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

BAB II
LANDASAN TEORI

2.1 Arsitektur jaringan

Arsitektur jaringan komputer terdiri dari protokol dan komponen yang dibutuhkan dalam menjalankan sebuah sistem. Dan satandar untuk menggambarkan arsitektur jaringan adalah model referensi *Open Sistem Interconnect* (OSI) pada 1977 yang dikembangkan oleh *Organization for Standarization* (ISO) yang dikenalkan pada tahun 1984. Standar model referensi OSI berguna dalam menggambarkan beberapa standar jaringan serta interoperabilitas nya dan termasuk dalam penggambaran jaringan *wireless* serta dalam setiap lapisan OSI tersebut mengilustrasikan fungsi-fungsi dari jaringan (Nethanel, Junior dan Harianto. 2009).

Berikut pembagian fungsi-fungsi dari jaringan berdasarkan lapisan OSI yaitu :

1. Lapisan ke 7-*Application*

   Lapisan yang dapat memberikan layanan jaringan kepada pengguna sistem, berisikan protokol-protokol yang umum biasa digunakan oleh pengguna. Dengan demikian lapisan ini merupakan sistem yang paling dekat dengan pengguna.
2. Lapisan ke 6-*Presentation*

   Merupakan lapisan yang bertugas dalam menentukan format data yang akan dipindahkan diantara sistem dan informasi tersebut dikelola oleh lapisan sistem sehingga informasinya dapat dibaca oleh lapisan sistem pada sistem lain. Pada lapisan ini menyediakan berupa pelayanan transformasi format data, enkripsi dan kompresi.
3. Lapisan ke 5-*Session*

   Lapisan yang berfungsi sebagai penyelenggara, mangatur, dan memutuskan sesi komunikasi. Lapisan ini menyediakan pelayanan terhadap lapisan *presentation*, mangatur men-singkronisasikan dialog antara dua komputer pada lapisan *Presentation* serta mengatur pertukaran data.

4. Lapisan ke 4-*Transfort*

   Merupakan lapisan yang memiliki fungsi sebagai pemecah paket-paket yang akan dikirim, dan menyusun paket-paket tersebut kembali menjadi informasi yang dapat diterima.

5. Lapisan ke 3-*Network*

   Lapisan berfungsi sebagai penyedia transfer informasi dari ujung sistem melewati beberapa dari jaringan komunikasi berurutan. Pada lapisan ini melakukan pemilihan jalur terbaik dalam komunikasi jaringan terpisah secara geografis.

6. Lapisan ke 2-Data *Link*

   Lapisan ini berfungsi mengubah paket-paket data dalam bentuk *frame*, menghasilkan alamat fisik, pesan-pesan kesalahan, pemesanan pengiriman data. Lapisan ini juga berfungsi sebagai lapisan yang mengupayah kan agar lapisan *physical* dapat bekerja dengan baik dengan mangaktifkannya, dan mempertahankan serta menon-aktifkan hubungan

7. Lapisan ke 1- *Physical*

   Lapisan ini berfungsi dalam menjamin transmisi data berjalan dengan baik dengan cara mengatur karakteristik dari tinggi tegangan, periode perubahan tegangan, lebar jalur komunikasi, jarak minimum dari komunikasi dan koneksi. Pada lapisan ini juga menjamin transmisi data dalam bentuk bit melalui jalur komunikasi.

2.2 TCP/IP

TCP/IP adalah sekumpulan protokol yang terdapat di dalam jaringan komputer (*network*) yang digunakan untuk berkomunikasi atau bertukar data antar komputer. TCP/IP merupakan protokol standar pada jaringan internet yang menghubungkan banyak komputer yang berbeda jenis mesin maupun sistem operasi agar dapat berinteraksi dengan yang lainnya. TCP adalah protokol yang telah diterapkan hampir ke semua perangkat keras dan sistem operasi (Syafrizal, 2005).

© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU
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 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.

2.3 IDS (*Intrusion Detection Sistem*)

IDS (*Intrusion Detection Sistem*) adalah sebuah sistem perangkat lunak atau perangkat keras yang bertugas sebagai pendeteksi dan memonitori aktivitas mencurigakan yang sedang terjadi dalam sebuah sistem atau jaringan (Bace dan Mell, 2005 dikutip oleh Ulfa, 2013). Jadi fokus utama dari IDS itu sendiri adalah memonitoring aset jaringan terhadap kegiatan yang tidak lazim seperti biasanya dan kegiatan yang tidak sesuai (Thomas, 2005 dikutip dalam Ulfa, 2013). IDS sering disebut dengan kunci alarm pencuri, contohnya kunci di buat dengan alarm pencuri untuk menjaga rumah dari pencurian namun jika kunci tersebut dilanggar atau dirusak maka alarm pencuri yang akan mendeteksi dan memberikan tanda kepada pemiliknya bahwa kunci tersebut dirusak atau dilanggar (Vijayarani dan Sylviaa, 2015).

Intrusion Detection Sistem (IDS) dalam melakukan tugasnya berada pada lapisan jaringan OSI *(Open Sistem Interconnection*), OSI ini terdapat pada lapisan ketiga yaitu pada lapisan *Network* dan sensor jaringan pasif yang secara khusus diposisikan pada *choke point* pada jaringan dari metode lapisan OSI.

Dalam pengembangannya IDS 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 menggunakan metode dalam pengenalan serangan berdasarkan pola atau *rule* pada data yang ada. Dalam mendeteksi serangan, teknik mesin banyak dikembangkan dalam bermacam-macam berdasarkan dari teknik pembelajar mesin. Misalnya beberapa mesin menerapkan pembelajaran teknik tunggal, seperti Jaringan Syaraf Tiruan, Algoritma Genetika, mesin pendukung *Vector* dan lainnya. Dari beberapa pembelajaran mesin tersebut penelitian ini akan menggunakan Jaringan Syaraf Tiruan sebagai pembelajarannya (Tsai *et al*. 2009)

2.3.1 Tipe IDS

IDS terbagi kedalam 2 bentuk, yaitu IDS berbasis jaringan (NIDS) dan IDS berbasis *host* (HIDS) (Nethanel, Junior dan Harianto. 2009).

1. *Network-Based Intrusion Detection Sistem* (NIDS)

Network-Intrusion Detection sistem merupakan sebuah pemantauan pada seluruh bagian jaringan komputer dengan cara mengumpulkan paket-paket yang telah dipantau, dan melakukan analisa terhadap paket-paket tersebut apakah normal atau merupakan serangan. NIDS biasa nya dikembangkan di depan dan dibelakang *firewall* dan VPN *gateway* untuk mengukur keefektifan peranti-peranti keamanan dan berinteraksi dengan peranti tersebut untuk memperkuat keamanan jaringan.

2. *Host-based Intrusion Detection Sistem* (HIDS)

   HIDS merupakan pemantaun terhadap bagian tertentu dari jaringan komputer. Salah satu contoh nya memantau kesalahan login yang dilakukan berulang kali dan melakukan pengecekan pada file tersebut.

2.3.2 Karakteristik IDS

Berikut adalah beberapa kriteria untuk menciptakan IDS yang ideal (Balasubramanyan dkk, 2008 dikutip oleh Ulfa, 2013) yaitu:

1. Meminimalkan *overhead* dari sistem untuk tidak mengganggu operasi normal.
2. Konfigurasi yang mudah untuk disesuaikan pada kebijakan keamanan sistem.
3. Mudah dalam proses instalisasi (*deploy*).
4. Mudah dalam beradaptasi dengan perubahan sistem dan perilaku *User*.
5. Mampu memonitori sejumlah *host* dengan tetap menghasilkan hasil yang cepat dan tepat.
6. Dapat meminimalkan dampak negatif.
7. Memungkinkan terjadi konfigurasi yang dinamis, khusus pemantauan yang dilakukan terhadap sejumlah *host* besar.
8. Berjalan secara kontinu.
9. Mampu mendeteksi serangan baik itu yang bersifat *false positive false negative*.
10. Mampu melakukan *recover* dari sistem yang *crash* baik akibat dari insidesial maupun aktivitas tertentu.

© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU
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.

11. Serangan tidak bisa mengubah atau memodifikasi jaringan. Karena IDS mampu memonitori dirinya sendiri dan mendeteksi kalau dirinya telah diubah oleh penyerang.

2.3.3 Implemetasi IDS

Dalam implementasi IDS ada dua hal yang perlu diperhatikan (Nethanel, Junior dan Harianto, 2009) yaitu:

1. Perihal *false positive*

   Merupakan sebuah peringatan serangan yang dihasilkan oleh IDS akan sebuah paket normal pada sistem yang sedang dimonitori.

2. *False Negative*

   Merupakan sebuah serangan yang terjadi akibat dari terlewatkannya serangan oleh IDS sehingga tidak ada pemberitahuan atau peringatan apapun akan ada nya serangan tersebut. IDS tidak dapat mengenali serangan akibat dari IDS yang tidak mengenali serangan atau serangan tersebut menggunakan metode lain supaya terhindar dari IDS.

2.3.4 Cara Kerja IDS

IDS memiliki cara kerja dalam melakukan anlisa apakah paket jaringan tersebut merupakan sebuah serangan atau bukan serangan dan IDS membagi kedalam 2 bentuk analisa cara kerja nya yaitu (Ulfa, 2013):

1. *Knowledge-based* atau *misuse detection*.

   Cara kerja dari *Knowledge-based* adalah mengenali serangan berdasarkan perbandingan 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. Dan begitu juga sebaliknya jika pola paket data di *database rule* tidak sama dengan paket data yang dianalisa maka paket tersebut dianggap bukan serangan.

2. *Behavior based (anomaly).*

   Jenis IDS seperti ini mendeteksi serangan dengan mengamati adanya kejanggalan atau penyimpangan yang terjadi pada sistem dari kondisi normal. Salah satu contohnya adanya koneksi pararel dari 1 buah IP dalam jumlah yang banyak dalam waktu bersamaan atau adanya penggunaan

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

memori yang melonjak secara terus-menerus. Dari semua kejanggalan tersebut dianggap sebagai serangan.

2.3.5 Fungsi IDS

Secara singkat dapat disimpulkan bahwa IDS mempunyai fungsi sebagai pemberi peringatan kepada admimistrator atas adanya sebuah serangan terhadap sistem kita. Alasan dari mempergunakan IDS menurut (Bace and Mell, 2005 dan Balasubraminiyan dkk, 2008 dikutip oleh Ulfa, 2013) adalah :

1. Mencegah resiko timbulnya sebuah masalah dari jaringan.
2. Mencegah suatu pelanggaran dan serangan pada jaringan yang tidak dicegah oleh perangkat lain.
3. Mendeteksi adanya usaha serangan yang berkaitan dengan *probing*, aktivitas *doorknob rattling* dan lainnya.
4. Dapat membuat dokumentsai tentang ancaman jaringan kedalam suatu organisasi, sehingga dapat mengambil keputusan tentang sumber daya jaringan.
5. Sebagai pengendali kualitas pada administrasi dan perancangan keamanan, khususnya pada organisasi yang besar dan komplek.
6. Dapat memberikan informasi tentang serangan yang terjadi, peningkatan diagnosa, *recovery* dan perbaikan dari factor-faktor penyebabnya.

2.4 Normalisasi

Normalisasi adalah merubah data (nilai) yang akan digunakan menjadi skala kisaran 0 sampai 1. Ini bertujuan untuk perhitungan Euclidean, karena atribut yang ber-skala panjang dapat mempunyai pengaruh yang lebih besar dari pada atribut dengan skala pendek. Oleh karna itulah dibutuhkan Normalisasi untuk mencegahnya. (Teknomo, 2016 dikutip oleh Budianita, 2013 dalam Ariani, 2015).

Berikut rumus Normalisasi, yaitu:

$$X^{*} = \frac{X - min(X)}{\max(X) - \min(X)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.1)$$

Penjelasan:

X^{*} = nilai setelah selesai dinormalisasi

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

X = nilai sebelum dinormalisasi

min(X) = nilai minimum dari fitur

max(X) = nilai maksimum dari fitur

2.5 Jaringan Syaraf Tiruan (JST)

Jaringan Syaraf Tiruan (JST) merupakan suatu model jaringan yang meniru model sistem pemrosesan informasi menyerupai karakteristik jaringan biologis atau jaringan syaraf tiruan adalah representasi buatan dari otak manusia yang ingin selalu mencoba mensimulasikan proses pembelajaran dari kerja otak manusia. Istilah dari buatan digunakan karena jaringan syaraf tiruan tersebut di implementasikan dengan menggunakan komputer sebagai proses penghitungan selama pembelajaran masih berjalan (Kusumadewi, 2003 dikutip oleh Ranadhi, Indarto dan Hidayat 2006).

JST adalah prosesor tersebar *parallel* yang sangat besar. JST menyerupai otak manusia seperti pengetahuan diperoleh dari hasil pembelajaran, dan kekuatan dari hubungan sel syaraf (neuron) yang disebut sebagai bobot-bobot sinaptik yang digunakan menyimpan pengetahuan. JST diciptakan sebagai suatu generalisasi model matematis dari pemahaman manusia (*human cognition*) berdasarkan asumsi sebagai berikut (Dessy dan Irawan 2012):

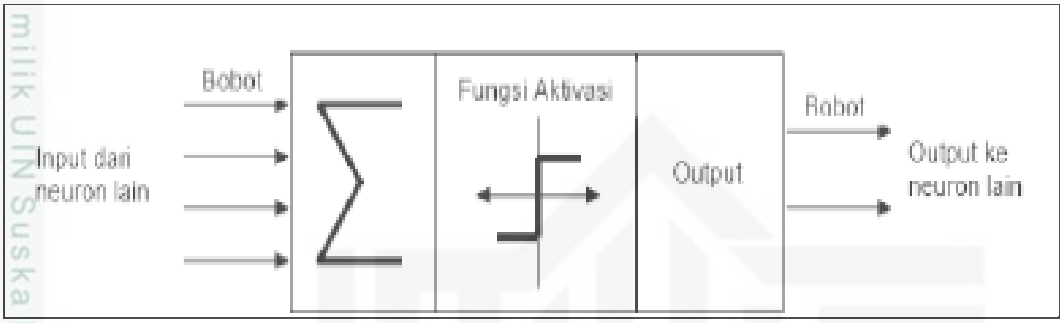
1. Pemrosesan informasi yang terjadi pada elemen sederhana disebut dengan *neuron*
2. Sinyal yang mengalir diantara sel saraf/neuron melalui suatu media sambungan penghubung.
3. Setiap sambungan memiliki bobot yang saling bersesuain. Dan bobot tersebut akan digunakan untuk menggandakan sinyal yang akan dikirim.
4. Setiap sel saraf akan menerapkan fungsi aktivasi terhadap sinyal dari hasil penjumlahan berbobot yang akan masuk kedalamnya untuk menentukan sinyal keluaran.

Dari penjelasan di atas dapat disimpulkan bahwa Jaringan Syaraf Tiruan adalah suatu jaringan syaraf yang cara kerjanya menyerupai cara kerja otak

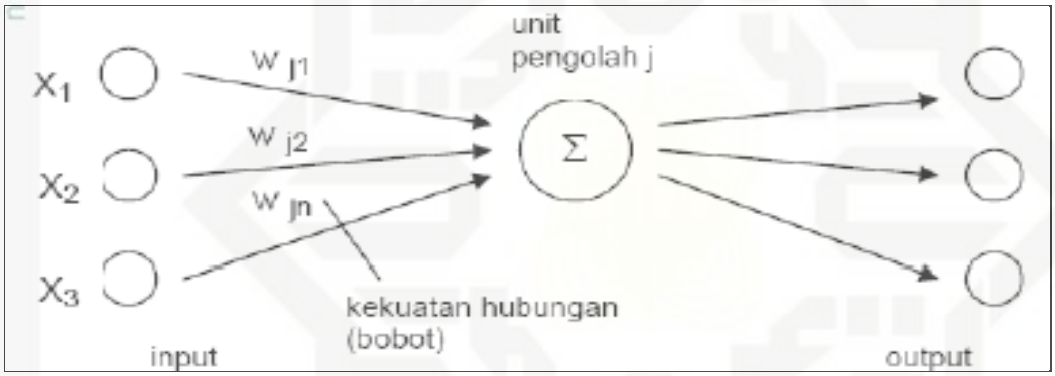
Hak Cipta Dilindungi Undang-Undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan 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

manusia dan hal itu didukung dengan proses pembelajaran dari jaringan tersebut karena selalu ingin men-simulasikan proses kerja otak manusia.

Berikut gambar dari model struktur neuron jaringan Syaraf tiruan:



Gambar 2. 1 Model Struktur Jaringan Syaraf Tiruan (JST)(Dessy dan Irawan 2012)



Gambar 2. 2 Model Struktur Jaringan Syaraf Tiruan (JST)(Dessy dan Irawan 2012)

Berdasarkan perjelasan di atas, Jaringan Syaraf Tiruan meniru sistem jaringan Biologis (Manusia), maka sistem jaringan saraf tiruan tersebut mempunyai 3 karakteristik utama (Siahaan, 2011 di kutip oleh Budianita dan Firdaus, 2016) yaitu :

a. Arsitektur jaringan

   Merupakan pola keterhubungan antara neuron. Keterhubungan tersebut yang membentuk suatu jaringan.

b. Algoritma Jaringan

   Metode yang dapat menemukan nilai bobot hubungan. Pada Algoritma Jaringan Syaraf Tiruan ini terdapat 2 metode yaitu : metode tersebut dapat melakukan pelatihan (Pembelajaran), metode bagaiamana melakukan Pengenalan (Sistem).

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

c. Fungsi aktivasi

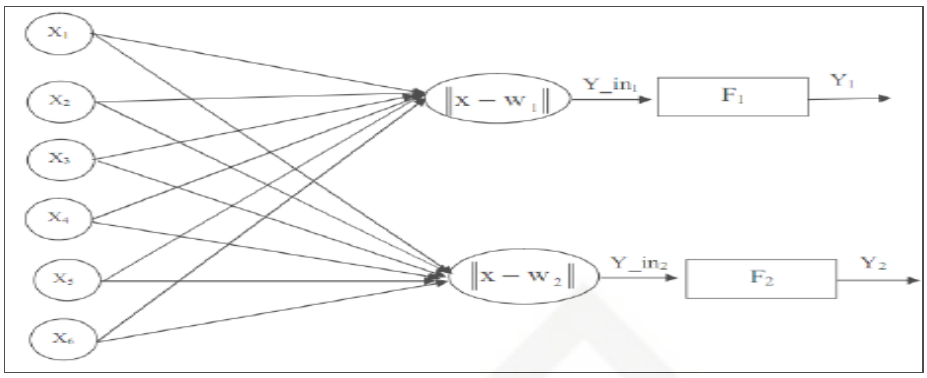
Merupakan metode yang dapat menentukan nilai keluaran berdasarkan nilai total masukan pada neuron. Fungsi aktivasi suatu algoritma jaringan dapat berbeda dengan fungsi aktivasi algoritma lain.

2.6 Learning *Vector* Quantization

Learning Vector Quantization (LVQ) merupakan suatu metode dari jaringan Syaraf Tiruan dengan tipe arsitektur jaringan lapis-tunggal umpan-maju (*Single Layer Feedforward*) yang terdiri dari unit masukan dan keluaran. Metode LVQ disebut juga dengan metode 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 dan Irawan 2012).

LVQ terdiri dari lapisan input (input layer), lapisan kompetitif, dan lapisan *output*. Pada lapisan input dihubungkan dengan lapisan kompetitif oleh bobot, dalam lapisan kompetitif dilakukan proses pembelajaran secara terawasi. Input akan bersaing untuk masuk kedalam suatu kelas (Hidayati dan Warsito, 2010). Lapisan kompetitif ini menghasilkan berupa kelas, kemudian kelas tersebut akan dihubungkan dengan lapisan *output* oleh fungsi aktivasi. Fungsi aktivasi yang digunakan adalah fungsi aktivasi linear dengan tujuan kelas yang didapat nantinya pada lapisan *output* sesuai dengan kelas yang dimasukkan kelapisan *output*. Berikut arsitektur dari LVQ adalah:

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



Gambar 2. 3 Arsitektur *Learning Vector Quantization* (LVQ)(Azmi . 2014)

Keterangan Simbol Gambar 2.3:

X = *Vector* Masukan (x1….,xi….,xn)

F = Lapisan Kompetitif

Y_in = Masukan kelapisan kompetitif

Y = Keluaran(*Output*)

W = *Vector* bobot untuk unit keluaran

||X-W|| = Selisih nilai jarak *Euclidean* antara *vector* input dengan *vector* bobot untuk unit *Output*.

Untuk menghitung jarak euclidean dapat digunakan persamaan berikut.

$$C = \sqrt{(x_1 - w_1)^2 + \ldots + (x_n - w_n)^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.2)$$

Keterangan:

C adalah jarak *euclidean* antara data latih inputan dengan bobot kelas

x_1, x_n adalah nilai – nilai pada data latih inputan

w_1, w_n adalah bobot – bobot pada suatu kelas

Adapun langkah-langkah Algoritma Pelatihan LVQ adalah sebagai berikut:

1. Terapkan: bobot (W), maksimum iterasi (maksimum *epoch*), eror minimum m(Eps), dan *learning rate* α.
2. Masukkan :
   a. Input : X (m,n); dimana m = jumlah input dan n = jumlah data
   b. Target : T (1,n)
3. Tetapkan kondisi awal :
   a. *Epoch* = 0

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

b. Err = 1

4. Kerjakan jika : (*epoch* < maksimum iterasi) atau (α. > Eps)

   a. *Epoch* = *epoch* + 1

   b. Kerjakan untuk i = 1 sampai n

      Tentukan J sehingga $||x-w_j||$ adalah minimum

      Perbaiki w_j dengan ketentuan :

      Jika T = J maka : W_j (baru) = W_j (lama) + α. (X_i-W_j(lama))…...(2.3)

      Jika T ≠ 1 maka : W_j (baru) = W_j (lama) - α. (X_i-W_j(lama))……(2.4)

   c. Kurangi nilai α

      Setelah dilakukan pelatihan, maka akan diperoleh bobot akhir (W). bobot ini nantinya akan digunakan untuk melakukan simulasi atau pengujiam.

      Misalnya dilakukan pengujian terhadap np buah data. Maka algoritma nya yaitu:

      1. Masukkan data yang akan di uji, misal dengan i =1, 2,… np dan j = 1, 2,…,
      2. Kerjakan untuk i=1 hingga np
         a. Tentukan J sedemikian hingga ||Xij-Wij|| minimum
         b. J adalah kelas untuk Xi

Dalam pengembangannya, metode *Learning Vector Quantization* (LVQ) memiliki beberapa variasi salah satunya LVQ 2.

2.7 Learning *Vector* Quantization 2 (LVQ 2)

Learning Vector Quantization 2 (LVQ 2) adalah metode yang tidak jauh beda dengan metode LVQ 1, perbedaannya terletak pada algoritma LVQ 1 *vector* referensi yang dekat input saja yang akan diperbaharui. Sedangkan pada LVQ 2 dua *vector* (pemenang dan *runner-up*) akan diperbaharui jika kondisi tertentu telah dipenuhi (Budianita dan Firdaus, 2016). Ide dari pengembangan algoritma LVQ adalah jika input dari *vector* memiliki jarak yang sama dengan *vector* pemenang dan *runner-up* maka akan dilakukan pembelajaran terhadap pembelajan terhadap *vector* tersebut (Fausett, L., 1994) dalam (Budianita dan Firdaus 2016).

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

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

Jadi LVQ 2 adalah algoritma hasil pengembangan dari LVQ awal (LVQ 1), kondisi dimana kedua *vector* diperbaharui jika (Budianita dan Firdaus, 2016):

1. Unit pemenang dan *runner-up* (*vector* terdekat kedua) mempresentasikan kelas yang berbeda
2. *Vector* masukan mempunyai kelas yang sama dengan *runner-up*
3. Jarak *vector* masukan antara *vector* pemenang dan *runner-up* kira-kira sama.

Kondisi tersebut dapat dilihat pada notasi berikut :

X *vector* masukan saat ini

Yc *vector* referensi terdekat dengan X

Yr *vector* referensi terdekat berikutnya dengan X (*Runner-up*)

Dc jarak dari X ke Yc

Dr jarak dari X ke Yr

Vector referensi bisa diperbaharui jika masuk ke dalam daerah yang disebut *Window* (ε). *Window* yang digunakan memperbaharui *vector* referensi didefinisikan sebagai berikut:

$$\frac{dc}{dr} > 1-\in, \frac{dc}{dr} > 1+\varepsilon \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.5)$$

Dengan nilai ε tergantung dari jumlah data pelatihan. Berdasarkan kohonen (1990a) dalam Fausett (1994) nilai ε = 0,3 merupakan nilai yang disarankan. *Vector* Yc dan Yr akan dilakukan perbaharui jika kondisi 1, 2 dan 3 terpenuhi. *Vector* Yc dan Yr diperbaharui dengan menggunakan persamaan:

$$Yc\,(t+1) = Yc(t)-\alpha(t)\,[X(t)-Yc(t)] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.6)$$

$$Yr\,(t+1) = Yr(t)+\alpha(t)\,[X(t)-Yr(t)] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (2.7)$$

Berikut tahapan algoritma LVQ 2 yaitu:

1. Inisialisasi bobot *w* dan *j*
2. Input α (*learning rate*) atau derajat pembelajaran dan ε (*window*)
3. Untuk setiap *vector* pelatihan *W* temukan j sehingga $|X_i-W_j|$ bernilai minimum.
4. Perbaiki W_j dengan ketentuan :
   a. Jika $T = Cj$ maka $Wj = Wj + \alpha\,(Xi-Wj)$
   b. Jika $T \neq Cj$ maka $D_1 > (1-\varepsilon) * D_2$ AND $D_2 < (1+\varepsilon) * D_1$

Jika *true* maka W yang tidak termasuk veltor X diperbaharui sebagai berikut:

$YC_j\ (t+1) = YC_j\ (t) - \alpha(t)[X(t) + YC_j(t)]$

Sedangkan *W* termasuk *vector X* diperbaharui sebagai berikut :

$YC_j\ (t+1) = YC_j\ (t) + \alpha(t)[X(t) + YC_j(t)]$

c. Maka akan diperoleh W_j baru

Jika *false* maka $W_j = W_j - \alpha\ (X - W_j)$

d. Lakukan pengurangan α.

Berikut contoh perhitungan menggunakan jaringan syaraf tiruan LVQ 2 untuk mencari *vector* bobot masing-masing kelas, pada perhitungan ini terdapat dua kelas yang berbeda (kelas 1 dan 2). Seperti pada tabel 2.1 (Ariani, 2015 oleh Nugroho, 2011 dalam Budianita, 2013)

Tabel 2.1 contoh perhitungan data pelatihan *vector* dengan ukuran 1x4

(x1, x2, x3, x4)	T
1100	1
0001	2
0011	2
1000	1
0110	2

Pelatihan

Ambil dua *vector* masukan pertama sebagai inisialisasi bobot awal masing-masing kelas

Bobot awal kelas ke-1	w1 = (1, 1, 0, 0)
Bobot awal kelas ke-2	w2 = (0, 0, 0, 1)
Learning rate	α = 0.1 dengan nilai α akan dikurangi sebesar 0.1 α pada akhir *epoch* saat ini
Window	ε = 0.3

Epoch-1

a. *Vector* masukan 0 0 1 1

$D1 = \text{sqrt}\ ((0-1)^2 + (0-1)^2 + (1-0)^2 + (1-0)^2\ ) = 2$

$D2 = \text{sqrt}\ ((0-0)^2 + (0-0)^2 + (1-0)^2 + (1-1)^2) = 1$

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

Jarak terdekat dalah D2 sehingga J = 2 yang menujukkan *vector* masukan masuk kategori 2 (C_2) sehingga C2 = T dengan T = 2, sehingga bobot w2 diperbaiki dengan persamaan 2.2 :

W2 (baru) = (0, 0, 1, 1) + 0.1 * {(0, 0, 1, 1) – (0, 0, 0, 1)} = (0, 0, 0, 1.1)

b. *Vector* masukan 1 0 0 0

Jarak terdekat adalah D1 sehingga J = 1, sehingga C_1 = T dengan T dengan T = 1, sehingga bobot w1 (baru) = (1, 0.9, 0, 0)

c. *Vector* masukan 0110

D1 = 1.418

D2 = 1.792

Jarak terdekat adalah D1 sehingga J = 1, tapi C1 ≠ T dengan T = 2, maka perlu diperiksa apakah jarak *runner up* (D2) masih masuk kedalam *window* ε = 0.3 dengan menggunakan persamaan (2.5). Pernyataan kondisional ((D1) > (1- ε) * D2) AND ((D2) < (1 + ε) * D1) akan menghitung ((1.418) > (0.7 * 1.792)) AND ((1.792) < (1.3 * 1.418) menghasilkan (*True AND True*), jadi hasil akhirnya adalah *True* sehingga bobot w1 dan w2 diperbaharui dengan persamaan (2.6) (2.7)

W1 (baru) = (1, 0.9, 0, 0) – 0.1 * {(0, 1, 1, 0) – (1, 0.9, 0, 0)}

= (1.1, 0.89, -0.1, 0)

W2 (baru) = (0, 0, 0, 1.1) + 0.1 * {(0, 0, 0, 1.1) – (0, 0, 0, 1.1)}

= (0, 0.1, 0.1, 0.99)

Namun, jika nilai *window* nya *False* maka bobot diperbaharui dengan persamaan pada LVQ (LVQ1) yaitu:

Wj = Wj – α (X – Wj) atau W(baru) = W(lama) – α (X – W)

d. Kurangi nilai α

α(baru) = α(lama) – 0.1 α(lama) = 0.1 – 0.1 * 0.1 = 0.09

e. Tes Kondisi berhenti

Jika jumlah *epoch* telah melebihi jumlah maksimal *epoch* yang diperbolehkan, jika nilai α lebih kecil dari nilai maksimum error.

© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
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.

2.8 KDD CUP

KDD CUP merupakan suatu 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 menyelengarakan 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 data laporan intrusi serangan pada jaringan komputer yang dapat digunakan sebagai acuan data latih dan uji untuk mendeteksi ancaman serangan (www.kdnuggets.com).

KDD Cup adalah dataset yang dikeluarkan oleh DARPA (Defense Anvanced Research Projects Agency) dan dikelola oleh MIT Loncoln Lbs. Kumpulan dari data ini digunakan sebagai alat kompetisi internasional ilmu pengetahuan dan data mining yang ke 3, yang diadakan secara bersamaan dengan konfrensi internasional ilmu pengetahuan dan data mining KDD-99 yang ke lima, tujuan dari kompetisi adalah untuk membangun detektor intrusi jaringan, yang mampu membuat model perbedaan prediksi antara koneksi "buruk" disebut dengan gangguan atau serangan dan baik disebut koneksi normal (http://kdd.ics.uci.edu)

Adapun atribut dari dataset KDD CUP 1999 dapat dilihat Tabel 2.2:

Tabel 2.2 Atribut data KDD CUP 1999

No	*Fitur*	Deskripsi
1	*Duration*	Lama (detik) koneksi
2	*protocol_type*	Tipe protokol (tcp, udp, dll)
3	*service*	Network service di destination (http, telnet, dll)
4	*Flag*	flag
5	*scr_bytes*	Jumlah bytes dari source ke destination
6	*dst_bytes*	Jumlah bytes dari destination ke source
7	*Land*	Status koneksi, normal atau error
8	*wrong_fragment*	Jumlah fragment yang salah
9	*Urgent*	Jumlah paket yang urgent
10	*Count*	Jumlah koneksi ke host yang sama dengan koneksi yang ada sekarang dalam rentang 2 detik
11	*serror_rate*	% dari keneksi yang terdapat “SYN” error
12	*rerror_rate*	% dari koneksi yang terdapat “REJ” error
13	*same_srv_rate*	% dari koneksi ke service yang sama
14	*diff_srv_rate*	% dari koneksi ke service yang berbeda
15	*srv_count*	Jumlah koneksi ke service yang sama terakhir

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.

No	*Fitur*	Deskripsi
16	*srv_serror_rate*	% dari koneksi yang terdapat “SYN”
17	*srv_rerror_rate*	Error % dari koneksi yang terdapat
18	*srv_diff_host_rate*	% dari koneksi ke host yang berbeda
19	*dst_host_count*	Jumlah koneksi ke host yang sama dengan koneksi ke host yang sama sekarang dalam rentang 2 detik
20	*dst_host_serror_rate*	% dari koneksi yang terdapat “SYN” error
21	*dst_host_rerror_rate*	% dari koneksi yang terdapat “REJ” error
22	*dst_host_same_srv_rate*	% dari koneksi ke service yang sama
23	*dst_host_diff_srv_rate*	% dari koneksi ke service yang berbeda
24	*dst_host_srv_count*	% dari koneksi yang terdapat “REJ”error
25	*dst_host_srv_serror_rate*	% dari koneksi yang terdapat “REJ”error
26	*dst_host_srv_rerror_rate*	% dari koneksi yang terdapat “REJ”error
27	*dst_host_srv_diff_host_rate*	% dari koneksi ke host yang berbeda
28	*dst_host_same_src_port_rate*	% dari koneksi ke port service yang sama
29	*Hot*	Jumlah indicator “hot” secara beruntun
30	*num_failed_logins*	Jumlah percobaan login yang gagal 1
31	*logged_in*	Jika berhasil login, o sebaliknya
32	*num_compromised*	Jumlah kondisi “compromised”
33	*root_sheel*	1 jika root shell didapat, 0 sebaliknya
34	*su_attempted*	1 jika dilakukan percobaan perintah “su root”, 0 sebaliknya
35	*num_root*	Jumlah “root” yang diakses
36	*num_file_creations*	Jumlah operasi pembuaan *file*
37	*num_shells*	Jumlah promt shell
38	*num_access_files*	Jumlah operasi pada *access control files*
39	*num_outbound_cmds*	Berurutan
40	*is_host_login*	1 jika login termasuk dalam daftar “hot” 0 sebaliknya
41	*is_guest_login*	1 jika login adalah “*guest*”, 0 sebaliknya
42	*Class*	Jenis trafik (normal, atau jenis seramgan tertentu)

2.9 Confusion Matrix

Confusion Matrix merupakan cara mem-visualisasi yang biasa digunakan pada *supervised learning*. Setiap kolom pada matrix merupakan contoh kelas prediksi, sedangkan kelas setiap baris mewakili kejadian di kelas sebenarnya. *Confusion Matrix* berisi informasi *actual* dan prediksi pada sistem klasifikasi (Gorunescu, 2011 di kutip dalam Arizona, 2016)

Evaluasi dengan *confusion matrix* menghasilkan nilai *accuracy*, *precision* dan *recall*. Nilai *accuracy* adalah persentase jumlah record data yang di klasifikasi secara benar berdasarkan peng-klasifikasian dari algoritma, *precision* merupakan proporsi kasus yang diprediksi positif dari dari data sebenarnya dan *recall* adalah proporsi kasus positif sebenarnya yang diprediksi secara benar. Berikut perhitungan *accuracy*, *precision* dan *recall* pada *confusion matrix*, yaitu:

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 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

Tabel 2.3 Confusion matrix

Actual class	Predicted Class	
	Serangan	Tidak Serangan
Serangan	A	C
Tidak serangan	B	D

Precision $= \frac{d}{b+d}$ …….. (2.8)

Recall $= \frac{d}{c+d}$ …….. (2.9)

Accuracy $= \frac{a+d}{a+b+c+d}$ X 100% …….. (2.10)

Keterangan :

1. a bernilai benar, karena data serangan menghasilkan data serangan
2. b bernilai salah, karena data serangan menghasilkan data bukan serangan
3. c bernilai salah, karena data bukan serangan menghasilkan data serangan
4. d bernilai benar, karena data bukan serangan menghasilkan data bukan serangan

2.10 Kajian Penelitian Terkait

Dalam melakukan sebuah penelitian dibutuhkan beberapa penelitian terkait yang dapat menunjang proses penelitian agar penelitian dapat berjalan dengan tujuan yang dicapai, berikut penelitian terkait yang dapat menunjang proses penelitian.

Adapun tabel penelitian terkait tentang Metode *Learning Vector Quantization* (LVQ) dapat dilihat pada Tabel 2.4

Tabel 2.4 Penelitian Terkait Tentang Metode LVQ.

Peneliti	Universitas	Judul	Akurasi	Keterangan
Soleiman dan Fetanat (2014)	*Maleke Ashtar Univ. of Tech*	*Using Learning Vector Quantization* (LVQ) *in Intrusion Detection Sistems*	81 %	Pada peneltian ini metode LVQ mengklasifikasi kan data kedalam 5 kelas (Normal, DOS, U2R, R2L, dan Prob), dengan akurasi tertinggi pada serangan DOS dan U2R yaitu 81 %. Pada penelitian ini hasil dari LVQ akan di hybrid metode KNN sehingga akurasi paling tinggi 99 %.
Budianita dan	UIN Suska	Penerapan *Learning*	80 %	Algorima LVQ dapat

Peneliti	Universitas	Judul	Akurasi	Keterangan
Arni (2015)	Riau	*Vector Quantization* Penentuan Bidang Konsentrasi Tugas Akhir (Studi Kasus: Mahasiswa Teknik Informatika UIN Suska Riau) Elvia		mengenal pola dan mengklasifikasikan bidang konsentrasi mahasiswa berdasarkan pembelajaran pola pada mata kuliah wajib dan mata kuliah pilihan.
Hidayati dan Warsito (2010)	UNDIP	Prediksi terjangkitnya pnyakit jantung dengan metode Learning *Vector* Quantization	66,79 %	LVQ mampu mengenali pola atau mengklasifikasi berdasarkan kedekatan jarak antar kelompok.

Adapun tabel penelitian terkait tentang Metode *Learning Vector Quantization* 2(LVQ 2) dapat dilihat pada tabel 2.5.

Tabel 2.5 Penelitian Terkait Tentang Metode LVQ2.

Peneliti	Universitas	Judul	Akurasi	Keterangan
Budianita dan Firdaus (2016)	UIN Suska Riau	Diagnosis Penyakit Jiwa Menggunakan Jaringan Syaraf Tiruan *Learning Vector Quantization* 2 (LVQ 2)	90 %	Metode LVQ 2 dapat diterapkan dalam mengklasifikasi penyakit jiwa dengan 132 data latih dan 30 data uji dengan akurasi paling tinggi 90 % dimana *window* yang digunakan 0,4
Ariani (2015)	UIN Suska Riau	Penerapan Jaringan Syaraf Tiruan Untuk Deteksi Penyakit Jantung Coroner (PJK) Menggunakan Metode *Learning Vector Quantization* 2 (LVQ 2)	93,3 %	Dari pengujian metode LVQ 2 dapat mengenali pola dan mampu mendeteksi factor-faktor jantung yang menyebabkan jantung coroner. Dimana akurasi tertinggi didapat dengan *window* 0,3
Arizona (2016)	UIN Suska Riau	Identifikasi Kesesuaian Lahan Tanam Untuk Budidaya Tanaman Pangan Dengan Menggunakan Metode *Learning Vector Quantization* 2 (LVQ 2)	90,91 %	Metode LVQ 2 dapat mengidentifikasi kesesuai lahan tanam untuk budidaya tanaman pangan berdasarkan pengklasifikasian algoritma LVQ 2, dengan menggunakan variabel kesesuaian sebanyak 22 karakteristik lahan dan 11 jenis tanaman pangan, dimana akurasi yang didapat dari pengujian 90,91% dengan nilai *window* 0,5
Setiawan (2016)	UIN Suska	Penerapan Metode	87,49 %	Metode dapat

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

Peneliti	Universitas	Judul	Akurasi	Keterangan
	Riau	Jaringan Syaraf Tiruan *Learning Vector Quantization* 2 (LVQ 2) Untuk Mengklasifikasi Jenis Penyakit Pada Ayam		mengklasifikasi jenis penyaki pada ayam berdasarkan variabel yang telah dientukan dan dengan data latih 70 buah dan 14 data uji. Dan penggunaan *window* dan *learning rate* sangat mempengaruhi tingkat akurasi penelitian.

Adapun tabel penelitian terkait tentang metode yang telah di implementasikan dengan IDS dapat dilihat pada tabel 2.6.

Tabel 2. 6 Penelitian Terkait Metode yang telah di implementasikan dengan IDS

Peneliti	Universitas	Judul	Akurasi	Keterangan
Mahrus , Mazharuddin dan Pratomo (2013)	Institut Teknologi Sepuluh November (ITS)	Sistem Pendeteksi Serangan Adaptif Dengan Menggunakan Algoritma Genetik	83,45 % menggunakan *dataset* NSL KDD dan 62,91 % menggunakan *dataset* DARPA	Pada penelitian menunjukkan akurasi yang baik, dengan jumlah data 200 data dari data NSL KDD dan dataset DARPA dengan masing-masing waktu dibutuhkan dalam pengujian 176,471 dan 300 detik
Wirawan dan Eksistyanto (2015)	Institut Teknologi Sepuluh November Surabaya	Penerapan *Naïve Bayes* Pada *Intrusion Detection Sistem* Dengan Diskritisasi Variabel	89 %	Metode *Naïve Bayes* dapat mendeteksi serangan dengan proses binning pada algorima *naïve bayes*
Susanto (2014)	BSI Yogyakarta	*K-NEARST NEIGBOUR (KNN)* untuk Mendeteksi Gangguan Jaringan Komputer Pada *Intrusion Detection Dataset*	79,36 %	Metode K-NN dapat mendeteksi gangguan pada jaringan dengan akurasi terbesar pada nilai k=1, banyak nya

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

Peneliti	Universitas	Judul	Akurasi	Keterangan
				atribut yang digunakan cukup membuat lama dalam testing.

© Hak cipta milik UIN Suska Riau
State Islamic University of Sultan Syarif Kasim Riau
UIN SUSKA RIAU
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.