**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

1. **IDENTITAS PENGUSUL**

**NAMA : PATRISIUS ARDIANTO CAHYADI**

**NRP : 5108 100 184**

**DOSEN WALI : SARWOSRI, S.Kom, M.T**

1. **JUDUL TUGAS AKHIR**

**“Pengembangan Intrusion Detection System Berbasis Support Vector Machine dan Decision Tree”**

1. **LATAR BELAKANG**

*Intrusions* adalah aktivitas-aktivitas yang dilakukan oleh *attacker* untuk masuk ke sebuah sistem sehingga *attacker* dapat memperoleh informasi-informasi penting dari sistem tersebut[6]. Jika Intrusions behaviours tersebut tidak segera ditangani, tentu akan berakibat buruk pada pihak yang diserang. Oleh karena itu diperlukan sebuah sistem pengaman untuk mendeteksi adanya *intrusion* sehingga *intrusion* tersebut dapat dicegah sebelum mengakibatkan kerugian besar pada sistem utama[1].

Pada awalnya, para *enterprise* menggunakan *firewall* sebagai *defense system* terhadap *intrusions* tersebut[7]. Tetapi *firewall* hanya berfungsi secara pasif sehingga kurang efektif untuk meminimalisir kerugian pada sistem akibat *intrusion*. Oleh karena itu diperlukan sebuah *defense system* yang mampu berfungsi secara aktif mengumpulkan paket-paket data yang keluar-masuk jaringan kemudian menentukan apakah paket-paket data tersebut normal atau tidak[6]. Sistem seperti itu disebut *Intrusion Detection System (IDS)*. *IDS* mampu menentukan apakah suatu paket data yang lewat jaringan merupakan sebuah serangan atau tidak sehingga *intrusion* dapat dicegah[1].

Pada dasarnya ada 2 metode Intrusion Detection yaitu *Misuse Detection* dan *Anomaly Detection*. Misuse Detection bekerja layaknya anti virus, yaitu membandingkan karakteristik dari sebuah activity dengan karakteristik dari serangan yang telah diketahui sebelumnya[7].

Pada *Anomaly detection* semua karakteristik dari aktivitas-aktivitas normal yang pernah terjadi di jaringan tersebut dipelajari oleh sistem. Jika ada aktivitas baru yang karakteristiknya tidak sesuai dengan karakteristik aktivitas-aktivitas normal, sistem akan memberikan peringatan adanya serangan[4].

Saat ini, *Intrusion behaviour* telah menjadi masalah yang cukup besar di bidang *network security* karena dapat memberikan dampak negatif yang sangat besar pada sistem[5]. Pengklasifikasian suatu aktivitas ke dalam suatu tipe serangan sesuai dengan karakteristiknya menjadi fokus utama dari masalah *Intrusion Detection* ini[6]. Metode *Misuse Detection* dapat melakukan klasifikasi aktivitas-aktivitas yang terjadi berdasarkan karakteristik yang telah diketahui sebelumnya. Untuk dapat melakukan klasifikasi, sistem harus diberi data learning terlebih dahulu. Data learning tersebut merupakan karakteristik dari aktivitas-aktivitas yang terjadi pada jaringan tersebut[7]. Setelah itu sistem menggunakan *Support Vector Machine* untuk melakukan klasifikasi pada aktivitas yang terjadi sesuai karakteristik yang telah diketahui[2]. Untuk memenuhi kebutuhan tersebut, maka penulis mengimplementasikan *Support Vector Machine* pada *Intrusion Detection System*.

1. **RUMUSAN MASALAH**

Rumusan masalah yang diangkat dalam Tugas Akhir ini dapat dipaparkan sebagai berikut :

1. Bagaimana cara melakukan *clustering* dan klasifikasi pada suatu data set yang berkaitan dengan *Intrusion Detection.*
2. Bagaimana mengimplementasikan *Support Vector Machine* pada *Intrusion Detection System.*
3. Bagaimana cara menentukan jenis suatu aktivitas berdasarkan karakteristik aktivitas dan serangan yang telah diketahui.
4. **BATASAN MASALAH**

Permasalahan yang dibahas dalam Tugas Akhir ini memiliki beberapa batasan, diantaranya sebagai berikut:

1. Ada beberapa jenis serangan dengan karakteristik masing-masing.
2. Metode klasifikasi yang digunakan adalah *Support Vector Machine.*
3. Data latihan yang digunakan adalah data dari *NSL-KDD* yaitu data set hasil penyederhanaan dari *KDD cup* 1999.
4. **TUJUAN TUGAS AKHIR**

Tugas akhir ini bertujuan untuk mengimplementasikan *Support Vector Machine* pada *Intrusion* *Detection System* dengan data set dari *NSL-KDD*.

1. **MANFAAT TUGAS AKHIR**

Manfaat dari tugas akhir ini adalah untuk menghasilkan aplikasi Intrusion Detection menggunakan Support Vector Machine untuk proses learning dan klasifikasi. Hasil dari penelitian ini diharapkan dapat digunakan untuk penelitian-penelitian selanjutnya mengenai *Intrusion Detection*. Selain itu, penelitian ini juga diharapkan dapat memajukan teknologi *network security* di Indonesia.

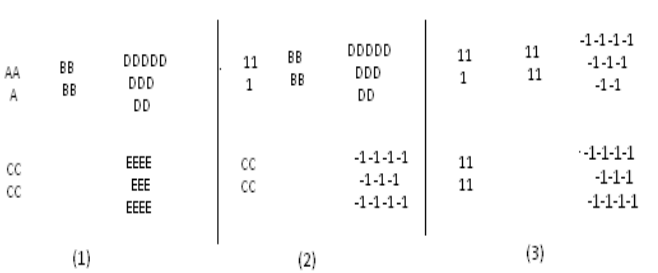
1. **RINGKASAN TUGAS AKHIR**

Permasalahan utama pada tugas akhir ini adalah bagaimana mengklasifikasikan suatu aktivitas ke dalam jenis intrusion yang berbeda-beda sesuai dengan karakteristik dari aktivitas tersebut. Dalam pembuatan tugas akhir ini, penulis membuat sebuah aplikasi yang berfungsi sebagai Intrusion Detection System. Pada mulanya aplikasi akan melakukan learning dari data set yang diperoleh dari *NSL-KDD* *data archive* dengan menggunakan *Support Vector Machine* untuk mengetahui bagaimana karakteristik aktivitas-aktivitas yang pernah terjadi. Sebelum melakukan learning, akan dilakukan *preprocessing* pada data set tersebut. Durasi dari proses learning tersebut tergantung dari ukuran data learning. Setelah proses learning selesai, informasi tentang tipe intrusion yang pernah terjadi akan tersimpan di dalam aplikasi. Sehingga aplikasi dapat menentukan jenis dari aktivitas berdasarkan karakteristik yang dimasukkan ke sistem[4].

Data set yang digunakan adalah data dari NSL-KDD data archive. NSL-KDD merupakan hasil penyederhanaan dari KDD cup 1999 data set dengan menghilangkan *redundant record*[3]. Pada dasarnya setiap *intrusion* dapat diklasifikasikan ke dalam 4 kelas, yaitu :

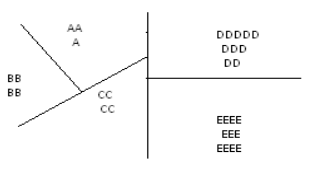
1. Denial of Service Attack (DoS). Pada Intrusion tipe ini, seorang *attacker* membuat *memory* atau kegiatan komputasi sebuah server terlalu sibuk sehingga dapat dengan mudah diserang.[9]
2. User to Root Attack (U2R). Pada Intrusion tipe ini, seorang *attacker* memulai serangan dengan melakukan akses ke sistem menggunakan beberapa normal user accout untuk mencari kelemahan sistem sehingga lebih mudah mendapatkan *root access* ke sistem.[9]
3. Remote to Local Attack (R2L). Intrusion tipe ini terjadi jika seorang attacker memiliki kemampuan untuk melakukan remote access pada suatu komputer di jaringan yang akan diserang.[9]
4. Probing Attack. Pada intrusion tipe ini, seorang attacker berusaha mencari informasi sebanyak-banyaknya dari sistem yang diserang untuk mencari celah dari sistem keamanannya.[9]

Jadi, hasil akhir dari tugas akhir ini adalah mengelompokkan suatu aktivitas ke dalam beberapa tipe serangan di atas sesuai dengan data training yang dimasukkan.



Gambar 1 Langkah-langkah melakukan clasifikasi 5 class dengan SVM model [10]

Oleh karena itu untuk melakukan klasifikasi dibutuhkan 4 class yaitu DoS, U2R, R2L dan Probing. Lalu dibutuhkan 1 class lagi untuk tipe serangan yang tidak termasuk ke 4 tipe tersebut (*unknown attack type*). Langkah-langkah klasifikasi 5 class dengan SVM model ditunjukkan pada gambar 1. Misalnya jika DoS, U2R, R2L, Probing dan *unknown attack type*, masing-masing disimbolkan dengan huruf D, A, B, C dan E maka akan dihasilkan gambar 1.1[10]. Pada gambar 1.1 jarak antara A dan E merupakan jarak yang terbesar sehingga A dan E yang akan dipisahkan terlebih dahulu. Tipe A dianggap sebagai 1 dan Tipe E dianggap sebagai -1 sesuai dengan gambar 2.2. Berikutnya dilakukan pencarian jarak yang paling besar. Menurut gambar 2.2 dapat disimpulkan bahwa jarak C ke D lebih besar dari jaraj B ke D sehingga C diganti 1 dan D diganti -1 dan dihasilkan gambar 1.3.[10]



Gambar 2 Hasil akhir klasifikasi 5 class dengan SVM model [10]

Setelah dilakukan pencarian hyperplane-hyperplane (garis) yang mungkin untuk membagi data menjadi 5 class yang berbeda, dihasilkan posisi hyperplane-hyperplane(garis) yang ditunjukkan pada gambar 2.[10].

Secara umum, langkah-langkah pembuatan Intrusion Detection System dengan SVM model, ditunjukkan pada gambar 3.

Gambar 3. Langkah-langkah pembuatan Intrusion Detection System

**TINJAUAN PUSTAKA DAN DASAR TEORI**

* 1. **Intrusion Detection System**

IDS (Intrusion Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan[8]. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal/ anomali melalui aksi pemblokiran seorang user atau alamat IP (Internet Protocol)[6].

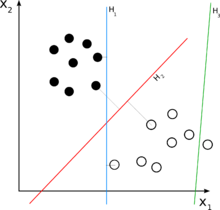
Ada IDS yang bekerja dengan cara mendeteksi berdasarkan pada pencarian ciri-ciri khusus dari percobaan yang sering dilakukan atau sering disebut *Misuse Detection*. Cara ini hampir sama dengan cara kerja perangkat lunak antivirus dalam mendeteksi dan melindungi sistem terhadap ancaman. Kemudian ada juga IDS yang bekerja dengan cara mendeteksi berdasarkan pada pembandingan pola traffic normal yang ada dan kemudian mencari ketidaknormalan traffic yang ada atau sering disebut *Anomaly Detection*. Ada IDS yang fungsinya hanya sebagai pengawas dan pemberi peringatan ketika terjadi serangan dan ada juga IDS yang bekerja tidak hanya sebagai pengawas dan pemberi peringatan melainkan juga dapat melakukan sebuah kegiatan yang merespon adanya percobaan serangan terhadap sistem jaringan dan komputer[8].

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan[7].

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai Anomaly-based IDS. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi[4]. Metode ini menawarkan kelebihan dibandingkan signature-based IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data signature IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan false positive (suatu aktivitas yang normal dianggap sebagai ancaman ). Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan *false positive* yang muncul[7].

* 1. **Support Vector Machine**

Support Vector Machine (SVM) pertama kali diperkenalkan oleh Vapnik pada tahun 1992 sebagai rangkaian harmonis konsep-konsep unggulan dalam bidang *pattern recognition*[8]. Sebagai salah satu metode *pattern recognition*, usia *SVM* terbilang masih relatif muda. Walaupun demikian, evaluasi kemampuannya dalam berbagai aplikasinya menempatkannya sebagai *state of the art* dalam *pattern recognition*, dan dewasa ini merupakan salah satu tema yang berkembang dengan pesat[2].



Gambar 4 Ilustrasi Klasifikasi menggunakan SVM model [2]

Klasifikasi merupakan suatu proses yang umum di bidang *machine learning*. Suatu proses klasifikasi dapat diilustrasikan seperti gambar 4. Pada gambar 4 terdapat 2 jenis lingkaran (class) yaitu lingkaran yang hitam dan putih pada bidang 2 dimensi. Tujuan akhir dari proses klasifikasi tersebut adalah menemukan suatu (p-1) hyperplane (dalam kasus ini 1 dimensi yaitu garis) yang dapat memisahkan kedua jenis lingkaran pada bidang tersebut. H3(garis hijau) tidak memisahkan kedua class dengan baik. H1(garis biru) memisahkan kedua class tapi menyisakan pembatas yang sangat sempit antara kedua class sehingga kurang efektif. H2(garis merah) memisahkan kedua kelas dan menyisakan selisih yang maksimal sehingga H2 merupakan *hyperplane* yang paling efektif. Fokus utama dari SVM adalah cara menemukan *hyperplane* yang efektif tersebut[2].

1. **METODOLOGI**

## Studi Literatur

Pada tahap ini dilakukan pengumpulan dan penggalian informasi dan literatur yang diperlukan dalam proses perancangan dan implementasi sistem yang akan dibangun. Literatur yang digunakan adalah terkait dengan *Intrusion Detection, Support Vector Machine* dan data set dari KDD cup 99.

## Perancangan Aplikasi

Tahap ini meliputi perancangan sistem berdasarkan studi literatur dan pembelajaran konsep teknologi dari perangkat lunak yang ada. Tahap ini merupakan tahap yang paling penting dimana bentuk awal program yang akan diimplementasikan, didefinisikan. Pada tahap ini dilakukan perancangan tentang tampilan antar muka dan implementasi SVM pada Intrusion Detection System.

## Implementasi Pembuatan Program

Pada tahap ini dilakukan pembuatan program yang merupakan implementasi dari rancangan yang telah dibuat sebelumnya.

## Uji coba dan evaluasi

Pada tahap ini akan dilakukan pengujian terhadap program menggunakan data atau skenario yang telah dipersiapkan sebelumnya. Uji coba dan evaluasi program dilakukan untuk mencari masalah yang mungkin timbul, mengevaluasi jalannya program, dan mengadakan perbaikan jika ada kekurangan.

## Penyusunan Buku Tugas Akhir

Pada tahap ini melakukan pendokumentasian dan laporan dari seluruh konsep, dasar teori, implementasi, proses yang telah dilakukan, dan hasil-hasil yang telah didapatkan selama pengerjaan tugas akhir. Buku tugas akhir ini bertujuan untuk mendapatkan gambaran dari pengerjaan tugas akhir ini dan diharapkan dapat berguna untuk pembaca yang tertarik untuk melakukan pengembangan lebih lanjut.

Secara garis besar, buku tugas akhir nantinya terdiri atas beberapa bagian yaitu :

1. Pendahuluan
   1. Latar Belakang
   2. Permasalahan
   3. Batasan Tugas Akhir
   4. Tujuan
   5. Metodologi
   6. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Uji Coba dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

# JADWAL KEGIATAN

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Kegiatan** | **Bulan (Tahun 2012)** | | | | | | | | | | | | | | | |
| **Maret** | | | | **April** | | | | **Mei** | | | | **Juni** | | | |
| 1. | Penyusunan Proposal Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2. | Studi Literatur |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3. | Implementasi & Pembuatan Program |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4. | Pengujian dan Evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5. | Penyusunan Buku Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Tabel 1. Jadwal Kegiatan

# DAFTAR PUSTAKA

1. Wikipedia, 2012, Intrusion Detection System, [online], (<http://en.wikipedia.org/wiki/Intrusion_detection_system>, diakses tanggal 1 Maret 2012 ).
2. Wikipedia, 2012, Support Vector Machine, [online],

(<http://en.wikipedia.org/wiki/Support_vector_machine>, diakses tanggal 1 Maret 2012).

1. NSL-KDD 1999 data set, [online],

(NSL-KDD 1999 Data Set archive : <http://iscx.ca/NSL-KDD/> , diakses tanggal 1 Maret 2012).

1. Weijun Li, Zhenyu Liu, A method of SVM with normalization in Intrusion Detection, in: Procedia Environmental Sciences 11 (2011) 256 – 262.
2. Peng Ning, Sushil Jajodia, “Intrusion Detection Techniques”, North Carolina State University, 2005.
3. Rung-Ching Chen, Kai-Fan Cheng, Chia-Fen Hsieh, Using Rough Set and Support Vector Machine for Network Intrusion Detection in : International Journal of Network Security and Its Applications (IJNSA), Vol 1, No 1, April 2009.
4. Rahedy, 2010, Apakah Itu IDS (Intrusion Detection System), [online],

(<http://rahedy.wordpress.com/2010/06/10/apakah-itu-ids-intrution-detection-system/>, diakses tanggal 3 Maret 2012).

1. Anto Satriya Nugroho , Support Vector Machine, [online],

(<http://asnugroho.net/papers/ikcsvm.pdf> , diakses tanggal 3 maret 2012).

1. Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, Ali Ghorbani, A Detailed Analysis of the KDD CUP 99 Data Set in : IEEE Symposium on Computational Intelligence in Security and Defense Application (CISDA 2009).
2. Snehal A. Mulay, P.R. Devale, G.V Garje, Intrusion Detection System using Support Vector Machine and Decision Tree in : International Journal of Computer Applications (0975-8887) Volume 3 – No 3, June 2010.