BAB I

PENDAHULUAN

1.1 Latar belakang

Pengguna internet yang terus meningkat telah mendorong perkembangan infrastruktur jaringan. Banyaknya konten yang ditawarkan melalui media internet telah menjadi trend dalam dunia maya saat ini. Dengan meningkatnya penggunaan internet ini, memicu pesatnya perkembangan teknologi jaringan yang bisa meningkatkan trafik jaringan. Dari tahun ke tahun trafik jaringan terus meningkat, tahun 2013 sebanyak 36,709 PB per bulan dan tahun 2014 kenaikan trafik jaringan sangat signifikan sebanyak 47,176 PB per bulan (Kelechi, 2011).

Meningkatnya pengguna internet dari tahun ke tahun,maka tidak terlepas dari serangan yang timbul dari teknologi jaringan seperti serangan *malware infection*. Oleh karena itu, diperlukan keamanan dalam sistem komputer untuk mencegah dari serangan. Keamanan pada sistem komputer dapat diartikan sebagai usaha melakukan perlindungan data dari sumber yang tidak berhak mangakses, dari perusakan dan kegagalan pemakaian. Pada dasarnya keamanan pada sistem komputer melakukan realisasi terhadap orang yang berhak mengakses informasi. Beberapa tipe serangan yang digunakan untuk teknologi jaringan yang mengancam keamanan sistem komputer, diantaranya dilakukan dengan tipe *malware infection* dari tahun 2009 dan tahun 2010 sangat meningkat (Richardson, 2011).

Peningkatan penyerangan tahun 2009 – 2010 sangat signifikan dari 64% sampai 67%, bentuk-bentuk serangan harus diwaspadai karena dapat merusak sistem dan data yang ada. Untuk itu perlu aplikasi menjaga keamanan komputer dari pihak yang tidak berhak mengaksesnya. Saat ini banyak aplikasi yang bisa digunakan untuk keamanan komputer. Hal tersebut dilakukan sebagai pencegahan terhadap segala bentuk ancaman (*attack*), teknologi yang digunakan untuk mencegah dari ancaman (*Attack*) yang beredar dari hasil data survey CSI/FBI pada tahun 2008 adalah anti virus *software, firewall, Intrusion Detection System*

(IDS), pada survey CSI/FBI *Intrusion Detection System* (IDS) telah diimplementasikan sebesar 62,4% (Richardson, 2011). Hal ini membuktikan bahwa banyak yang menggunakan IDS untuk menjaga keamanan data dari ancaman serangan, IDS merupakan suatu tindakan untuk mendeteksi adanya trafik paket yang tidak diinginkan dalam sebuah jaringan atau *device* (Nugroho, 2009).

Dalam perkembangan aplikasi IDS dapat dibangun dengan menggunakan *Machine Learning Based* yang dikenal dengan *Intelligence Intrusion Detection System* (IIDS). Teknik *Machine Learning* didasarkan pada pembentukan model eksplisit dan implisit yang memungkinkan untuk dianalisis dan dikategorikan sesuai dengan pola data. Didalam *Machine Learning* ada beberapa metode dan algoritma yang digunakan yaitu *Anomaly Detection Algorithm, Local Outlier Factor (LOF) Algorithm, Bayesian Network, Markov Model, Neural Network,Fuzzy Logic,Genetic Algorithm, cluster, k-nearest Neighbor (K-NN)* (Iskandar, 2011). Dari beberapa metode *Machine Learning Based* penelitian ini memilih metode *k-nearest Neighbor (K-NN)* sudah baik dalam mendeteksi serangan (Anisyah, dkk, 2011).

Dengan menerapkan *K-nearest Neighbor(K-NN)* kedalam sistem IIDS diperlukan data serangan untuk menentukan variable- variable *K-nearest Neighbor*. Dalam pengumpulan data serangan dapat dilakukan dengan cara *Sniffing*. *Sniffing* paket berfungsi untuk memonitoring semua paket data yang melalui *interface Ethernet* router. Aplikasi yang digunakan untuk memantau paket data adalah snort. Setelah data semua sudah terkumpul selanjutnya di analisa untuk menentukan K yang dibutuhkan untuk menghitung jarak antara input dan data training.

IDS juga memiliki cara kerja dalam menganalisa apakah paket data yang dianggap sebagai *intrusion* oleh *intruser*. Cara kerja IDS terbagi dua yaitu : *knowledge based , behavior based. Knowledge Based* adalah cara kerja IDS dengan menyadap paket data dan membandingkan dengan data *rules* yang telah ada. *Behavior Base* adalah cara kerja IDS dengan mengamati adanya kejanggalan pada sistem atau adanya kejanggalan dari kondisi normal. Pada penelitian ini memakai cara kerja IDS *knowledge based.*

Pada penelitian yang dilakukan Ririn Dwi jayanti, 2014, metode *K-nearest Neighbor (K-NN)* ketepatan prediksi resiko kredit yang dianalisis sebesar 84,33% pada nilai Kadalah 7. Sedangkan ketepatan prediksi resiko kredit yang dianalisis dengan analisis Diskriminan adalah sebesar 76,5%. Namun pada penelitian sebelumnyametode *K-nearest Neighbor (K-NN)* tingkat akurasinya sudah tinggi pada kasus prediksi resiko kredit di KOPINKRA sumber rejeki, tingkat akurasi yang didapat sebesar 84,33% pada nilai k adalah 7.

Pada penelitian yang dilakukan Novi Anisyah, 2011, aplikasi mobile untuk *K-nearest neoghbor (K-NN)* pada intrusion detection sistem berbasis snort, penelitian ini mendapatkan hasil bahwa metode KNN sudah baik untuk mendeteksi serangan jika dibandingkan dengan fuzzy maka semakin besar data base dan semakin kecil K makan persen bedanya semakin kecil.

Berdasarkan penelitian sebelumnya maka penelitian ini akan membuat aplikasi *Intelligence Intrusion Detection System* (IIDS) dengan menggunakan metode *K-nearest Neighbor (K-NN)* untuk mendeteksi serangan pada jaringan. Inputan parameter pada penelitian ini adalah protokol, *Destination Bytes* dan frekuensi, hasil dari inputan atau *output* dari aplikasi IIDS adalah serangan atau bukan serangan. Diharapkan pada penelitian ini metode *KNN* mampu memprediksi dengan akurasi yang tepat.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dapat dirumuskan rumusan masalah, yaitu Bagaimana mendeteksi serangan dalam jaringan dengan *Intelligence Intrusion Detection System* (IIDS) menggunakan metode *K-nearest Neighbor (K-NN).*

1.3 Batasan masalah

Dalam melakukan suatu penelitian, diperlukan batasan-batasan agar penelitian tidak menyimpang dari yang telah direncanakan, sehingga tujuan yang sebenarnya dapat dicapai. Adapun batasan masalah penelitian ini :

1. Pada penelitian ini menggunakan data latih yang diambil dari KDD *dataset* cup 1999 yang dikeluarkan oleh DARPA *(Defense Advances Research Project Agancy)* sebanyak 200 data.

2. Paket – paket serangan yang dideteksi adalah paket normal, paket UDP (*user datagram protocol*) *flooding*, paket TCP (*transmission control protocol*) *flooding*, paket ICMP (*internet control message protocol*) *flooding.*
3. Parameter keanggotaan *K-NN*: Frekuensi, Protokol dan *Destination Bytes.*
4. Kelas *output* pada penelitian ini adalah serangan atau bukan serangan.

1.4 Tujuan

Adapun tujuan dari pembuatan tugas akhir ini adalah membuat aplikasi IIDS menggunakan metode KNN untuk mendeteksi serangan sebagai upaya peningkatan keamanan jaringan.

1.5 Sistematika Penulisan

Laporan penelitian ini terdiri dari enam bab, dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Berisikan tentang latar belakang permasalahan, rumusan masalah, batasan masalah, tujuan dipenelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bagian ini membahas teori-teori yang mendukung dalam proses pengerjaan penelitian yang akan dibuat. Teori yang digunakan dalam penelitian ini yaitu tentang *Intelligence Intrusion Detection System* (IIDS) menggunakan metode *K-nearest Neighbor(K-NN).*

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang rangkaian tahapan dalam penelitian, tahapan pengumpulan data, analisa kebutuhan sistem, perancangan perangkat lunak, implementasi, pengujian sistem dan waktu penelitian.

BAB IV ANALISA DAN PERANCANGAN

Bab ini membahas analisa proses mendeteksi serangan yang datang dengan *Intelligence Intrusion Detection System* (IIDS) menggunakan metode *K-nearest Neighbor(K-NN).*

BAB V IMPLEMENTASI DAN PENGUJIAN

Berisikan penjelasan mengenai *Intelligence Intrusion Detection System* (IIDS) menggunakan metode *K-nearest Neighbor(K-NN)*.

BAB VI PENUTUP

Bab ini berisi tentang kesimpulan dan saran yang dimaksudkan agar sistem yang telah dibuat dapat dikembangkan menjadi lebih baik lagi.