Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini pengguna internet di dunia telah mencapai 3.675.824.813 pengguna. Indonesia menjadi negara pengguna internet no 3 terbanyak di Asia yaitu sebanyak 132.700.000 pengguna pada juni 2016 (www.internetworldstats.com). Hal ini menandakan bahwa jaringan internet merupakan teknologi dengan perkembangan yang sangat pesat. Dengan demikian internet dapat membuat urusan kita dalam mencari dan berbagi informasi lebih mudah dan efisien, serta berkomunikasi menjadi lebih murah dan sederhana (Sudarma, 2010).

Jaringan komputer atau kumpulan jaringan kecil dari jaringan internet merupakan sebuah sistem yang terdiri dari berbagai komputer dan komponen-komponen komputer yang saling terkoneksi satu sama lainnya (Sudarma, 2010). Dengan demikian jaringan komputer dapat memberikan kita kemudahan dalam berbagi informasi dan data (Sudarma, 2010). Jaringan komputer menjadi sangat penting karena mempunyai tujuan yang menguntungkan bagi manusia, keuntungan tersebut seperti *Resource Sharing* (Berbagi Sumber), *High Reliability* (kehandalan tinggi), dan *Scalability* (Skalabilitas) (Tannenbaum, 2003 di kutip oleh Silitonga dan Morina, 2014)

Seiring dengan kemudahan yang didapatkan dari jaringan komputer, bukan berarti tidak mengalami masalah. Masalah tersebut adalah sebuah serangan terhadap jaringan komputer, salah satu contoh bentuk serangan seperti *Buffer Overflow, DOS attack, SMB Probes, OS Fingerprint* dan lain-lain (Takyudin, 2012). Serangan dapat membuat tiga aspek penting dalam jaringan komputer menjadi terganggu yaitu : penyusup mempunyai akses ke informasi atau data rahasia, keaslian informasi dapat dimodifikasi oleh penyerang dan ketersedian akan informasi menjadi tidak dapat digunakan secara normal (Soleiman dan Fetanat 2014). Bentuk nyata serangan tersebut bisa dilihat pada kasus serangan

yang berhasil direkam dalam bentuk data KDD *(Knowledge Discovery and Data Mining) Dataset Cup* 1999.

KDD *Dataset Cup* merupakan dataset yang dikeluarkan oleh DARPA (*Defense Anvance Research Project Agency*) pada tahun 1998. Data ini digunakan sebagai versi data kompetisi di bidang Data Mining dan Ekplorasi ilmu pengetahuan diseluruh dunia yang diadakan oleh *ACM SIGKDD* (*Special Interest Group on Knowledge Discovery and Data Mining*). Organisasi ini menyelenggarakan kompetisi tersebut pada setiap tahun dengan fokus yang berbeda-beda. Pada tahun 1999 kompetisi KDD Cup berfokus kepada *Intrusion Detection and Report*. *Intrusion Detection and Report* merupakan suatu dataset laporan intrusi serangan pada jaringan komputer (www.kdnuggets.com), dan dengan adanya kebijakan keamanan yang baik analisa yang baik terhadap intrusi akan membuat sistem yang lebih aman dari intrusi.

Intrusion Detection Sistem (IDS) merupakan sistem yang digunakan dalam mendeteksi akan adanya serangan pada jaringan. IDS adalah sebuah sistem perangkat lunak atau perangkat keras yang bertugas sebagai pendeteksi dan memonitoring aktivitas mencurigakan yang sedang terjadi dalam sebuah sistem atau jaringan (Bace dan Mell, 2005 di kutip oleh Ulfa, 2013). IDS memantau atau memonitoring setiap aktivitas yang mencurigakan pada jaringan komputer berdasarkan parameter-parameter yang telah ditentukan. IDS memiki dua cara kerja dalam menganalisa paket, apakah paket yang di analisa merupakan serangan atau hanya paket normal (Ulfa, 2013). Cara kerja IDS tersebut yaitu : *Knowledge-based* atau *misuse detection* dan *Behavior based* (*anomaly*). *Knowledge-based* adalah mengenali dengan membandingan paket data *rule* IDS dengan paket data yang sedang dinalisa, jika paket data tersebut memiliki pola yang sama dengan pola di *database rule* IDS maka paket tersebut dianggap sebagai serangan. Begitu juga sebaliknya jika pola paket data di *database rule* tidak sama dengan paket data yang dianalisa maka paket tersebut dianggap bukan serangan (Ulfa, 2013). *Behavior based* (*anomaly*) mendeteksi serangan dengan mengamati adanya kejanggalan atau penyimpangan yang terjadi pada sistem dari kondisi normal. Pada penelitian ini memakai cara kerja *Knowledge Based* karena cara kerja

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Knowladge Based sesuai dengan sistem yang akan dibangun dengan mencocokkan paket data atau *rule* serangan (Ulfa, 2013).

Dalam pengembangannya, IDS juga dapat dibangun dengan teknik *Machine Learning Based* atau dikenal dengan *Intelligence Intrusion Detection Sistem* (IIDS) (Tsai *et al*. 2009). Teknik *Machine Learning Based* merupakan teknik dengan menggunakan metode dalam pengenalan serangan berdasarkan pola atau *rule* pada data yang ada. Dalam mendeteksi serangan, teknik *Machine Learning Based* dapat dikembangkan dengan bermacam-macam teknik berdasarkan teknik pembelajaran mesin. Misalnya beberapa mesin menerapkan pembelajaran teknik tunggal, seperti Jaringan Syaraf Tiruan, Algoritma Genetika, mesin pendukung *Vector* dan lainnya (Tsai *et al*. 2009). Penelitian dengan menggunakan metode atau menerapkan teknik pembelajaran dalam mengenal serangan sudah banyak dilakukan, contohnya adalah menggunakan Jaringan Syaraf Tiruan.

Jaringan syaraf tiruan adalah representasi buatan dari otak manusia yang ingin selalu mencoba mensimulasikan proses pembelajaran dari kerja otak manusia (Kusumadewi, 2003 dikutip oleh Ranadhi, Indarto dan Hidayat 2006). Jaringan syaraf tiruan memiliki beberapa metode yang dapat digunakan dalam melakukan pembelajaran, salah satunya adalah metode *Learning Vector Quantization* (LVQ). *Learning Vector Quantization* (LVQ) merupakan metode dari jaringan syaraf tiruan yang dapat mengklasifikasikan berdasarkan pembelajaran pada lapisan kompetitif yang terawasi (Budianita dan Arni 2015). Lapisan kompetitif ini akan secara otomatis belajar untuk mengklasifikasikan *vector-vector* masukan. Kelas-kelas yang didapat dari hasil kompetitif berdasarkan data jarak antara *vector-vector* masukan. Jika dari kedua *Vector* tersebut mendekati sama maka lapisan kompetitif akan meletakakan kedua *vector* tersebut pada lapisan kelas yang sama (Dessy, Irawan 2012). Berdasarkan penelitian dari Soleiman dan Fetanat, 2014 dengan kasus *Intrusion Detection Sistem*, metode LVQ menghasilkan tingkat akurasi 81 %. Dari tingkat akurasi tersebut, untuk mencoba meninggkatkan akurasi penelitian selanjutnya, maka

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU

penelitian ini akan mencoba menggunakan metode dari perkembangan metode LVQ, salah satunya adalah LVQ 2.

LVQ 2 adalah metode pengembangan dari LVQ biasa (LVQ 1). Perbedaan dari LVQ 1 dengan LVQ 2 tersebut adalah LVQ 2 tidak hanya memperoses pembelajaran dari *vector* pemenang saja tetapi juga memperoses *vector runner up* atau pemenang kedua dan *vector* (pemenang dan *runner-up*) tersebut akan diperbaharui jika memenuhi kondisi tertentu (Budianita dan Firdaus, 2016). Penerapan metode LVQ 2 pada *machine learning* berfungsi untuk melakukan pengklasifikasian terhadap data serangan yang telah dikumpulkan, data tersebut akan di jadikan inputan dalam pengujian sistem untuk menentukan hasil kelas pada sistem.

Berdasarkan penelitian dari Budianita dan Firdaus (2016) dengan kasus Diagnosis Penyakit Kejiwaan, menyatakan LVQ 2 dalam mengelompokkan data sesuai dengan target asli yaitu mencapai 100 %, semakin sering data dilatih maka tingkat akurasi pengujiannya akan semakin baik dan untuk hasil pengujian nya mencapai 90%. Selanjutnya berdasarkan penelitian dari Ariani (2015) dengan kasus Mendeteksi Penyakit Jantung Coroner (PJK), menyatakan metode LVQ 2 dapat mengklasifikasi Penyakit Jantung Coroner (PJK) dengan akurasi 89.97 % dan selanjutnya Penelitian dari Setiawan (2015) dengan kasus Mengklasifikasi Jenis Penyakit Pada Ayam, menyatakan LVQ 2 dapat Mengklasifikasi Jenis Penyakit Pada Ayam dengan akurasi 89,49 %.

Dari penjabaran di atas, maka akan dilakukan penelitian dengan Penerapan Metode *Learning Vector Quantization* 2 (LVQ 2) untuk Klasifikasi Serangan pada Jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas yang telah dijelaskan, maka rumusan masalah penelitian ini adalah “Bagaimana penerapan Metode *Learning Vector Quantization* 2 (LVQ 2) untuk klasifikasi serangan pada jaringan serta mengetahui tingkat akurasi yang dihasilkan”

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU

1.3 Batasan Masalah

Batasan masalah dalam penelitian tugas akhir ini antara lain sebagai berikut:

1. Data latih dan uji bersumber dari KDD *Dataset Cup* 1999 yang dikeluarkan oleh DARPA, data yang digunakan sebanyak 1000 data dari KDD *Dataset Cup* 1999.
2. Variabel yang digunakan sebanyak 36
3. Kelas *ouput* dari penelitian adalah berupa serangan dan normal.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini yaitu:

1. Mengklasifikasikan ancaman serangan terhadap jaringan komputer menggunakan metode LVQ 2.
2. Mengetahui tingkat akurasi yang dihasilkan dari penerapan metode LVQ 2 dalam mengklasifikasi serangan pada jaringan.

1.5 Sistematika Penulisan

Berikut merupakan rencana susunan sistematika penulisan laporan penelitian tugas akhir yang akan dibuat:

BAB I Pendahuluan

Bab ini berisikan penjelasan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan dari penelitian tugas akhir yang dilakukan.

BAB II Landasan Teori

Bab ini membahas tentang teori-teori umum dan khusus yang berhubungan dengan penelitian ini yaitu Arsitektur Jaringan, TCP/IP, *Intrusion Detection Sistem* (IDS), jaringan syaraf tiruan, *Learning Vector Quantization*, KDD Cup, *Confussion Matrix*, Kajian Penelitian terkait.

BAB III Metodologi Penelitian

Bab ini membahas data penelitian menggunakan Metode *Learnig Vector Quantization* 2 (LVQ 2) dan membahas langkah-langkah yang akan dilaksanakan dalam proses penelitian.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU

BAB IV Analisa dan Perancangan

Bab ini berisi tentanng analisa pembuatan aplikasi penerapan metode LVQ 2 untuk Klasifikasi serangan pada jaringan serta melakukan desain perancangan aplikasi yang akan dibuat.

BAB V Implementasi dan Pengujian

Pada tahap ini membahas proses Implementasi tetang pembuatan aplikasi berdasarkan rancangan yang telah dibuat. Dan pada tahap ini juga akan dilakukan proses pengujian aplikasi setelah pembuatan aplikasi selesai.

BAB VI Kesimpulan dan Saran

Bagian ini berisi kesimpulan yang dihasilkan dari penelitian yang dilakukan serta saran yang bisa membantu dalam pengembangan aplikasi selanjutnya.

Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.
© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU