# BAB II

# TINJAUAN PUSTAKA

## II.1. Keamanan Sistem Informasi

Keamanan sistem informasi merupakan hal yang perlu mendapat perhatian saat membangun sebuah sistem informasi. Bayangkan kita membuat sebuah rumah yang lengkap dengan jendela dan pintu, tetapi kita tidak membuat kunci untuk pintu dan jendela. Hal ini dapat menyebabkan seseorang bisa dengan mudah memasuki rumah kita, bahkan mungkin melakukan pencurian. Sama halnya dengan membangun sistem informasi, keamanan sistem informasi digunakan untuk menghindari seseorang yang tidak memiliki akses untuk dapat masuk ke dalam sistem mengeluarkan pengeluaran ekstra untuk melakukan pengamanan sistem informasi dan perbaikan atas ancaman yang sudah terjadi. Apabila menggangu performansi dari sistem, sering kali keamanan dikurangi atau ditiadakan (Chalifa Chazar, 2015).

*Prevention is better than cure*, mencegah lebih baik dari pada mengobati. Keamanan sistem informasi bertujuan untuk memastikan dan menyakinkan integritas, ketersediaan dan kerahasiaan dari pengolahan informasi. Pengelolaan keamanan sistem informasi harus dimulai ketika sebuah sistem informasi dibangun, bukan hanya sebagai pelengkap sebuah sistem informasi. Dengan adanya pengelolaan keamanan sistem informasi yang baik, maka diharapkan perusahaan dapat memprediksi resiko-resiko yang muncul akibat penggunaan sistem informasi sehingga dapat menghindari atau mengurangi resiko yang

mungkin dapat merugikan perusahaan. Keamanan sistem informasi merupakan tanggungjawab semua pihak yang ada di dalam perusahaan (Chalifa Chazar, 2015).

Oleh karena itu bagaimana perusahaan dapat menerapkan dan mengelola keamanan sistem informasi, melatar belakangi disusunnya seri ISO/IEC 27000, merupakan standar untuk manajemen keamanan sistem informasi. Seri ISO/IEC 27000 menawarkan satu set spesifikasi, kode etik dan pedoman praktik terbaik (*best practise*) untuk memastikan manajemen layanan TI (Teknologi Informasi) [8]. ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi (Chalifa Chazar, 2015).

### II.1.1. Aspek-aspek Terhadap Keamanan Informasi

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini:

1. Kerahasiaan (*Confidentiality*)

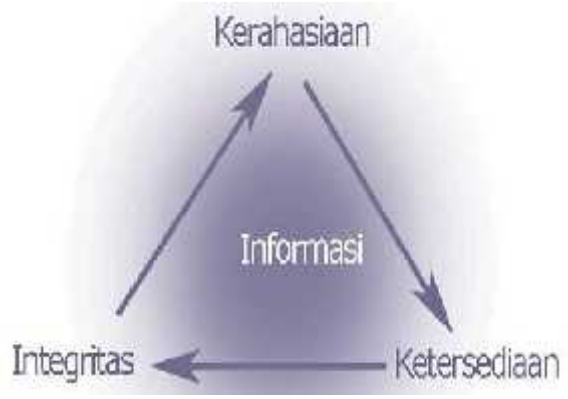
   Aspek yang menjamin kerahasian data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasian data yang dikirim, diterima dan disimpan.

2. Integritas (*Integrity*)

   Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.

3. Ketersediaan (*Availability*)

   Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan *user* yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).




**Gambar II.1 Aspek-Aspek Keamanan Sistem Informasi**
**(Sumber: Chalifa Chazar, 2015)**

Sumber lain menyebutkan bahwa aspek keamanan sistem informasi melingkupi 4 aspek. Grafinkel mengemukakan bahwa keamanan komputer melingkupi 4 aspek, yaitu *privasi*, *integrity*, *authentication* dan *availability*.. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation* (Chalifa Chazar, 2015).

## II.2. *Spam*

Pada zaman seperti sekarang ini teknologi sudah sangat semakin maju. Perkembangan teknologi yang begitu cepatnya membuat berbagai penemuan di segala bidang. Tidak ketinggalan pula perkembangan di dunia maya, dimana

internet adalah yang utama. Sekarang ini bisa dikatakan internet telah menjadi salah satu hal sangat berpengaruh dalam hampir setiap kehidupan manusia. Manusia sekarang hampir tidak bisa dipisahkan dari internet, seperti sudah menjadi kebutuhan. Terutama bagi mereka yang bergerak di bidang media dan teknologi. Namun seiring dengan segala pesatnya kemajuan yang membawa dampak positif bagi umat manusia, tidak bisa dipungkiri juga bahwa perkembangan teknologi ini membawa dampak yang tidak begitu baik, bahkan beberapa efek negatif bisa dikatakan sangat buruk dan sangat merugikan bagi beberapa pihak terutama masyarakat umum. Salah satu dampak negatif dari perkembangan teknologi komunikasi ini adalah adanya "*spam*", yang merupakan pemanfaatan peralatan elektronik yang digunakan untuk mengirimkan informasi atau pesan berupa tulisan, gambar, video, atau bentuk yang lainnya kepada orang lain secara terus menerus tanpa diminta atau tanpa melalui persetujuan dari para penerimanya.

### II.3 Captcha

Captcha (*Completely Automated Public Turing test to tell Computers and Human Apart*) pada dasarnya adalah suatu progam yang sebagian besar manusia dapat melewatinya, akan tetapi komputer tidak dapat melewatinya. Dengan arti yang lain, captcha adalah sebuah program yang melindungi situs dengan menghasilkan tes gradasi bahwa manusia dapat lulus tapi program komputer saat ini tidak (http://www.captcha.net). Captcha dapat digunakan untuk memverifikasi pengisian *form* agar terhindar dari pengisian otomatis (*bot*). Selain itu captcha

memiliki kemampuan untuk melindungi sistem dari serangan berbahaya di mana setengah *hackers/crackers* akan coba mempermainkan sistem dengan menciptakan perisian atau sebuah program yang dapat masuk secara otomatis. Fungsi dari captcha sendiri bisa juga diartikan untuk menguji kebenaran dari suatu jawaban yang soalnya diberikan oleh komputer berupa angka dan huruf. Tujuan captcha adalah untuk membedakan apakah jawaban itu dari komputer atau dari manusia.

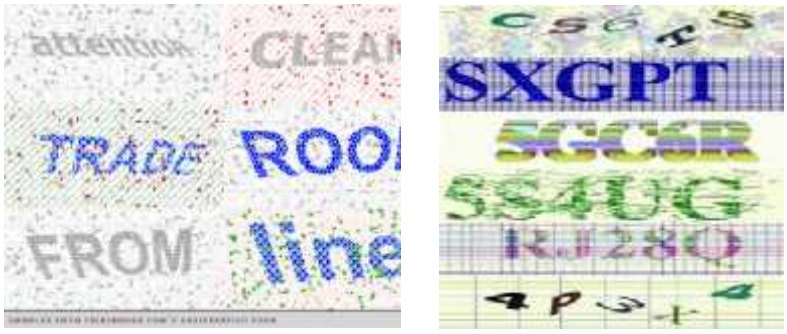
(Saini & Bala, 2013) menyatakan bahwa captcha (*Completely Automated Public Turingtest to tell Computers and Humans Apart*) merupakan suatu teknik yang digunakan untuk membedakan manusia dan komputer (*bots*). Captcha mengikuti *turing test* terbalik (*reverseturing test*), pada *test* tersebut program Captcha bertindak seperti penilai dan partisipan bertindak sebagai *user*. Jika *user* dapat melewati test itu, maka *user* adalah manusia, jika tidak maka *user* adalah mesin. Captcha diklasifikasikan menjadi beberapa kelompok berdasarkan pada bagian apa dilakukan distorsi, apakah karakter, gambar, suara,atau video.

Aplikasi captcha banyak digunakan pada penyedia *web mail* contohnya *Hotmail* dan *Yahoo*. Captcha dikembangkan untuk mencegah program robot atau *bots* yang menciptakan ratusan *email account* untuk mengirimkannya ke *user*. *Bots* ini digunakan oleh *spammer* untuk melakukan penyerangan terhadap sistem dengan menggunakan *HTTP POST request submission*. Program robot akan mengambil nilai variabel yang terdapat pada HTTP *POST request* tersebut dari *form* yang akan disubmit sebelumnya dan mengirimkannya kembali secara berulang-ulang. Penyerang dapat dengan mudah melakukan hal tersebut dengan

menulis *script* menggunakan bahasa perl. Captcha terbagi dalam beberapa jenis, antara lain:

1. Berdasarkan *Visual* (*Visual Based*)

   *Virtual Based* captcha memiliki beberapa variasi, yang paling umum digunakan saat ini adalah *teks* yang dimiringkan dan ditempelkan pada sebuah gambar dan pengenalan bentuk. Captcha yang menggunakan *teks* dimiringkan yang ditempelkan pada gambar disebut *Gimpy*, *EZ-Gimpy* adalah varian dari *Gimpy*, *Pessimal print* dan *buffletext. Gimpy* pertama kali dikembangkan oleh Luis Von Ahn dari *Carnegie Mellon University* yang mendesain versi paling sederhana dari *Gimpy*, disebut *EZ-Gimpy*. *Ez-Gimpy* yang sekarang ini digunakan oleh *Yahoo* dan suatu versi serupa digunakan oleh *Hotmail*. Perbedaan yang mendasar antara *gimpy* dan *EZ-gimpy* adalah *Gimpy* memiliki tiga atau lebih kata yang dimiringkan yang ditempelkan pada suatu gambar, sedangkan *EZ-Gimpy* hanya memiliki satu kata yang dimiringkan pada suatu gambar.




**Gambar II.2 Contoh *Visual Based* Captcha**
**(Sumber: Eko Budi Setiawan, 2012)**

2. Berdasarkan Suara (*Sound Based*)

   *Sound based* captcha kebanyakan digunakan untuk membantu mereka yang tuli atau mempunyai masalah dengan pendengaran. Suatu contoh *sound based* captcha adalah bunyi yang sesuai. Captcha ini digunakan pada *Hotmail, Yahoo* dan *Altavista* sebagai tambahan terhadap captcha *visual based* ketika pendaftaran sebuah *email account* untuk masing-masing penyedia layanan *email* ini. Tes ini menjalankan klip *audio* yang berisi rekaman suatu urutan kata atau angka-angka yang dimiringkan dan jika kata atau angka- angka yang diduga tepat maka dapat melewati tes ini (Eko Budi Setiawan, 2012).

### II.3.1. Karakteristik Captcha

Captcha adalah sebuah proses yang secara otomatis membangkitkan sebuah tes dengan karakteristik sebagai berikut (Eko Budi Setiawan, 2012):

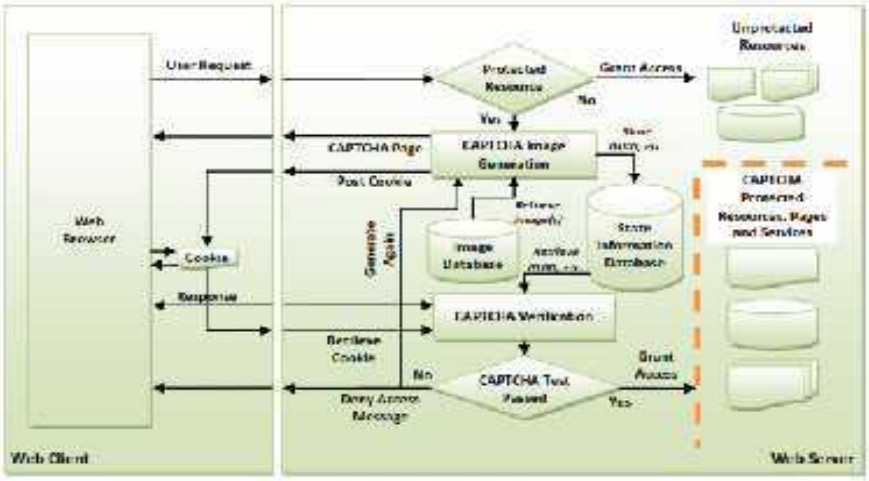
1. *Automated,* tantangan yang dilakukan harus dihasilkan secara otomatis dan dapat ditingkatkan *level* kesulitannya dengan mudah oleh computer
2. *Open, database* dan algoritma dari tantangan yang dilakukan harus bersifat publik.
3. *Usable,* tantangan harus mudah untuk diselesaikan oleh manusia dalam waktu yang wajar.
4. *Secure,* tantangan yang dilakukan harus sulit bagi komputer untuk memecahkan algoritmanya.

Meskipun captcha pada dasarnya adalah suatu tes untuk membedakan manusia dari komputer namun captcha tidaklah cukup hanya dengan memasang

sebuah *checkbox* yang berisi pernyataan bahwa apakah pengujung manusia atau bukan karena bagaimanapun cukup mudah untuk membuat *script* untuk memanipulasi jawaban dari tes tersebut.

### II.3.2. Sistem Kerja Captcha

Sebuah *web server* memegang sumber daya publik dan terlindungi yang terdapat pada halaman *web*. Data disimpan didalam sebuah *database* atau *files* atau layanan lainnya yang akan dipergunakan oleh manusia sebagai klien. Permintaan pengguna terhadap sumber daya dikirim melalui komputer klien ke *server*, yang mana sumber daya tersebut tidak memiliki perlindungan. Jika sumber daya dilindungi oleh captcha, akses akan diberikan jika telah melewati atau menyelesaikan uji captcha. Penjelasan terhadap cara kerja captcha dijelaskan pada gambar II.3




**Gambar II.3 Sistem Kerja Captcha**

**(Sumber: Hendra Aulia, 2013)**

*Server* menggunakan beberapa algoritma pengolahan gambar captcha untuk mengolah sebuah gambar captcha. Berbeda teknik captcha, maka berbeda pula algoritma yang digunakan dan pengolahan gambar yang mungkin disimpan di *database* gambar. Informasi pernyataan (*the state information*) terdapat pada *Global Unique Identifier* (GUID) pada pihak klien, dan solusi captcha disimpan di *The State Information Database* (SID) pada *server*. Penyimpanan GUID klien memastikan bahwa hanya klien yang menerima captcha yang mendapatkan solusi yang sesuai. Selain menyimpan solusi captcha dan informasi pernyataan (*the state information*), SID pada *server* juga memungkinkan untuk menyimpan bentuk *hash* atau enkripsi pada sisi klien. Sebuah halaman *web* yang berisi gambar captcha dihasilkan dan *cookies* dibentuk di *browser* pada sisi pengguna. Operator manusia memberi respon kepada uji captcha dan respon dikirim dari klien ke *server*. *Server* memverifikasi solusi captcha sesuai dengan yang disimpan pada GUID dan GUID klien mengirimkan solusi. Solusi disediakan oleh klien kemudian dibandingkan dengan solusi pada SID atau *cookies* dan ditentukan akses diberikan atau tidak. Jika akses ditolak, sebuah pesan akan ditampilkan untuk mengulang proses uji captcha kembali.

Pada implementasinya, ada beberapa captcha yang dapat memblok sementara jika terjadi kesalahan yang berulang. Jika captcha telah disahkan oleh klien, akses terhadap sumber daya akan diberikan tanpa memberikan uji pemeriksaan lebih lanjut.

### II.3.3 Serangan Terhadap Captcha

Serangan terhadap captcha di antaranya adalah sebagai berikut:

1. *Brute force*, dengan cara sederhana menebak dan menelusuri semua kemungkinan berdasarkan *entry* yang ada di dalam kamus. Serangan ini efektif untuk persoalan yang melibatkan penggunaan kata aktual.
2. *Artificial intelligence techniques*, untuk menganalisa atau mempersempit kemungkinan jawaban sampai ke kondisi dimana *brute force* berkemungkinan berhasil. Fungsi pengenalan objek (*object recognition*) dapat digunakan untuk mengenai huruf dan angka yang telah didistorsi.
3. *Hijacking attacks*, sangat efektif karena serangan ini mengeliminasi kebutuhan penyerang untuk memproses captcha. dihadapkan dengan kebutuhan untuk menjawab persoalan captcha, maka *hijacker* mengatur situasi dimana ia dapat menantang pengguna lain dalam *setting* berbeda. Misalnya seorang *spammer* ingin mendaftar secara gratis *email account*, mungkin akan membuat situs gratis dan mengiklankan dengan menggnakan *engine spam*-nya. Apabila pengunjung membuka situs tersebut, maka *script* registrasi yang dibuat *spammer* akan menginisialisasi registrasi *email*, dan menampilkan captcha yang dimiliki *email* sebagai bagian dari syarat untuk mengakses situs tersebut. Jika pengunjung menjawab dengan benar maka jawaban tersebut dikirimkan ke situs penyedia *email* untuk memperoleh akses.

### II.3.4. Kelemahan Captcha

Penggunaan captcha selain dapat mengamankan *website* dari serangan *bots*, juga terkadang terlalu menyulitkan untuk diselesaikan sehingga dapat menyita waktu untuk menjawab pertanyaan yang ditampilkan. Tidak jarang bahkan harus sampai beberapa kali untuk mengulang pertanyaan yang berbeda. Dari segi keamanan captcha itu sendiri, para analis keamanan mengkonfirmasi bahwa serangan otomatis terhadap Captcha *text-based* telah berhasil dilakukan sebesar 20% terhadap Google's captcha [12], 30-35% berhasil dilakukan terhadap Microsoft's captcha[13], 35% terhadap Yahoo! captcha[14]. Sedangkan serangan terhadap audio-based captcha miliknya Google bahkan sekitar 90% berhasil dipecahkan [15].

**Tabel II.1 Persentase Keberhasilan Serangan Terhadap Captcha**

| Jenis Captcha | Keberhasilan Serangan |
|---|---|
| Google's Captcha | 20% |
| Microsoft's Captcha | 30-35% |
| Yahoo's Captcha | 35% |
| Google Audio Captcha | 90% |

**(Sumber: Eko Budi Setiawan, 2012)**

### II.3.5 Klasifikasi Captcha

Pada saat ini captcha secara garis besar diklasifikasikan sebagai berikut:

1. **Captcha Menggunakan Gambar**

   Metode captcha yang menggunakan Gambar dapat dibagi menjadi 3 jenis yaitu *Optical Character Recognition* (OCR), *Visual Pattern Recognition Bongo,* dan Kombinasi dari gambar dan karakter *alphanumeric*. Dalam

metode captcha berbasis OCR, pengguna diberikan gambar sebuah kata yang telah diberikan distorsi dan efek-efek pengganggu. Karena adanya efek pada gambar, maka komputer akan mengalami masalah dalam memecahkan susunan karakter tersebut, sedangkan manusia dapat mengenalinya. Tetapi metode ini biasanya menghasilkan ketidak puasan pengguna karena tingkat kesulitan pembacaan karakter yang ditampilkan. Di sisi lain, captcha berbasis OCR telah banyak dibuat program pemecahnya (OCR-*Breaker*) Contoh captcha yang menggunakan metode ini adalah *Gimpy, EZ-Gimpy, PessimalPrint*, *BaffleText* dan *ScatterType*.

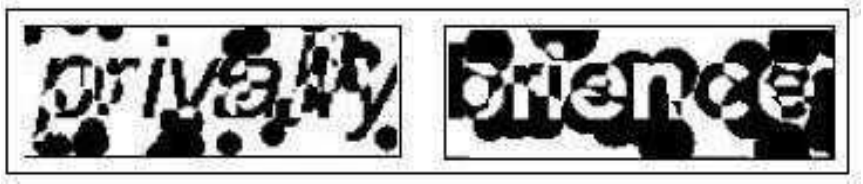
a. *EZ-Gimpy*, captcha jenis ini dikembangkan oleh *The School of Computer Science di Carnegie-Mellon University* dan digunakan oleh *yahoo*, tujuannya adalah untuk melindungi berbagai layanan yang diberikan oleh *yahoo* termasuk layanan *email* gratis. Teknik yang digunakan adalah dengan mengambil kata dari sebuah kamus yang berisi 850 kata dalam bahasa inggris kemudian dibuat gambar dan dirusak yang selanjutnya ditampilkan kepada *user*, berikut ini adalah gambar dari captcha *EZ-Gimpy* yang digunakan oleh *Yahoo*:

**Gambar II.4 Captcha *EZ-Gimpy* yang digunakan *Yahoo*!**
**(Sumber: Hendra Aulia, 2013)**

b. *PessimalPrint*, sama halnya dengan *EZ-Gimpy,* captcha jenis ini pun menggunakan kamus. Kamus tersebut hanya mengandung 70 kata dengan setiap kata terdiri dari lima sampai delapan huruf. Gambar di bawah ini menunjukkan captcha *PesimmalPrint* yang kemungkinan menggambarkan sebuah *string* "*reason*" atau "reason":

**Gambar II.5 Captcha *PesimmalPrint***
**(Sumber: Hendra Aulia, 2013)**

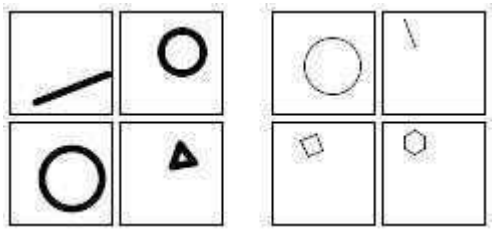
*c.* *BaffleText*, captcha jenis ini memiliki perbedaan dengan dua jenis captcha sebelumnya, dimana kata yang ditampilkan bukanlah kata yang memiliki arti. Di bawah ini adalah salah satu contoh dari captcha *BaffleText:*



**Gambar II.6 Captcha *BaffleText***
**(Sumber: Hendra Aulia, 2013)**

*Visual Pattern Recognition Bongo*, captcha jenis ini terdiri dari dua kumpulan gambar. Setiap gambar di salah satu sisi memiliki gambar yang mirip di sisi lainnya. *User* diminta untuk memasangkan gambar dari

kumpulan yang satu dengan kumpulan yang lainya. Berikut ini adalah gambar dari *Visual Pattern Recognition Bongo* di mana gambar terdiri dari dua bagian, yakni bagian kiri dan kanan:



**Gambar II.7 *Visual Pattern Recognition* Bongo**
**(Sumber: Hendra Aulia, 2013)**

Kombinasi dari gambar dan karakter alphanumerik, sistem menampilkan gambar-gambar yang sering ditemui dalam kehidupan sehari-hari, kemudian *user* diminta untuk mengisikan karakter yang secara umum telah melekat pada gambar yang dimaksud. Captcha jenis ini lebih sulit karena *user* diharuskan berpikir untuk menemukan karakteristik yang dimaksud, ini menyebabkan kemungkinan solusi (jawaban) tidak hanya satu tetapi tergantung dari pengguna.

2. **Captcha Berbasis Suara**

Sistem mengeluarkan suara yang dibangkitkan dari sekumpulan karakter secara otomatis, proses tersebut dilakukan oleh *Text-to-Speech Syntheziser* (TTS) kemudian ditambahkan dengan suara-suara gemuruh untuk sedikit mempersulitnya. Batasan dari bahasa dan dialek merupakan sebuah kesulitan dalam mengembangkan captcha jenis ini. Berikut ini adalah tabel yang menunjukkan apakah suatu jenis captcha rentan terhadap suatu serangan.

**Tabel II.2 Perbandingan Jenis Captcha dari Kemungkinan Serangan**

| **Jenis Captcha** | **Kemungkinan Serangan** | | | |
|---|---|---|---|---|
| | **OCR** | ***Dictionary*** | ***Simple Brute Force*** | ***Database*** |
| Bongo | No | No | Yes | Yes |
| Gimpy | Yes | Yes | No | No |
| BaffleText | Yes | No | No | Yes |
| Pix | No | No | No | Yes |
| PesimmalPrint | Yes | Yes | No | No |
| Sound | No | No | No | Yes |

**(Sumber: Hendra Aulia, 2013)**

Pada tabel II.2 di atas, sebagai contoh terlihat bahwa jenis captcha *Bongo* rentan terhadap serangan *simple brute force attack* dan *database attack* tetapi di sisi lain captcha jenis ini tidak rentan terhadap *OCR attack* dan *dictionary attack*.

**Tabel II.3 Perbandingan Kebutuhan Perangkat Lunak Captcha**

| **Jenis Captcha** | **Kebutuhan Perangkat Lunak** | |
|---|---|---|
| | ***Database*** | ***Image Processing*** |
| Bongo | Yes | No |
| Gimpy | No | Yes |
| BaffleText | Yes | Yes |
| Pix | Yes | No |
| PesimmalPrint | No | Yes |
| Sound | Yes | No |

**(Sumber: Hendra Aulia, 2013)**

Tabel II.3 menunjukkan kebutuhan perangkat lunak dari masing-masing jenis captcha, sebagai contoh adalah captcha jenis *sound* di mana captcha jenis ini membutuhkan perangkat lunak *database* tetapi tidak membutuhkan perangkat lunak untuk *image processing*. Sedangkan tabel II.4 di bawah ini menunjukkan apakah suatu jenis captcha mudah dibaca oleh

manusia (*user*) atau tidak.

**Tabel II.4 Perbandingan Kemudahan Manusia Membaca Captcha**

| Jenis Captcha | Mudah Dibaca Manusia |
|---|---|
| Bongo | Yes |
| Gimpy | No |
| BaffleText | No |
| Pix | Yes |
| PesimmalPrint | No |
| Sound | Yes |

**(Sumber: Hendra Aulia, 2013)**

Secara umum permasalahan yang akan ditampilkan oleh captcha haruslah dipilih secara acak dan dibangkitkan secara otomatis. Pada beberapa jenis captcha tingkat kesulitannya akan bertambah seiring dengan pertambahan jumlah sumber captcha dalam basis data (Hendra Aulia, 2013).