

BAB II

LANDASAN TEORI

2.1. Definisi Sistem Pakar

Sistem pakar adalah program yang berbasis pengetahuan yang menyediakan solusi kualitas pakar kepada masalah-masalah dalam bidang (domain) yang spesifik (Luger dan Stubblefield, 2001).

Sistem pakar adalah program komputer yang mempresentasikan dan melakukan penalaran dengan pengetahuan beberapa pakar untuk memecahkan masalah atau memberikan saran (Jackson P, 1999).

Sistem pakar adalah sebuah sistem yang dirancang untuk menirukan keahlian seorang pakar dalam menjawab pertanyaan dan memecahkan suatu masalah. Sistem pakar akan memberikan pemecahan suatu masalah yang didapat dari dialog dengan pengguna (Sutojo T, 2010).

2.1.1. Konsep Dasar Sistem Pakar

Konsep sistem pakar meliputi enam hal berikut:

1. Kepakaran (*Expertise*)

Kepakaran merupakan suatu pengetahuan yang diperoleh dari pelatihan, membaca dan pengalaman. Kepakaran inilah yang memungkinkan para ahli dapat mengambil keputusan lebih cepat dan baik daripada seseorang yang bukan pakar. Kepakaran itu sendiri meliputi pengetahuan tentang:

- a. Fakta-fakta tentang bidang permasalahan tertentu.
- b. Teori-teori tentang bidang permasalahan tertentu.
- c. Aturan-aturan dan prosedur-prosedur menurut bidang permasalahan umumnya.
- d. Aturan *heuristic* yang harus dikerjakan dalam satu situasi tertentu.
- e. Strategi global untuk memecahkan permasalahan.
- f. Pengetahuan tentang pengetahuan (*meta knowledge*)

2. Pakar (*Expert*)

Pakar adalah seorang yang mempunyai pengetahuan, pengalaman dan metode khusus, serta mampu menerapkan untuk memecahkan masalah atau memberi nasehat. Seorang pakar harus mampu menjelaskan dan mempelajari hal-hal yang berkaitan dengan topik permasalahan, jika perlu harus menyusun kembali pengetahuan-pengetahuan yang didapatkan, dan dapat memecahkan aturan-aturan serta menentukan relevansi, kepakarannya. Jadi seorang pakar harus mampu melakukan kegiatan-kegiatan berikut:

- a. Mengenali dan memformulasikan permasalahan.
- b. Memecahkan permasalahan dengan cepat dan tepat.
- c. Menerangkan pemecahannya
- d. Belajar dari pengalaman
- e. Merestrukturasikan pengetahuan
- f. Memecahkan aturan-aturan
- g. Menentukan relevansi

3. Pemindahan kepakaran (*Transferring Expertise*)

Tujuan dari sistem pakar adalah memindahkan kepakaran dari seseorang pakar ke dalam komputer, kemudian ditransfer kepada orang lain yang bukan pakar. Proses ini melibatkan empat kegiatan yaitu:

- a. Akuisisi pengetahuan (dari pakar atau sumber lain)
- b. Representasi pengetahuan (pada komputer)
- c. Inferensi pengetahuan
- d. Pemindahan pengetahuan ke pengguna

4. Inferensi (*Inferencing*)

Inferensi adalah sebuah prosedur (program) yang mempunyai kemampuan dalam melakukan penalaran. Inferensi ditampilkan pada suatu komponen yang disebut mesin inferensi yang mencakup prosedur-prosedur mengenai pemecahan masalah. Semua pengetahuan yang dimiliki oleh seorang pakar disimpan pada basis pengetahuan oleh sistem pakar. Tugas mesin inferensi adalah mengambil kesimpulan berdasarkan basis pengetahuan yang dimilikinya.

5. Aturan-aturan (*Rule*)

Kebanyakan *software* sistem pakar komersial adalah sistem yang berbasis rule (*rule-based system*), yaitu pengetahuan disimpan terutama dalam bentuk *rule*, sebagai prosedur-prosedur pemecahan masalah.

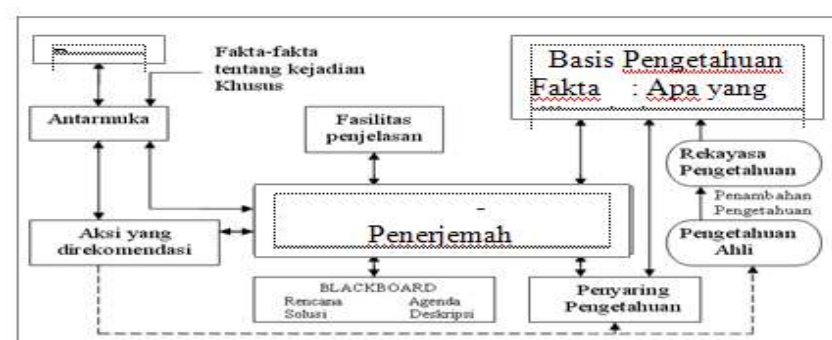
6. Kemampuan menjelaskan (*Explanation Capability*)

Fasilitas lain dari sistem pakar adalah kemampuan untuk menjelaskan saran atau rekomendasi yang diberikannya. Penjelasan dilakukannya dalam subsistem yang disebut subsistem penjelasan (*explanation*). Bagian dari sistem ini memungkinkan sistem untuk memeriksa penalaran yang dibuatnya sendiri dan menjelaskan operasi-operasinya.

2.1.2. Struktur Sistem Pakar

Ada dua bagian penting dalam sistem pakar, yaitu lingkungan pengembangan (*development environment*) dan lingkungan konsultasi (*consultation environment*). Lingkungan pengembangan digunakan dan oleh pembuat sistem pakar untuk membangun komponen-komponen dan memperkenalkan pengetahuan ke dalam *knowledge base* (Sutojo T, 2010).

Lingkungan konsultasi digunakan oleh pengguna untuk berkonsultasi sehingga pengguna mendapatkan pengetahuan dan nasihat dari sistem pakar layaknya berkonsultasi dengan seorang pakar. Gambar berikut menunjukkan komponen-komponen yang penting dalam sebuah sistem pakar.



Gambar 2.1 *Komponen-Komponen Yang Penting Dalam Sebuah Sistem Pakar*

Sumber : Sutojo (2010) Kecerdasan Buatan

2.1.3. Manfaat Sistem Pakar

Manfaat dari Sistem Pakar diantaranya yaitu:

1. Dapat memecahkan masalah lebih cepat daripada kemampuan manusia dengan catatan menggunakan data yang sama.
2. Memungkinkan orang awam bias mengerjakan pekerjaan para ahli.
3. Menyimpan pengetahuan dan keahlian para pakar.
4. Mampu menyediakan pelatihan. Pengguna pemula yang bekerja dengan sistem pakar akan menjadi lebih berpengalaman.
5. Dapat beroperasi di lingkungan yang berbahaya.
6. Mampu bekerja dengan informasi yang tidak lengkap atau tidak pasti.
7. Tidak memerlukan biaya saat tidak digunakan, sedangkan pakar manusia memerlukannya.
8. Menghemat waktu dalam mengambil keputusan.
9. Meningkatkan kualitas karena dapat memberi saran yang konsisten dan mengurangi kesalahan.
10. Memudahkan akses pengetahuan seorang pakar.

2.2. *Malware*

Malware atau perangkat lunak berbahaya yang berjenis aplikasi atau kode yang berniat jahat atau destruktif. *Malware* telah dirancang secanggih mungkin untuk membuat celah pada sistem keamanan pada suatu komputer. Berbagai cara perlindungan keamanan tidak sepenuhnya dapat menjadi jaminan sistem aman dari serangan *malware* karena setiap *malware* diberikan teknologi pertahanan tersendiri untuk melindungi dirinya dari segala acaman. (Yudha, 2018)

Terdapat lima jenis *malware* yang di bahas pada penelitian ini diantaranya adalah :

1. Virus komputer

Virus komputer ini merupakan sebuah program atau *software* yang berekstensi .exe atau *executable* atau sebuah *software* yang bias kita jalankan. Kebanyakan virus komputer ini menyamar dalam bentuk *installer* sebuah aplikasi, *shortcut* dan berbagai macam jenis berekstensi .exe. virus komputer ini sebenarnya tidak berbahaya apabila tidak kita jalankan *software* .exe nya. Namun terkadang tidak sadar bahwa yang dijalankan adalah sebuah virus dan akhirnya menyerang komputer.

2. *Worm*

Malware bernama *Worm* ini mampu masuk kedalam komputer melalui kelemahan atau *vulnerability* dari jaringan komputer yang kemudian menggandakan dan memperbanyak dirinya dalam komputer dan menginfeksi komputer secara perlahan hingga seluruh bagian komputer.

3. *Spyware*

Spyware adalah sebuah jenis *malware* atau *software* yang tidak diinginkan yang fungsinya adalah memata-matai segala hal yang dilakukan oleh *user* di dalam komputer tersebut. *Spyware* akan menyallin aktivitas yang dilakukan dan informasi yang disimpan di dalam komputer kepada orang tertentu untuk kepentingan yang tentu saja tidak baik.

4. *Adware*

Virus, *worm* dan *spyware* yang akan terasa dampak buruknya ketika sudah membuka atau mengeksekusi suatu file tertentu atau karena kelemahan jaringan internet dan jaringan komputer, berbeda dengan *adware* yang masuk kedalam komputer bersamaan dengan program yang sengaja di unduh.

5. Trojan

Malware berupa Trojan memiliki fungsi yaitu untuk memberikan fasilitas bagi para malware lainnya seperti virus, *worm* dan sebagainya untuk masuk kedalam komputer.

2.3. Metode penelitian

2.3.1. Studi literatur

Studi literatur adalah cara yang digunakan dalam memperoleh informasi dari beberapa sumber bacaan dan media internet serta berbagai dokumen yang bisa dipergunakan untuk menunjang dalam menyelesaikan laporan dan sebagai referensi untuk penyusunan dan pembuatan aplikasi.

2.3.2. Pengumpulan Data

Metode pengumpulan data untuk penelitian ini dilakukan yaitu dengan beberapa cara, yaitu:

1. Observasi

Pengumpulan data yang dilakukan secara langsung dengan mempelajari jenis-jenis *malware*.

2. Wawancara

Wawancara merupakan teknik pengumpulan data yang dilakukan melalui tatap muka dan tanya jawab langsung antara pengumpul data maupun peneliti terhadap nara sumber.

2.3.3. Pengujian

Pada tahap ini dilakukan pengujian dan akurasi sistem yang telah dibuat pada tahap implementasi. Pengujian dilakukan dengan cara memeriksa sistem apakah sudah beroperasi dengan baik atau masih ada *error* yang perlu diperbaiki

2.4. Elaboration

Tahapan yang dilakukan yaitu perancangan dan gambaran perangkat lunak secara *interactive* melalui aktivitas-aktivitas seperti *modeling* menggunakan (UML) *Unified Modelling Language, requirements, analysis* dan *design*, meskipun baru tahap awal. Tahapan perancangan ini terdapat beberapa *planning* agar mempermudah pada tahap pengkodean sistem yang akan dibuat.

1. Perancang UML (*Unified Modelling Language*)

UML (*Unified Modelling Language*) adalah metode pemodelan secara visual sebagai sarana untuk merancang *software* berorientasi objek. UML tersebut memberikan standar penulisan sebuah sistem *blue print* meliputi konsep bisnis proses, penulisan *class-class* dalam bahasa pemrograman yang spesifik, skema database, dan komponen-komponen yang diperlukan dalam sistem *software*. Pemaparan UML pada aplikasi yang akan dibangun yaitu *Use Case*, *Sequence Diagram*, *Class Diagram* dan *State Diagram*.

2. Perancangan *Interface*

Tahapan ini dilakukan dengan melakukan desain antarmuka atau tampilan sistem yang dirancang, apakah sesuai dengan rancangan awal atau tidak. Perancangan ini juga menjadi bayangan hasil akhir sistem yang akan dibangun dengan penyesuaian kepada *user/client* yang membutuhkan sistem agar nantinya sesuai dengan kebutuhan saat digunakan.

2.5. Basis Data

Basis data terdiri dari dua buah kata yaitu Basis dan Data. Basis dapat diartikan sebagai markas atau tempat bersarang atau berkumpul, sedangkan Data adalah representasi fakta dunia nyata yang mewakili suatu objek. Basis data sendiri dapat didefinisikan dalam sejumlah sudut pandang tertentu, diantaranya:

- a. Kumpulan data yang saling berhubungan yang disimpan secara bersama sedemikian rupa tanpa pengulangan (redudansi) yang tidak perlu, untuk memenuhi berbagai kebutuhan.
- b. Kumpulan *file-file* yang saling berelasi dan relasi tersebut biasanya ditunjukkan dengan kunci dari tiap *file* yang ada, yang disimpan dalam media penyimpanan elektronis. Satu basis data menunjukkan satu kumpulan data yang dipakai dalam lingkup perusahaan, instansi.

Basis data terdapat istilah-istilah, diantaranya adalah sebagai berikut:

- a. *Entity* merupakan individu yang mewakili sesuatu yang nyata dan dapat dibedakan dari sesuatu yang lain, misalnya orang, tempat, kejadian, atau konsep yang informasinya direkam.
- b. *Attribute* merupakan sesuatu hal yang mendeskripsikan karakteristik (*property*) dari entitas.
- c. *Data Value* (nilai atau isi data) adalah data aktual atau informasi yang disimpan pada atribut.
- d. *Record* (Tupel) yaitu kumpulan elemen-elemen yang saling berkaitan menginformasikan tentang suatu *entity* secara lengkap.
- e. *File* merupakan kumpulan *record-record* sejenis yang mempunyai panjang elemen yang sama, atribut yang sama, namun berbeda-beda data *valuenya*.
- f. *Data Base Management Sistem* (DBMS) merupakan kumpulan *file* yang saling berkaitan bersama dengan program untuk mengelolanya.

2.6. PHP

PHP (*PHP: Hypertext Preprocessor*) sudah dikenal sebagai bahasa scripting yang menyatu dengan tag-tag HTML, dieksekusi di server, dan digunakan untuk membuat halaman web yang dinamis seperti halnya *Active Server Pages (ASP)* dan *Java Server Pages (JSP)*. PHP sering digunakan karena beberapa sebab diantaranya:

1. *Life cycle* yang singkat, sehingga PHP selalu *up-to-date* mengikuti perkembangan teknologi internet.
2. *Cross Platform*, PHP dapat dipakai pada web server yang ada dipasaran seperti Apache, AOLServer, fhttpd, phttpd, Microsoft IIS, dan lain-lain. Serta dapat dijalankan pada berbagai sistem operasi seperti Linux, Unix, Solaris, Windows.
3. PHP mendukung berbagai macam database, baik yang komersial maupun yang non komersial, seperti SQL, MySQL, Oracle, SQL Server, Informix, dan lain-lain.
4. PHP dapat diinstal sebagai bagian dari CGI Script yang mandiri. Banyak keuntungan yang diperoleh apabila menggunakan PHP, diantaranya waktu eksekusi lebih cepat, akses database yang lebih fleksibel, dan tingkat keamanan lebih tinggi.

2.7. MySQL

MySQL termasuk jenis RDBMS (*Relational Database Management System*) sehingga istilah tabel, baris dan kolom tetap digunakan dalam

MySQL. Sebuah database mengandung satu atau beberapa tabel, tabel terdiri dari sejumlah baris dan kolom. MySQL sangat populer di kalangan pemrogram web, MySQL adalah database yang menghubungkan *script* PHP menggunakan perintah *query* dan *escape character* yang sama dengan PHP. PHP memang mendukung banyak jenis *database*, tetapi untuk mendesain sebuah website yang dinamis dan selalu *Up-to-Date*, MySQL merupakan pilihan database tercepat saat ini.

Kelebihan dari MySQL dapat melakukan transaksi dengan mudah dan efisien, mampu menangani jutaan user dalam waktu yang bersamaan dan mencukupi untuk kebutuhan database perusahaan-perusahaan skala menengah hingga kecil. MySQL merupakan *database* yang digunakan oleh situs-situs terkemuka di internet untuk menyimpan datanya. MySQL menggunakan bahasa dasar SQL untuk mengakses *database*-nya dan sebuah *database* pada MySQL mengandung satu atau sejumlah tabel, sejumlah *field* dan *record*. Perintah pada lingkungan MySQL ada dua macam yaitu perintah untuk lingkungan MySQL itu sendiri dan perintah untuk mengelola *database*.

2.8. XAMPP

XAMPP merupakan *web server* untuk penghubung antara bahasa pemrograman dan pengolahan database dengan menggunakan fasilitas *server* Apache dan *MySQL Connection* untuk menghubungkan ke database.

PhpMyAdmin adalah aplikasi bantu dengan antarmuka berbasis web yang dapat dijalankan pada internet *browser*.

Penggunaan PhpMyAdmin lebih kearah untuk mempermudah pembuatan database pada MySQL beserta strukturnya misalnya membuat Database, membuat Tabel, membuat *Field* dengan beragam pilihan tipe data, manipulasi data seperti *Insert, Update, Select, Delete*. Pembuatan database (untuk administrasi MySQL) dan Zend Optimizer yang dapat digunakan untuk membantu proses instalasi Apache, bahasa pemrograman dan MySQL.

2.9. Black Box

Menurut Rosa (2011) *Black-Box Testing* terfokus pada spesifikasi fungsional dari perangkat lunak *tester dapat mengidentifikasi kumpulan kondisi input dan melakukan pengetesan pada spesifikasi fungsional program*. Black Box Testing bukanlah solusi alternatif dari *White Box Testing* tapi lebih merupakan pelengkap untuk menguji hal-hal yang tidak dicakup oleh *White Box Testing*.

1. *Black Box Testing* cenderung untuk menemukan hal-hal berikut
 - a. Fungsi yang tidak benar atau tidak ada
 - b. Kesalahan antarmuka (*interface error*)
 - c. Kesalahan pada struktur data dan akses basis data
 - d. Kesalahan performansi dan terminasi
2. Pengujian desain untuk menjawab pertanyaan-pertanyaan berikut:
 - a. Bagaimana fungsi-fungsi diuji agar dapat dinyatakan *valid*?

- b. *Input* seperti apa yang dapat menjadi bahan kasus uji baik?
- c. Apakah sistem sensitif pada *input-input* tertentu?
- d. Bagaimana sekumpulan data dapat diisolasi?
- e. Berapa banyak rata-rata data dan jumlah data yang dapat ditangani spesifik pada operasi sistem?

2.10. Penelitian Terkait

Referensi penelitian terdahulu yang relevan dengan permasalahan yang akan diteliti mengenai sistem pakar tertera pada tabel 2.1 :

Tabel 2.1 Deskripsi Mengenai Penelitian Terkait

No	Judul	Metode	Pembahasan	Perbandingan
1.	Sistem Pakar Diagnosa Virus Komputer Berbasis WEB Penulis : Setiyani Diah, Hari Murti	<i>Forward Chaining.</i>	Mendeteksi virus pada komputer	Pada penelitian ini menggunakan metode <i>forward chaining</i> dan tidak terdapat halaman informasi virus , sedangkan pada penelitian yang akan dirancang menggunakan metode <i>certainty factor</i> dengan menambah informasi mengenai <i>malware</i> itu sendiri.
2.	Sistem Pakar Deteksi Virus Pada Komputer Penulis : Damanik	<i>Forward Chaining.</i>	Mendeteksi virus pada komputer <i>software</i> komputer.	Sistem pakar ini menggunakan metode <i>Certainty Factor</i> (CF) yang dapat mendeteksi tiga jenis malware yaitu Trojan, virus dan worm, sedangkan pada penelitian yang akan dirancang menggunakan metode <i>certainty factor</i> dan dapat mendeteksi hingga lima jenis

				malware yaitu virus, worm, trojan, adware, dan spyware.
3.	<p>Sistem Pakar Identifikasi Jenis Virus Pada Komputer Menggunakan Metode <i>Dempster Shafer</i> Berbasis Android</p> <p>Penulis :</p> <p>Hendrik Setiawan</p>	<i>Dempster Shafer</i>	<p>Identifikasi jenis virus komputer berbasis android</p>	<p>Pada penelitian ini bertujuan untuk dapat mengidentifikasi jenis <i>malware</i> yang mengidentifikasi komputer yang didasarkan pada gejala yang ditimbulkan dan sistem pakar ini berbasis android menggunakan metode <i>Dempster Shafer</i> yang mengidentifikasi tiga jenis malware yaitu <i>spyware</i>, worm dan Trojan. Sedangkan pada penelitian yang akan dirancang pada sistem pakar akan menggunakan metode <i>certainty factor</i> dengan mengidentifikasi lima jenis <i>malware</i> yaitu virus, Trojan, worm, spyware dan adwarea dengan menambahkan informasi <i>malware</i>.</p>

Perbedaan penelitian sebelumnya dengan penelitian yang akan dilakukan adalah dengan menggunakan metode yang berbeda yaitu metode *Certainty Factor* (CF) karena metode ini dapat memecahkan permasalahan dengan mengukur sesuatu apakah pasti atau tidak pasti dalam mendiagnosis *malware* dan dengan menggunakan metode ini akan terlihat kemungkinan terbesar sehingga data dapat terjaga kebenarannya.