TUGAS AKHIR – KI141502

EVALUASI SISTEM PENDETEKSI INTRUSI BERBASIS ANOMALI DENGAN N-GRAM DAN INCREMENTAL LEARNING

I MADE AGUS ADI WIRAWAN
NRP 5112 100 036

Dosen Pembimbing I
Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D.

Dosen Pembimbing II
Baskoro Adi Pratomo, S.Kom., M.Kom.

JURUSAN TEKNIK INFORMATIKA
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

UNDERGRADUATE THESES – KI141502

EVALUATION OF ANOMALY BASED INTRUSION DETECTION SYSTEM WITH N-GRAM AND INCREMENTAL LEARNING

I MADE AGUS ADI WIRAWAN
NRP 5112 100 036

Supervisor I
Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D.

Supervisor II
Baskoro Adi Pratomo, S.Kom., M.Kom.

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA 2016

LEMBAR PENGESAHAN

EVALUASI SISTEM PENDETEKSI INTRUSI BERBASIS ANOMALI DENGAN N-GRAM DAN INCREMENTAL LEARNING

TUGAS AKHIR

Diajukan Guna Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Bidang Studi Komputasi Berbasis Jaringan
Program Studi S-1 Jurusan Teknik Informatika
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :
I MADE AGUS ADI WIRAWAN
NRP : 5112 100 036

Disetujui oleh Dosen Pembimbing Tugas Akhir :

ROYYANA MUSLIM IJTIHADIE, S.Kom., M.Kom., Ph.D. ..... (pembimbing 1)
NIP: 19770824 202624 1 001

BASKORO ADI PRATOMO, S.Kom., M.Kom. ..... (pembimbing 2)
NIP: 19870218 201404 1 001

SURABAYA
JULI, 2016

EVALUASI SISTEM PENDETEKSI INTRUSI BERBASIS ANOMALI DENGAN N-GRAM DAN INCREMENTAL LEARNING

Nama Mahasiswa	**: I MADE AGUS ADI WIRAWAN**
NRP	**: 5112100036**
Jurusan	**: Teknik Informatika FTIF-ITS**
Dosen Pembimbing 1	**: Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D.**
Dosen Pembimbing 2	**: Baskoro Adi Pratomo, S.Kom., M.Kom.**

Abstrak

Keberadaan teknologi informasi yang terus berkembang dengan pesat menjadikan kebutuhan akan penggunaannya semakin hari semakin meningkat. Transaksi data melalui internet telah menjadi kebutuhan wajib hampir dari semua perangkat lunak yang ada saat ini. Perangkat lunak seperti media social, colud server, online game, aplikasi layanan pemerintah, aplikasi pengontrol suatu tempat secara remote, dsb. Tentu dengan berbagai macam penggunaan internet tersebut dibutuhkan metode untuk mengamankan jaringannya.

Sistem pendeteksi intrusi atau yang pada umumnya disebut IDS (Intrusion Detection System) merupakan solusi untuk mengamankan suatu jaringan. Sistem ini nantinya bertugas untuk menentukan apakah suatu paket merupakan bentuk serangan atau paket biasa sesuai dengan kondisi tertentu. Saat ini telah banyak dikembangkan aplikasi IDS (Intrusion Detection System), namun sebagian besar yang dikembangkan berbasis signature atau menggunakan rule, dan sebagaian kecil menggunakan anomali. Anomali adalah suatu metode untuk mencari penyimpangan dalam sebuah data.

Pada aplikasi ini konsep IDS yang diterapkan adalah IDS berbasis anomali dimana analisis datanya pada infromasi paket data yang dikirimkan. Pada tugas akhir ini menggunakan dua metode, yaitu metode n-gram yang digunakan untuk mengitung distribusi byte karakter pada paket data sedangkan metode

mahalanonis distance digunakan untuk menghitung jarak antara paket data normal dan paket data yang berupa intrusi.

Metode mahalanobis distance dapat membedakan paket data yang normal dan paket data yang berupa intrusi dengan menghitung rata-rata dan standar deviasi dari paket data.

Kata kunci : N-Gram, Mahalanobis Distance, Incremental Learning

EVALUATION OF ANOMALY BASED INTRUSION DETECTION SYSTEM WITH N-GRAM AND INCREMENTAL LEARNING

Student's Name	**: I MADE AGUS ADI WIRAWAN**
Student's ID	**: 5112100036**
Department	**: Teknik Informatika FTIF-ITS**
First Advisor	**: Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D.**
Second Advisor	**: Baskoro Adi Pratomo, S.Kom., M.Kom.**

Abstract

The rapid development of information technology is inevitable wich made its necessity is growing every single day. Data transaction through internet has become the primary need of most software nowadays. Software like social media, cloud server, online game, e-government, remote application, etc. With the various needs of the internet, it is obvious that we need a method that can guarantee its safety.

IDS which stands for Intrusion Detection System is the solution to protect the internet network. This system will decide wether a packet is safe or dangerous for the network depends on certain condition. Nowadays many IDS (Intrusion Detection System) has been developed, but most are developed base signature or use the rule, and a small part sing anomaly. Anomaly is a method to look for irregularities in the data.

In this application IDS concept that is applied is based anomaly in which the data analysis on the data packets transmitted. In this thesis using two methods, the n-gram method used to calculate the distribution of byte character data paket while the mahalanobis distance methods used to calculated the distance between the normal data packets and intrusion data packets.

Mahalanobis distance methods can distinguish between normal data packets and intrusion data packets by calculating the average and standar deviation of the data packets.

Keyword : N-Gram, Mahalanobis Distance, Incremental Learning

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PERSAMAAN

BAB VI
KESIMPULAN DAN SARAN

Pada bab ini akan dibahas mengenai kesimpulan yang dapat diambil dari perancangan sistem hingga hasil pengujian. Selain itu juga akan dibahas mengenai hasil yang sudah dicapai dan belum dicapai. Pada bab ini juga akan menjawab pertanyaan yang dikemukakan pada Bab 1. Pada penutup ini juga terdapat saran-saran untuk pengembangan selanjutnya.

6.1 Kesimpulan

Dalam proses pengerjaan Tugas Akhir yang melalui tahap perancangan, implementasi, serta uji coba, didapatkan kesimpulan sebagai berikut :

1. Metode Mahalanobis *Distance* dapat digunakan untuk mengklasifikasikan antara paket data normal dan paket data yang berupa intrusi, namun tidak berlaku untuk protokol HTTP.
2. Sistem yang dibuat untuk pendeteksi intrusi menggunakan metode Mahalanobis *Distance* tanpa proses *incremental learning* dapat mendeteksi intrusi dengan persentase kebenaran sekitar 93%, namun dengan tambahan proses *incremental learning* hanya dapat mendeteksi intrusi dengan persentase kebenaran sekitar 20%. Dari hasil tersebut, dengan tambahan proses incremental learning mangurangi tingkat akurasi pendeteksian intrusi.

6.2 Saran

Adapun saran-saran yang diberikan untuk pengembangan sistem ini selanjutnya adalah karena membedakan paket data normal dengan paket data serangan menggunakan metode mahalanobis *distance* dengan proses *incremental learning* kurang akurat dibandingkan tanpa proses *incremental leraning*. Hal ini dikarenakan dengan menambahkan proses *incremental learning*,

rata-rata dan standar deviasi pada model diperbaharui tetapi *threshold* yang digunakan untuk mendeteksi intrusi tidak diperbaharui, sehingga *threshold* yang ada tidak akurat untuk mendeteksi intrusi. Perlu ada implementasi metode lain sehingga dapat membantu meningkatkan keakuratan pendeteksian intrusi.

DAFTAR PUSTAKA

[1] SANS Institute, "Understanding Intrusion Detection System," *SANS Institute Reading Room,* pp. 1-9, 2001.

[2] "Intrusion detection system," [Online]. Available: https://en.wikipedia.org/wiki/Intrusion_detection_system. [Diakses 22 June 2016].

[3] K. Fuji, "a Java library for capturing and sending network packets," Jpcap, 15 May 2007. [Online]. Available: http://jpcap.gitspot.com/. [Diakses 23 May 2016].

[4] A. Hanafi, "Pengenalan Bahasa Suku Bangsa Indonesia Berbasis Teks Menggunakan Metode N-gram. IT TELKOM," 2009.

[5] "Mahalanobis distance," [Online]. Available: https://en.wikipedia.org/wiki/Mahalanobis_distance. [Diakses 22 June 2016].

[6] D. E. Knuth, "The Art of Computer Programming," *Fundamental Algorithms. Addison Wesley*, vol. 1, 1973.

[7] MIT Lincoln Laboratory, "MIT Lincoln Laboratory: Cyber system & technolog: DARPA Intrusion Detection," MIT Lincoln Laboratory, [Online]. Available: https://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/docs/index.html. [Diakses 23 Mei 2016].

[8] V. Galleys, "Cross Validation," 2006. [Online]. Available: http://www.cse.iitb.ac.id/~tarung/smt/papers_ppt/ency-cross-validation.pdf. [Diakses 24 June 2016].

[9] Kohavi, "Confusion Matrix," 1999. [Online]. Available: http://www2.cs.uregina.ca/~dbd/cs831/notes/confusion_matix/confusion_matrix.html. [Diakses 24 June 2016].

BIODATA PENULIS

I Made Agus Adi Wirawan, lahir di Desa Celagi, 4 Agustus 1994. Penulis adalah anak kedua dari dua bersaudara. Menempuh pendidikan di SD No. 3 Denbantas, SMP Negeri 1 Tabanan, SMA Negeri 1 Tabanan, dan terakhir melanjutkan kuliah di jurusan Teknik Informatika – ITS.

Selama berkuliah penulis aktif dalam kegiatan dan organisasi keprofesian informatika sebagai administrator sekaligus koordinator laboratorium Arsitektur dan Jaringan Komputer. Pernah mengikuti dan mendapatkan sertifikasi HCNA-WCDMA yang diselenggarakan oleh Huawei.

Selain itu, penulis juga aktif dalam organisasi kampus sebagai anggota Himpunan Mahasiswa Teknik Computer-Informatika, staf departemen dalam negeri dan menjadi panitia berbagai kegiatan di tingkat jurusan maupun fakultas.

Selain menjalankan tugas mahasiswa, penulis juga aktif menjadi asisten dosen mata kulish sistem operasi, jaringan komputer, dan keamanan informasi dan jaringan, disamping asisten dosen juga sekaligus menjadi asisten praktikum untuk mata kuliah sistem operasi dan jaringan komputer,

Ketertarikan penulis dibidang informatika berada pada bidang sistem teknologi informasi, sekuritas jaringan, perancangan keamanan sistem dan jaringan, teknologi antar jaringan, dan teknologi tepat guna.

Penulis dapat dihubungi dengan mengirimkan pesan elektronik ke alamat imadeagus.04@gmail.com.