada data IDS, dapat menghasilkan waktu proses klasifikasi yang cepat dengan akurasi yang baik.
2. Pengujian parameter *Sigma* dan *Lambda* yang digunakan dalam klasifikasi pada metode IVM, dapat ditemukan parameter terbaik untuk melakukan klasifikasi IDS.
3. Pengklasifikasian data IDS dengan menggunakan algoritma IVM dapat mengatasi permasalahan waktu *testing* yang lama pada metode klasifikasi yang sudah ada.

## 1.6 Batasan Masalah

Ruang Lingkup dari pengerjaan riset ini adalah :

1. Penelitian menggunakan dataset NSL-KDD dan klasifikasi berupa klasifikasi binary.
2. Penelitian berfokus untuk mencari akurasi, dan waktu testing dari algoritma IVM dengan meneliti parameter sigma dengan batas nilai (2,4,6,8,10,12) dan parameter lambda dengan batas nilai (1,3,5,7,9,11).
3. Metode klasifikasi yang akan dibandingkan dengan IVM adalah metode SVM, KNN, dan ANN.
4. Dilakukan Feature Selection terhadap dataset NSL-KDD, 41 fitur, 35 fitur, 25 fitur, dan 10 fitur.

## 1.7 Kontribusi

Pengerjaan tugas akhir ini akan melakukan klasifikasi pada data IDS menggunakan algoritma IVM, dan akan menambah variasi metode klasifikasi yang sangat berguna nantinya dibidang keamanan jaringan.

## 1.8 Sistematika Penulisan

Secara garis besar TA saya akan terdiri dari beb-bab seperti berikut :

1. Bab 1 Pendahuluan  
Pada bab ini berisikan penjelasan tentang latar belakang awal mula motivasi dari Tugas Akhir ini, memahami masalah dan tujuan utama dari Tugas akhir ini, serta mengetahui methodology penulisan dan sistematika penulisan.
2. Bab 2 Kajian Pustaka  
Berisikan segala sesuatu yang berkaitan dengan riset dan berisi hasil-hasil riset yang sudah ada.
3. Bab 3 Methodology dan Desain sistem  
Berisikan penjelasan mengenai gambaran umum sistem dan perancangan desain sistem pada penulisan Tugas AKhir ini. Penjelasan bagaimana sistem ini berkerja terdapat pada subbab pada bab ini.
4. Bab 4 Hasil dan Pembahasan  
Berisikan cara pengujian sistem dan hasil pengujian yang akan dilakukan pada Tugas Akhir ini. Penjelasan setiap pengujian terdapat dalam subbab pada bab ini.

## 5. Bab 5 Kesimpulan dan Saran

Pada bab ini menampilkan kesimpulan yang didapat dari bab-bab sebelumnya, dan mengetahui saran-saran dari penulis untuk kepentingan penelitian kedepannya.

### **1.9 Ringkasan**

Pada bab ini dijelaskan dasar dari penelitian yang akan dilakukan pada tugas akhir ini. Bab ini berisikan latar belakang sebagai dasar permasalahan, rumusan masalah, tujuan penelitian, batasan masalah, dan sistematika penulisan pada tugas akhir ini.