BAB I
PENDAHULUAN

Bab ini akan menguraikan latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, dan sistematika penulisan laporan.

1.1 Latar Belakang

Dewasa ini, penggunaan komputer di masyarakat semakin meningkat. Komputer sendiri sudah menjadi salah satu kebutuhan pokok masyarakat jaman sekarang. Karena meningkatnya penggunaan komputer, maka aktifitas bisnis dan penyimpanan serta penggunaan data pun sudah mulai dialihkan, dari yang awalnya menggunakan berkas-berkas dokumen dialihkan menjadi aktifitas komputasi dan data digital yang tersimpan didalam komputer dalam bentuk sistem informasi.

Penggunaan sistem informasi juga tidak bisa terlepas dari penggunaan sistem jaringan komputer. Sistem jaringan komputer digunakan sebagai media komunikasi antar berbagai pihak untuk saling bertukar data secara lebih efektif dan efisien. Penggunaan sistem jaringan komputer ini tentu bukan tanpa kekurangan dan resiko. Salah satu resiko besar yang dihadapi dalam sistem jaringan komputer adalah keamanan data yang tersimpan dalam sistem informasi. Berbagai cara telah dilakukan untuk bisa mengamankan data yang disimpan agar terhindar dari akses paksa dari pihak-pihak yang tidak berhak akan informasi tersebut.

Aturan-aturan keamaanan dari sistem informasi sudah banyak dibuat dan diterapkan untuk menjaga baik integritas dari kerahasiaan data, maupun integritas dari ketersediaan data bagi pihan-pihak yang memang diperuntukkan mengakses dan menggunakannya. Bagaimanapun, berbagai pihak yang ingin mengakses paksa suatu sistem informasi selalu saja bisa menemukan kelemahan dan celah dalam aturan-aturan keamanan yang telah diterapkan, hal ini diperkuat dengan adanya pendapat bahwa sehebat apapun keamanan yang diterapkan, tetap saja data yang tersimpan menjadi tidak aman (Elhag, Fernandez, Bawakid, Alshomrani, & Herrera, 2015).

Topik yang sering diperbincangkan dalam keamanan komputer terpusat pada penggunaan alat dan teknik untuk mengamankan jaringan komputer. Telah banyak

cara yang dikembangkan untuk mendapatkan sistem keamanan yang bagus, dikarenakan seperti yang dikemukakan pada sebuah jurnal bahwa penggunaan firewall, pendeteksi virus, dan mekanisme enkripsi data tidaklah cukup untuk mengamankan sistem jaringan komputer (Ravale, Marathe, & Padiya, 2015).

Setiap serangan didalam jaringan dapat dikategorikan menjadi empat kategori, dan jenis serangan yang paling lazim dan sering diterima oleh suatu sistem jaringan adalah serangan DOS. Serangan DOS adalah sebuah tipe serangan dimana hacker membuat proses komputasi atau sumber daya memori menjadi terlalu sibuk dan terlalu penuh untuk melayani permintaan pelayanan yang sebenarnya. DOS menyebabkan permintaan akses dari pengguna sebenarnya menjadi ditolak (Hoque, Mukit, & Bikas, 2012).

Sudah banyak kasus serangan DOS yang terbukti sangat merugikan banyak pihak. Seperti dikutip dari salah satu jurnal, bahwa kasus awal terjadi pada tahun 1996, dimana pada saat itu terjadi serangan SYN, dengan tingkat serangan mencapai 200 packet/s, selanjutnya pada 7 Februari tahun 2000, terjadi serangan secara besar-besaran yang terjadi pada banyak situs organisasi komersial, seperti yahoo.com, CNN, e-Bay, Amazon dan lain-lain (Kumar & Selvakumar, 2013). Terdapat berbagai macam cara yang dapat dilakukan untuk dapat mendeteksi serangan DOS, diantaranya adalah menggunakan sebuah protokol keamanan (Darwish, Ouda, & Capretz, 2015), menerapkan penjadwalan dengan teknik probabilitas (Seo, Lee, & Perrig, 2013), menggunakan fitur statistikal (Gavrilis & Dermatas, 2005), dan yang paling terkenal adalah menggunakan IDS (Intrusion Detection System).

Selain di luar negeri, seranga DOS juga pernah terjadi di Indonsia, antara lain:

a. Serangan oleh anak komunitas YogyaFree terhadap website kaskus pada tahun 2008. Serangan ini berlangsung pada 16-17 Mei 2008. Serangan yang dilakukan oleh komunitas yogyafree ini mengakibatkan situs kaskus tidak dapat di akses dan corrupt. Penyerangan ini mengakibatkan thread-thread yang telah dibuat terpaksa dikunci (locked) oleh administrator kaskus. Karena hal ini berlangsung cukup lama akhirnya administrator kaskus terpaksa mematikan server kaskus. Penyerangan ini

meruapakan balasan dari komunitas yogyafree terhadap kaskus, menurut sumber penyerangan ini dilakukan karena yogyafree telah dicela pada salah satu forum di kaskus. Beberapa waktu terjadilah pertikaian antara dua komunitas ini. Akhirnya pertikaian ini selesai ketika pengelola situs menandatangani memorandum online untuk menyudahi pertikaian di antara keduanya. Saat itu pesan tersebut dipampang selama beberapa minggu di halaman situs masing-masing. Dari kejadian ini kaskus meluncurkan server baru yang lebih dilengkapi dengan pengamanan data yang tangguh dan siap untuk menghadapi berbagai serangan dari berbagai pihak.

b. Insiden yang menyerang DDOS juga terjadi pada pertengahan tahun 2009 dimana domain.co.id sempat drop selama 4 hari akibat serangan DDOS. Hal ini menunjukkan adanya kelemahan yang sangat mendasar dalam sistem DNS CCTLD-ID. Situasi ini sangat berbahaya mengingat domain.co.id merupakan salah satu infrastruktur Internet Indonesia yang strategis. Kegagalan sistem DNS CCTLD-ID berpotensi menimbulkan kerugian ekonomi. Karena domain drop otomatis para pengguna tidak dapat mengakses situs dengan domain.co.id . bagi pengguna email di yahoo.co.id. tidak dapat mengakses emailnya karena domainnya telah down. Beberapa saat setelah kejadian tersebut administrator diberitakan melakukan maintenance terhadap system keamanan domain tersebut dan sampai sekarang masih dapat dinikmati oleh masyarakat.

Terdapat berbagai macam cara yang dapat dilakukan untuk dapat mendeteksi serangan DOS, diantaranya adalah menggunakan sebuah protokol keamanan (Darwish, Ouda, & Capretz, 2015), menerapkan penjadwalan dengan teknik probabilitas (Seo, Lee, & Perrig, 2013), menggunakan fitur statistikal (Gavrilis & Dermatas, 2005), dan yang paling terkenal adalah menggunakan IDS (Intrusion Detection System).

IDS adalah salah satu jenis manajemen keamanan yang bisa diterapkan untuk komputer dan sistem jaringan komputer. Beberapa IDS mampu untuk mendeteksi serangan secara *real-time* dan dapat membantu kita untuk menghentikan serangan terhadap sistem. Beberapa IDS yang lain mampu memberikan informasi-informasi

penting tentang serangan yang terjadi, sehingga mampu untuk mengurangi potensi terjadinya serangan dengan tipe yang sama di kemudian hari. Fungsi utama IDS adalah sebagai pendeteksi serangan dini sehingga pihak yang mengurus suatu sistem jaringan bisa mendapatkan informasi bila terjadinya serangan, hal ini diperkuat dengan adanya pendapat dari sebuah jurnal bahwa IDS akan memonitor kegiatan didalam sistem jaringan komputer secara terus- menerus, menganalisa data kegiatan tersebut, dan akan memberi tahu *system administrator* atau *network administrator* apabila terjadi serangan atau kegiatan yang mencurigakan (Ravale, Marathe, & Padiya, 2015).

Salah satu aplikasi IDS yang umum dipakai adalah Snort. Snort adalah *signature based* IDS yang dibuat pada tahun 1998 oleh Martin Roesch. Snort bersifat *open source* dan gratis. Tetapi, karena bersifat *signature based*, SNORT tidak mampu melakukan deteksi terhadap jenis serangan yang belum diketahui. Selain itu, karena bersifat *open source*, akan lebih mudah bagi *intruder* untuk memodifikasi serangannya agar tidak memancing deteksi dari Snort.

Untuk memaksimalkan fungsi deteksi, maka dibutuhkan IDS yang mampu melakukan proses deteksi terhadap jenis serangan yang belum diketahui. Hal ini memicu perkembangan pesat dari penggunaan teknik *data mining* dalam membuat IDS yang menerapkan *anomaly based.*

Anomaly based IDS tidak terlepas dari teknik *data mining*. IDS mampu menemukan perliaku jaringan secara rutin dengan cara menganalisa jejak data dari aktifitas yang terjadi menggunakan pendekatan *data mining*. Seperti yang dikutip dari sebuah jurnal, bahwa terdapat dua keuntungan yang didapat dari penggunaan pendekatan data mining pada IDS, yaitu (1) IDS akan mampu untuk menghasilkan model aktifitas jaringan secara otomatis, dan (2) pendekatan data mining dapat digunakan untuk membangun IDS untuk berbagai tipe lingkungan komputasi (S., P., S., & C., 2014).

Beberapa penelitian tentang IDS telah menggunakan teknik *clustering* dari pendekatan data mining. Salah satunya adalah algoritma sarang semut (Ramos & Abraham, 2005). Algoritma sarang semut yang merupakan salah satu teknik *data mining* diterapkan didalam IDS untuk mendapatkan hasil *clustering* dari data akses,

sehingga sistem mampu membedakan antara kegiatan normal dengan kegiatan abnormal. Namun penerapan teknik sarang semut memerlukan proses komputasi yang panjang, terutama jika training set yang digunakan berukuran besar (Feng, Zhang, Hu, & Huang, 2013).

Selain teknik *clustering*, teknik klasifikasi pada *data mining* juga sudah diterapkan dalam penelitian IDS. Salah satu teknik klasifikasi yang digunakan adalah dengan menerapkan algortima SVM untuk memecahkan permasalahan didalam IDS (Mohammed & Sulaiman, 2012). Dalam penelitian tersebut, algoritma SVM mampu melakukan deteksi intrusi dalam jaringan dengan cara mengenali pola serangan dari data-data akses didalam jaringan. Tetapi algoritma SVM tidak cocok digunakan untuk dataset yang memiliki skala besar, karena kompleksitas proses training sangat bergantung pada tingkat kompleksitas training set yang dipakai (Gupta & Shrivastava, 2015).

Selain penggunaan dua teknik *data mining* secara terpisah, kombinasi dua teknik dalam *data mining* (*clustering* dan klasifikasi) juga sudah mulai diterapkan untuk memecahkan permasalahan didalam IDS. Salah satunya terdapat IDS yang menggunakan pendekatan algoritma gabungan SVM dan algoritma sarang semut yang disebut CSVAC (S., P., S., & C., 2014). Dalam jurnal ini, dua algoritma *data mining* yang masing-masing terbukti efektif dalam penerapannya di IDS kemudian dikombinasikan bersama, dan ternyata terbukti mendapatkan hasil klasifikasi intrusi sistem jaringan yang lebih baik ketimbang penggunaan kedua algoritma sebelum dikombinasikan. Walaupun begitu, penggambungan dua algoritma tetap memerlukan waktu komputasi yang signifikan. Selain itu, karena memiliki dua proses besar, pembuatan model menggunakan CSVAC menggunakan penggunaan I/O yang tinggi.

Dalam penelitian ini, akan diajukan algoritma CM-SPADE untuk diterapkan dalam mesin IDS, guna menemukan pola serangan DOS pada suatu jaringan. Algoritma CM-SPADE adalah optimisasi algoritma SPADE. CM-SPADE menambahkan proses identifikasi dan penyimpanan co-occurences information, sehingga dapat memangkas waktu proses pencarian sequence. Selain itu, algoritma CM-SPADE melakukan proses mining dengan menggunakan proses lattices,

sehingga bisa mengurangi penggunaan I/O dan meminimalisir proses pembacaan dataset.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka dirumuskan masalah sebagai berikut:

1. Bagaimana model IDS yang dihasilkan dengan mengimplementasi algoritma CM-SPADE?
2. Berapa training time yang dibutuhkan algoritma CM-SPADE dalam membentuk model IDS?
3. Bagaimana hasil akurasi CM-SPADE dalam mendeteksi serangan pada IDS?
4. Bagaimana perbandingan performa model IDS menggunakan CM-SPADE dengan model IDS yang lain?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada, maka tujuan penelitian ini yaitu sebagai berikut:

1. Mengetahui model yang dihasilkan dengan penerapan algoritma CM-SPADE dalam menentukan pola serangan DOS pada teknik deteksi IDS.
2. Mengetahui training time yang dibutuhkan oleh algoritma CM-SPADE dalam membentuk model IDS.
3. Mengetahui tingkat akurasi dari penerapan algoritma CM-SPADE dalam menentukan pola serangan DOS.
4. Mengetahui perbandingan hasil performa penerapan algoritma CM-SPADE pada IDS dengan algoritma lain.

1.4 Batasan Masalah

Berikut merupakan beberapa batasan masalah dalam penelitian ini yaitu sebagai berikut:

1. Penelitian ini hanya akan membahas tentang sistem deteksi interupsi, tanpa membahas sistem penanggulangannya.
2. Penelitian ini hanya akan berfokus kepada tipe serangan DOS, tanpa memperhatikan tipe seranga jaringan yang lainnya.

1.5 Manfaat Penulisan

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Bagi peneliti

   Peneliti diharapkan mendapatkan pengetahuan baru mengenai *data mining* dan *intrusion detection system*.

2. Bagi pihak lain

   Hasil penelitian ini membantu praktisi dan peneliti pada bidang *data mining* dan *intrusion detection system* untuk mengetahui model hasil penerapan *data mining* menggunakan teknik CM-SPADE pada suatu lingkungan *intrusion detection system*. Selain itu, penelitian ini diharapkan mampu memberikan gambaran mengenai performa CM-SPADE beserta kekurangan dan kelebihannya dalam penerapannya pada lingkungan *intrusion detection system*.

1.6 Sistematika Penulisan

Adapun sistematika penulisan karya ilmiah ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab I atau pendahuluan akan menyampaikan tentang alasan penulis mengangkat topik ini sebagai skripsi di mana hal tersebut diuraikan pada sub bab latar belakang. Lalu dijelaskan juga rumusan masalah penelitian, tujuan dilakukannya penelitian, manfaat dari hasil penelitian, batasan masalah agar penelitian yang dilakukan tidak terlalu luas, dan sistematika penulisan yang menjelaskan apa saja isi dari penelitian ini.

BAB II KAJIAN PUSTAKA

Pada kajian pustaka akan diuraikan materi-materi yang berhubungan dengan penelitian. Materi ini mendasari penulis dalam melakukan penelitiannya. Materi yang disampaikan meliputi data, *data analysis, descriptive statistic*, data visualisasi, *python*, *Django*,

BAB III METODOLOGI PENELITIAN

Bab ini berisi tahap-tahap yang dilakukan pada penelitian ini, yaitu alat dan bahan penelitan, desain penelitian serta metode penelitian yang akan digunakan pada penelitian ini. Bagian-bagian tersebut akan dijelaskan secara lengkap pada bab ini.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab pembahasan menjelaskan bagaimana penelitian dilakukan, seperti apa proses yang terjadi saat penelitian, dan apa hasil yang didapat setelah melakukan penelitian. Pembahasan akan dibagi menjadi hasil dan pembahasan.

BAB V KESIMPULAN DAN SARAN

Bab ini akan memaparkan kesimpulan yang merupakan jawaban atas pertanyaan-pertanyaan pada sub bab rumusan masalah, dan saran yang merupakan kumpulan saran dan rekomendasi dari penulis untuk penelitian dan pengembangan selanjutnya.