

1. PENDAHULUAN

1.1 Latar belakang

Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah node dan teknologi yang digunakan. Dengan begitu jaringan komputer memerlukan pengelolaan yang baik agar ketersediaan jaringan selalu tinggi. Dalam hal ini keamanan jaringan komputer merupakan salah satu hal yang perlu diperhatikan secara khusus.

Penyusupan ataupun yang sering disebut dengan intrusi adalah salah satu jenis gangguan jaringan komputer. Definisi intrusi adalah sesuatu yang berusaha merusak atau menyalahgunakan sistem, atau setiap usaha yang melakukan *compromise* integritas, kepercayaan atau ketersediaan suatu sumberdaya komputer [2]. Intrusi berpotensi mengakibatkan ancaman terhadap integritas jaringan tanpa diketahui oleh pemiliknya. *Intrusion Detection System (IDS)* merupakan *tools* yang sangat populer saat ini yang digunakan untuk mengidentifikasi adanya intrusi didalam suatu jaringan[8].

Salah satu pondasi *tools* IDS adalah kemampuannya dalam memprediksi atau menggolongkan data hasil audit sebagai sebuah serangan atau bukan. Dalam implementasinya banyaknya jumlah data audit yang akan diprediksi, cepatnya pertambahan variasi tipe serangan atau intrusi membutuhkan mekanisme yang bekerja secara cerdas dan efektif. Dalam konteks inilah *data mining* diperlukan sehubungan dengan kemampuannya untuk mendapatkan informasi yang berharga dari sekumpulan besar data.

Banyak sekali metode statistika yang dapat digunakan untuk melakukan prediksi didalam *data mining*. Salah satunya adalah *Hidden Markov Model (HMM)*. *Hidden Markov Model* merupakan suatu model statistik yang dapat digunakan untuk menganalisa data sekuensial. HMM akan menggunakan parameter-parameter untuk menghasilkan suatu model. HMM menggunakan kombinasi linear dari setiap kemungkinan dan menggunakan pendekatan yang berdasar frekuensi dari kejadian dan nilai prediktif. Sudah banyak studi kasus yang dapat diselesaikan dengan metode HMM ini. Diantaranya adalah *Speech Recognition* dan pada bioinformatika yaitu mengimplementasikan pencarian gen pada data sekuens struktur genome untuk beberapa organisme.

Dalam tugas akhir ini akan dilakukan analisa dan implementasi teknik *data mining* pada domain *Intrusion Detection System (IDS)*. Metode HMM akan dipakai untuk menentukan karakteristik akses yang digolongkan kedalam suatu intrusi atau normal dengan menggunakan atribut *Network based*.

1.2 Perumusan masalah

Dalam tugas akhir ini, penulis akan mencoba untuk mengimplementasikan metode *Hidden Markov Model* pada pembangunan suatu *Intrusion Detection System* dan mencoba untuk menarik kesimpulan dari implementasi tersebut. Adapun rumusan masalahnya adalah sebagai berikut:

- a. Apakah metode *Hidden Markov Model* dapat digunakan dalam studi kasus *Intrusion Detection System* ?

- b. Bagaimana cara pembuatan model dengan menggunakan metode *Hidden Markov Model* dengan menggunakan dataset KDD cup 1999 ?
- c. Implementasi yang dilakukan hanya sampai terbentuknya misuse *Detection* model.
- d. Data set yang digunakan sudah melalui proses diskritisasi dan feature selection.
- e. Pengukuran keakuratan, sensitivitas pencarian intrusi dari metode *Hidden Markov Model*.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah :

- a. Mempelajari metode *Hidden Markov Model* dan pemanfaatannya pada *data mining*.
- b. Menganalisa penggunaan *Hidden Markov Model* jika diterapkan dalam *Intrusion Detection*.
- c. Mengukur tingkat efisiensi dan akurasi metode *Hidden Markov Model* pada *Intrusion Detection* dan melakukan implementasi dari proses.

1.4 Metodologi penyelesaian masalah

Metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah :

- a. Studi Literatur
Mempelajari dasar teori dan literatur-literatur tentang *Data mining*, *Hidden Markov Model*, *Intrusion Detection*, *Data set* KDD cup 1999 dan mempelajari cara pembangunan aplikasi.
- b. Perencanaan
Tahapan ini dilakukan untuk melakukan perencanaan tentang apa yang akan dikerjakan dan apa yang perlu dipersiapkan.
- c. Perancangan Perangkat Lunak
Bertujuan untuk melakukan analisa dan perancangan pengembangan perangkat lunak dengan menggambarkan dalam modul-modul perangkat lunak.
- d. Pembuatan Perangkat Lunak
Melakukan implementasi metode *Hidden Markov Model* pada perangkat lunak sesuai dengan analisa perancangan yang telah dilakukan.
- e. Pengujian dan perbaikan perangkat lunak
Dalam tahap ini akan diuji program untuk berbagai training data set dan mencari kesalahan-kesalahan yang masih muncul dalam perangkat lunak.
- f. Analisa terhadap hasil pengujian perangkat lunak.
- g. Pengambilan kesimpulan dan penyusunan laporan.