KEAMANAN LAYANAN *INTERNET BANKING* DALAM TRANSAKSI PERBANKAN

Decky Hendarsyah
Sekolah Tinggi Ilmu Ekonomi (STIE) Syari'ah Bengkalis
Email: deckydb@gmail.com

Abstrak

Internet saat ini merupakan salah satu kebutuhan pokok terutama bagi pengguna teknologi informasi. Internet sudah merambah ke seluruh bidang kehidupan mulai dari bisnis, pendidikan, kesehatan dan lain-lain sebagai wujud kemajuan teknologi dan informasi. Dunia perbankan seolah tidak mau ketinggalan dengan kemajuan teknologi dan informasi. Buktinya perbankan saat ini sudah mengembangkan layanan dan jasa-jasa perbankan yang diselaraskan dengan kemajuan teknologi dan informasi. Sebagai contoh saat ini perbankan sudah mengeluarkan suatu layanan yang bernama *Electronic Banking* (*E-Banking*). Di mana salah satu layanan dari *E-Banking* adalah *Internet Banking* yang berfungsi sebagai alternatif melakukan transaksi perbankan secara *online* menggunakan Internet.

Internet Banking mempermudah nasabah dalam bertransaksi perbankan secara *online* baik transaksi finansial maupun transaksi non finansial kecuali melakukan transaksi setoran atau penarikan tunai. Tetapi ketika menggunakan layanan *Internet Banking* apakah sudah aman? Karena ketika menggunakan Internet, perangkat komunikasi atau perangkat komputer terhubung ke jaringan komputer global, sehingga sangat rentan terhadap serangan keamanan atau kejahatan *Internet Banking*. Oleh sebab itu dalam makalah ini menjelaskan tentang konsep keamanan, manfaat *internet banking*, bagaimana bentuk-bentuk serangan keamanan terhadap Internet Banking. Kemudian dalam makalah ini juga memberi penjelasan bagaimana mencegah terjadinya serangan atau kejahatan dalam *Internet Banking*. Makalah ini juga menjelaskan model-model keamanan *Internet Banking* serta melakukan perbandingan terhadap layanan *Internet Banking* dari beberapa bank di Indonesia baik fasilitas maupun keamanannya. Sehingga nasabah bank yang ingin menggunakan layanan *Internet Banking* mendapat pengetahuan dan dapat memilih bank yang memberikan keamanan layanan *Internet Banking* lebih baik dan aman serta dapat mengurangi angka kejahatan online terutama dalam layanan *Internet Banking*.

Kata Kunci: Keamanan *Internet Banking*, Perbankan, Transaksi *Online*, *E-Banking*

1. Latar Belakang

Sebagaimana kita ketahui bahwa dalam dunia perbankan terdapat berbagai macam layanan transaksi seperti: setoran, penarikan, transfer, kliring dan sebagainya. Semua transaksi tersebut sampai saat sekarang masih banyak dilakukan oleh nasabah bank di bank yang bersangkutan. Sehingga ketika nasabah bank ramai melakukan transaksi perbankan maka nasabah lainnya terpaksa harus mengantri untuk dapat dilayani oleh bank. Ini merupakan masalah tersendiri bagi nasabah bank karena nasabah bank waktunya terbuang untuk menunggu antrian dan ini juga berimbas kepada pihak bank itu sendiri karena bank harus menyediakan unit pelayanan yang lebih banyak seperti *counter teller* harus

diperbanyak, memperbesar ruangan, menambah kursi dan sebagainya sehingga menimbulkan biaya yang cukup besar.

Kemudian perkembangan teknologi dan informasi saat sekarang sudah sangat pesat, begitu juga di dunia perbankan. Dunia perbankan seolah tidak mau ketinggalan dengan kemajuan teknologi dan informasi. Buktinya perbankan saat sekarang sudah mengembangkan pelayanan jasa-jasa perbankan yang diselaraskan dengan kemajuan teknologi dan informasi. Sebagai contoh dunia perbankan sudah mengeluarkan suatu layanan yang bernama *Electronic Banking (E-Banking)*.

E-Banking adalah layanan perbankan yang dilakukan secara elektronik. Jenis-jenis layanan *E-Banking* pada umumnya antara lain: ATM/Kartu Debit, Kartu Kredit, *TeleBanking/PhoneBanking*, SMS *Banking*, *Mobile Banking* dan *Internet Banking*[1] [2]. Nasabah bank saat sekarang sudah banyak menggunakan ATM atau Kartu Debit, itu disebabkan karena pada umumnya di bank sudah membatasi penarikan uang, jika melakukan penarikan uang di bawah lima juta rupiah harus melalui mesin ATM. Sedangkan Kartu Kredit banyak digunakan oleh kalangan tertentu karena tidak semua nasabah bank tertarik menggunakannya. *TeleBanking/PhoneBanking*, *SMS Banking*, *Mobile Banking* dan *Internet Banking* tidak semua nasabah bank yang menggunakan layanan tersebut hanya baru kalangan tertentu yang menggunakan terutama kalangan bisnis. Hal ini terbukti dengan masih panjangnya antrian di beberapa bank dan mesin ATM waktu melakukan transaksi perbankan.

Saat ini penggunaan Internet sudah dapat dibilang semakin baik, karena hampir setiap orang yang menggunakan perangkat komunikasi bisa terhubung ke Internet. Otomatis setiap orang yang terhubung ke Internet dapat melakukan transaksi secara *online*, tinggal kemauan individu dan jenis transaksi *online* apa yang dibutuhkan oleh pengguna internet tersebut. Jika dikaitkan dengan nasabah bank, kemungkinan besar rata-rata nasabah bank sudah menggunakan perangkat komunikasi atau perangkat lain yang bisa terhubung dengan Internet. Sehingga dapat menggunakan fasilitas Internet untuk melakukan transaksi perbankan secara *online* yaitu menggunakan layanan *Internet Banking*. Tetapi ketika menggunakan *Internet Banking* apakah sudah aman? Karena ketika menggunakan Internet, perangkat komunikasi atau perangkat komputer terhubung ke jaringan global, sehingga sangat rentan terhadap serangan keamanan *Internet Banking*. Untuk itu makalah ini akan membahas tentang keamanan layanan *Internet Banking* dalam transaksi perbankan.

2. Perumusan Masalah

Masalah yang dapat dirumuskan mengenai layanan Internet Banking yang disediakan oleh perbankan adalah sebagai berikut:

a. Bagaimana memilih layanan Internet Banking yang baik dan aman?
b. Bagaimana layanan Internet Banking dapat digunakan secara benar dan aman?

3. Tujuan Penulisan

Tujuan yang diharapkan dari penulisan makalah ini adalah sebagai berikut:

[1] Ahmad Kaleem dan Saima Ahmad, 2008, *"Bankers' Perceptions of Electronic Banking in Pakistan"*, dalam Journal of Internet Banking and Commerce, Vol. 13, no.1, April 2008, Lahore Pakistan, h. 3.

[2] Elisha Menson Auta, 2010, *"E-Banking In Developing Economy: Empirical Evidence From Nigeria"*, dalam Journal of Applied Quantitative Methods", Vol. 5 No. 2 Summer, Abuja Negeria, 2010, h. 213-214

a. Supaya nasabah bank dapat pengetahuan yang cukup untuk bertransaksi perbankan menggunakan *Internet Banking* secara benar dan aman.
b. Dengan adanya pengetahuan nasabah bank tentang *Internet Banking* yang aman diharapkan nasabah bank bisa mendapat kemudahan melakukan transaksi perbankan tertentu kapan dan dimana saja tanpa perlu datang ke bank.
c. Dengan adanya makalah ini diharapkan nasabah bank tidak perlu ragu atau takut dalam menggunakan layanan *Internet Banking* dan dapat meningkatkan kehati-hatian dalam melakukan transaksi perbankan melalui Internet Banking.

4. Konsep Keamanan

Keamanan merupakan sebagai kondisi atau kualitas yang bebas dari ketakutan, kecemasan, atau kepedulian. Jaringan komunikasi yang aman, dapat didefinisikan sebagai suatu jaringan dimana pengguna tidak merasakan ketakutan atau kecemasan sewaktu menggunakan jaringan[3]. Komputer dan sistem jaringan yang tidak terbatas telah memberi kesempatan untuk mengurangi biaya, meningkatkan efisiensi dan meningkatkan pendapatan. Sayangnya, ketergantungan tersebut menimbulkan risiko baru yang mengancam keamanan komputer dan sistem jaringan. Dengan demikian muncullah suatu tantangan baru untuk melindungi keamanan komputer dan sistem jaringan dari berbagai macam serangan keamanan[4]. Terdapat tiga komponen dasar sebagai pertimbangan dalam perancangan dan pembahasan sistem keamanan diantaranya adalah sebagai berikut[5]:

a. *Confidentiality*:
   Confidentiality adalah penyembunyian informasi atau sumber daya yang berkaitan dengan pencegahan akan pengaksesan terhadap informasi atau sumber daya yang dilakukan oleh pihak yang tidak berhak.
b. *Integrity*:
   Integrity merupakan keandalan data atau sumber daya dan biasanya dirumuskan untuk mencegah perubahan yang tidak sah. Integritas mencakup integritas data (isi dari informasi) dan integritas asli (sumber data, sering disebut otentikasi). Dengan demikian *integrity* berkaitan dengan pencegahan modifikasi informasi yang dilakukan oleh pihak yang tidak berhak.
c. *Availability*:
   Availability merupakan kemampuan untuk menggunakan informasi atau sumber daya yang diinginkan. *Availability* adalah aspek yang penting dalam mendesain sistem karena suatu sistem yang tidak memiliki availability sama buruknya dengan tidak ada sistem sama sekali. *Availability* dapat melakukan pencegahan akan penguasaan informasi atau sumber daya oleh pihak yang tidak berhak.

5. Internet Banking

Internet Banking secara ringkas dapat diartikan sebagai aktifitas perbankan di Internet. Pengertian *Internet Banking* dapat didefinisikan sebagai berikut:

---

[3] Praphul Chandra, 2005, *Bulletproof Wireless Security - GSM, UMTS, 802.11 and Ad Hoc Security*, USA: Newnes Elsevier Inc., h. 1.

[4] Nong Ye, 2008, *Secure Computer and Network - Systems Modeling, Analysis and Design*, England: John Wiley & Sons Ltd., h. 1.

[5] Matt Bishop, 2004, *Introduction to Computer Security*, New Jersey: Prentice Hall PTR, h. 2.

a. Menurut David Whiteley: [6]
   "*Internet Banking* adalah salah satu jasa pelayanan yang diberikan bank kepada nasabahnya dengan maksud agar nasabah dapat mengecek saldo rekening dan membayar tagihan selama 24 jam tanpa perlu datang ke kantor cabang".
b. Menurut Mary J. Cronin: [7]
   "*Internet Banking* adalah aplikasi layanan keuangan yang memungkinkan lembaga keuangan untuk menawarkan produk dan layanan perbankan tradisionalnya seperti cek saldo tabungan dan rekening pasar uang serta sertifikat deposito melalui internet".
c. Menurut Mahmood Shah dan Steve Clarke: [8]
   "Penyediaan informasi mengenai bank dan layanannya melalui halaman *website* di *World Wide Web* (WWW). Dimana layanan yang disediakan berupa akses pelanggan ke rekening, dapat mentransfer antar rekening yang berbeda dan dapat melakukan pembayaran atau mengajukan pinjaman melalui *channel* elektronik".

Internet Banking mempunyai tiga tingkatan definisi berdasarkan yang ditawarkan bank kepada nasabah yaitu sebagai berikut:[9]

a. Tingkat *Entry*:
   Merupakan definisi yang paling sederhana, dimana pada tingkatan ini hanya terdapat informasi statistik mengenai bank yang bersangkutan, jasa atau produk apa saja yang ditawarkan oleh bank dan juga pelayanan dasar seperti perkiraan pembayaran pinjaman. Pada tingkatan ini, hanya menampilkan situs yang bagus pada *web browser*.
b. Tingkat *Intermediate*:
   Pada tingkatan ini menawarkan seluruh layanan informasi keuangan seperti yang ditawarkan pada tingkat *entry* dan ditambah dengan layanan interaktif dasar dengan kemampuan dasar yaitu antara lain: perhitungan pembayaran kredit dan kemampuan untuk menampilkan rincian simpanan nasabah.
c. Tingkat *Advanced*:
   Pada tingkatan ini *Internet Banking* dapat didefinisikan sebagai tingkat yang paling lengkap layanannya, dimana layanan yang ditawarkan adalah seluruh fungsionalitas dan keamanan. Pada tingkatan ini nasabah bank dapat melakukan transfer dana antar bank, membayar tagihan dan membuka simpanan baru.

6. Fasilitas *Internet Banking*

Fasilitas yang terdapat pada *Internet Banking* pada umumnya hampir sama dengan fasilitas yang terdapat pada kegiatan transaksi tradisional di bank, yang membedakannya adalah kalau *Internet banking* transaksi dapat diakses melalui Internet kapan pun dan dimana pun berada sedangkan transaksi tradisional harus di bank. Fasilitas *Internet Banking* pada beberapa bank biasanya hampir sama, ada beberapa fasilitas yang terdapat pada suatu bank dan tidak ada pada bank lainnya. Fasilitas *Internet Banking* secara umum terbagi atas dua bagian yaitu:

---

[6] David Whiteley, 2000, *E-Commerce: Strategy, Technologies And Applications*, London: MC. Graw-Hill. h. 229.

[7] Mary J. Cronin, 1998, *Banking and Finance on the Internet*, Canada: John Wiley & Sons, h. 7.

[8] Mahmood Shah dan Steve Clarke, 2009, *E-Banking Management: Issue, Solutions and Strategies*, London: IGI Global. h. 2.

[9] Thomas P. Vartanian, Robert H. Ledig dan Lynn Bruneau, 1998, *21st Century Money, Banking And Commerce*, Washington: Fried, Frank, Harris, Shriver & Jacobson, h. 443.

a. Fasilitas Non Transaksional:
   Merupakan suatu fasilitas yang digunakan hanya untuk melihat rekening atau melakukan kegiatan administrasi dan tidak tercatat dalam transaksi rekening. Fasilitasnya antara lain:
   1) Melihat saldo rekening
   2) Melihat transaksi terakhir
   3) *Download* laporan transaksi
   4) Daftar rekening
   5) Melihat gambar cek yang sudah dibayar
   6) Memesan buku cek
   7) Ganti *Password*
   8) *Download* aplikasi *Mobile Banking*
   9) Dan lain-lain.
b. Fasilitas Transaksional:
   Merupakan suatu fasilitas yang langsung berhubungan dengan rekening dan setiap transaksi tercatat ke dalam rekening. Fasilitasnya antara lain:
   1) Transfer dana antar rekening
   2) Melakukan kliring
   3) Membayar tagihan (listrik, telepon/*handphone* dan air)
   4) Membayar zakat, wakaf dan sedekah
   5) Pembelian tiket
   6) Pembelian dan penjualan investasi
   7) Proses persetujuan transaksi
   8) Aplikasi dan transaksi pinjaman
   9) Dan lain-lain.

7. Web Browser

Internet Banking merupakan transaksi perbankan yang dilakukan melalui internet, tepatnya menggunakan aplikasi *web*. Untuk mengakses *web* diperlukan suatu perangkat lunak yang disebut dengan *web browser*, dengan menggunakan *web browser* ini *web* baru bisa di akses dan digunakan sesuai dengan fungsinya. Sebaiknya *Internet Banking* digunakan pada *web browser* yang sering digunakan oleh para pengakses Internet dengan versi terbaru. *Web browser* yang terkenal dan sering digunakan oleh para pengakses Internet adalah sebagai berikut:

a. *Google Chrome*:
   Google Chrome adalah *web browser* yang tergolong sebagai pendatang baru, namun *Google Chrome* telah bisa menyaingi *web browser* lainnya. Hal ini dikarenakan *Google Chrome* adalah *web browser* yang diciptakan oleh Google yang dianggap sebagai pernguasa Internet. Untuk men-*download Google Chrome* dapat mengakses website https://www.google.com/intl/id/chrome/browser/
b. *Internet Explorer*:
   Internet Explorer adalah *web browser* yang paling lama, bahkan hampir semua pengguna sistem operasi *Windows* mengenal *Internet Explorer* ini, karena *Internet Explorer* secara *default* telah tersedia saat pertama kali menginstal *Windows*. *Internet Explorer* dibuat oleh Microsoft, *Internet Explorer* seringkali dikatakan banyak kelemahan atau celah dalam memproteksi keamanan waktu melakukan

browsing. Untuk men-*download* versi terbaru *Internet Explorer* bisa mengakses *website* http://windows.microsoft.com/en-US/internet-explorer/products/ie/home

c. *Firefox*:
   Firefox atau juga biasa dikenal dengan nama *Mozilla Firefox* adalah *web browser* yang dikembangkan oleh Mozilla. Sampai saat *Firefox* adalah *web browser* yang paling populer dan juga handal selain itu *Firefox* dapat menjelajah Internet dengan cepat dan ringan. Banyak sekali *addons/plugins* atau *extention* tambahan yang disediakan oleh *Firefox* untuk meningkat kemampuan *browsing* di Internet. Dengan fitur yang lengkap tersebutlah *Firefox* menjadi *web browser* terpopuler. Untuk men-*download Mozilla Firefox* terbaru bisa mengakses *website* http:// http://www.mozilla.org/en-US/firefox/new/
d. *Opera*:
   Opera juga merupakan *web browser* yang tidak kalah populernya dengan *web browser* lainnya. Bahkan Opera memiliki ketersediaan dalam versi *mobile*. *Opera* versi *mobile* (*Opera Mini*) merupakan *web browser* tercepat saat ini. Untuk men-*download Opera* versi terbaru bisa mengakses website http://www.opera.com/
e. *Apple Safari*:
   Safari merupakan *web browser* yang diciptakan oleh Apple. Para pengguna Apple mengklaim bahwa *Safari* adalah *web browser* paling cepat dan tampilan yang *simple* ditambah lagi banyak *plugin* yang disediakan oleh Apple. Untuk men-*download* versi terbaru bisa mengakses *website* http://www.filehippo.com/download_safari/

Dari kelima *web browser* di atas, jika di-*download* menggunakan *website* di atas maka *website*-nya akan menyelaraskan kompetibel *web browser* dengan sistem operasi yang digunakan, kecuali untuk *Safari*, sistem operasinya harus menggunakan *Windows*. Selain kelima *web browser* di atas masih banyak lagi *web browser* yang populer. Sebagai contoh *Maxton* yang tersedia dalam sistem operasi *Linux, Netscape Navigator*, *Avant*, *Lunascape* dan lain sebagainya. Jadi untuk menggunakan *Internet Banking* dapat digunakan salah satu *web browser* yang di atas dan sebaiknya menggunakan versi terbaru.

8. Manfaat *Internet Banking*

Setiap layanan yang diberikan oleh bank mempunyai manfaat, baik untuk bank itu sendiri maupun untuk nasabahnya. Manfaat *Internet Banking* adalah sebagai berikut:

a. Bagi bank dapat mengurangi biaya operasional seperti: biaya kertas, biaya percetakan, biaya alat tulis dan lain-lain.
b. Mempermudah nasabah bank, dimana nasabah tidak perlu datang ke bank atau mesin ATM untuk melakukan transaksi seperti cek saldo, transfer, cek transaksi, membayar tagihan dan lain-lain kecuali untuk transaksi setoran tunai atau penarikan tunai. Sebagai contoh: nasabah bank yang mempunyai usaha online, dimana ketika pelanggan atau kliennya mentransfer uang langsung dapat dicek transaksi transfer masuk atau tidaknya pada waktu itu juga tanpa perlu datang ke bank atau ke mesin ATM. Kemudian contoh lainnya: nasabah bank dapat melakukan pembayaran atau transfer dari transaksi *online* atau berbelanja *online* meskipun pada waktu bank tutup atau libur.
c. Bagi bank dapat mengurangi jumlah karyawan atau staf operasional sehingga penggunaan ruangan lebih dapat diefisienkan.

d. Bank dapat melebarkan jangkauannya keseluruh dunia sehingga nasabah dapat berhubungan dengan bank dari manapun diseluruh dunia dengan waktu tidak terbatas.

9. Jenis Serangan Terhadap *Internet Banking*

Setiap perangkat apa pun yang terhubung ke Internet tidak tertutup kemungkinan mendapat serangan keamanan, karena selalu ada pihak-pihak yang ingin mengambil keuntungan dari serangan tersebut, ataupun hanya sekedar iseng untuk menguji keamanan dari perangkat yang diserangnya. Salah satu dari layanan perbankan yaitu *Internet Banking*, juga ada kemungkinan mengalami serangan keamanan, apalagi *Internet Banking* langsung berhubungan dengan rekening nasabah dimana dalam rekening tersebut terdapat sejumlah uang sehingga banyak pihak yang ingin menjebol keamanannya, supaya dapat dengan leluasa untuk menguasai rekening nasabah bank tersebut. Adapun jenis serangan keamanan terhadap *Internet Banking* adalah sebagai berikut:[10]

a. *Remote attacks*:
   Merupakan serangan keamanan dalam bentuk pengambilalihan atau pengendalian akses oleh pihak lain yang tidak bertanggung jawab. *Remote attacks* dapat dikelompokan kedalam beberapa jenis yaitu:
   1) *Phishing*:
      Merupakan serangan jarak jauh yang paling sering terjadi terhadap layanan keuangan *online*. Seorang penyerang membuat *website* persis sama dengan *website* aslinya dan menggunakan alamat *website* mirip dengan aslinya sehingga tidak mudah dicurigai. Kemudian penyerang mengirimkan *e-mail* ke sejumlah akun *e-mail* dimana isinya memberikan *link* (alamat *website* palsu yang tersembunyi) untuk diklik. Kemudian korban di yakinkan oleh penyerang bahwa harus mengisi data karena ada perbaikan di *server* atau dengan alasan lain yang meyakinkan serta memberikan embel-embel berupa hadiah atau uang. Sehingga akhirnya korban mengklik *link* palsu dan memasukan data-data pribadi yang digunakan untuk layanan keuangan *online* tertentu. Kemudian data-data pribadi tersebut disalahgunakan oleh penyerang untuk mencuri ataupun untuk keperluan negatif lainnya.
   2) DNS (*Domain Name System*) *attacks*:
      DNS *attacks* terbagi atas dua bagian antara lain:
      a) DNS *Cache Poisoning*:
         DNS *Cache Poisoning* merupakan suatu cara untuk menembus pertahanan DNS dengan cara menyampaikan informasi *IP Address* yang salah mengenai sebuah *host*, dengan tujuan untuk mengalihkan lalu lintas paket data dari tujuan yang sebenarnya. Cara ini banyak dipakai untuk menyerang situs-situs *e-commerce* dan *Internet Banking*. Teknik ini dapat membuat sebuah server palsu tampil identik dengan dengan *server Internet Banking* yang asli. Jadi dapat disimpulkan cara kerja DNS *cache poisoning* ini adalah dengan mengacaukan DNS Server asli agar pengguna Internet terkelabui untuk mengakses *website* palsu yang dibuat benar-benar menyerupai *website* aslinya tersebut, agar data dapat masuk ke server palsu.

[10] Candid Wüest, 2005, *White Paper: Symantec Security Response: "Phishing In The Middle Of The Stream" - Today's Threats To Online Banking*. Dublin: Symantec, h. 6-12.

b) DNS *Hijacking*:
DNS *Hijacking* merupakan suatu serangan keamanan jaringan komputer di mana penyerang dapat meletakkan dirinya di antara klien dan server DNS. Kemudian penyerang dapat mengambil informasi dari klien dan mengirimkan kembali informasi yang palsu ke klien sebelum informasi asli sampai ke server DNS. Tipe serangan ini bergantung dari kondisi siapa yang lebih cepat. Jika penyerang ingin serangannya berhasil, maka pernyerang harus membalas informasi yang diterimanya kepada klien sebelum informasi asli sampai ke server yang sesungguhnya.

3) *Interception*:
Pihak yang tidak berhak berhasil mengakses *asset* atau informasi. Contoh dari serangan ini adalah penyadapan.

b. *Local attacks*:
Local attacks merupakan serangan yang terjadi pada komputer lokal bisa melalui virus seperti trojan atau perangkat lunak yang bisa merekam kunci atau sering disebut dengan *key logger*. Virus komputer seperti trojan bisa mengambil informasi dari pengguna *website* walaupun *website*-nya sudah menggunakan SSL (*Secure Socket Layer*). Kemudian *key logger* saat ini sudah semakin canggih yang dahulunya hanya bisa merekam apa yang ditekan melalui *keyboard* sekarang bisa merekam apa saja yang diklik menggunakan *mouse* sewaktu mengakses *website* walaupun *website* sudah dilengkapi dengan *virtual keyboard*.

c. *Hybrid attacks*:
Tidak ada yang membatasi penyerang untuk melakukan satu jenis serangan keamanan jaringan komputer. Untuk melakukan serangan keamanan penyerang bisa menggunakan metode serangan gabungan (*hybrid*) yaitu dengan cara menggabungkan beberapa jenis serangan baik *local* dan *remote*.

10. Model Keamanan *Internet Banking*

Model saat ini diadopsi dalam sistem *Internet Banking* didasarkan pada beberapa lapisan keamanan, yang terdiri atas beragam solusi paralel dan mekanisme yang bertujuan untuk melindungi aplikasi perbankan dan data nasabah, menyediakan identifikasi, otentikasi dan otorisasi. Diantara model keamanan *Internet Banking* adalah sebagai berikut:[11]

a. *Digital Certificates* (Sertifikat Digital):
Sertifikat digital digunakan untuk otentikasi atau keabsahan antara pengguna dan sistem perbankan itu sendiri. Otentikasi ini tergantung pada keberadaan *Public Key Infrastructure* (PKI) atau infrastuktur kunci publik dan *Certificate Authority* (CA) atau sertifikat otoritas, yang dipercayakan kepada pihak ketiga untuk membuktikan validitas sertifikat digital mereka.

b. *One-Time Password Tokens*:
One-Time Password Tokens umumnya digunakan sebagai otentikasi kedua, yang dapat diminta dalam kondisi acak. Jenis perangkat ini membuat data otentikasi yang berguna untuk mengatasi serangan keamanan dengan cara menggunakan

[11] Laerte Peotta dkk, 2011, *A Formal Classification Of Internet Banking Attacks And Vulnerabilities*, dalam International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 1, Februari 2011. Brazil, Electrical Engineering Department, University of Brasilia, h. 188-189.

password secara dinamis atau berubah-ubah dan *password* hanya dapat digunakan sekali.

c. *One-Time Password Cards*:
   One-Time Password Cards merupakan model yang lebih murah untuk menghasilkan *password* yang dinamis, juga menyediakan otentikasi kedua. Namun dalam beberapa sistem perbankan, *password* yang dihasilkan oleh kartu OTP (*One Time Password*) dapat digunakan kembali beberapa kali sebelum dibuang, ini rentan terhadap serangan keamanan jangka pendek.
d. *Browser Protection*:
   Pada model ini, sistem dijamin pada tingkat *web browser* Internet, yang digunakan untuk mengakses *Internet Banking*. Para pengguna *browser* dilindungi dari *malware* dengan cara memantau wilayah memori yang dialokasikan oleh *browser* untuk mendeteksi *malware* dan menghalangi pencurian informasi yang sensitif seperti *user name* dan *password*.
e. *Virtual Keyboards*:
   Keyboard virtual yang dikembangkan untuk menggagalkan penggunaan *key loggers* (menangkap informasi yang diketik kedalam perangkat lunak). Alat ini biasanya merupakan perangkat lunak yang berbasiskan *Java* dan *Kriptografi* yang mendukung *web browser* yang berbeda.
f. *Device Registering*:
   Metode ini membatasi akses ke sistem perbankan melalui perangkat yang belum dikenal atau terdaftar pada sistem. Perangkat ini menggunakan *scan* sidik jari untuk identifikasi penggunanya.
g. CAPTCHA:
   Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) adalah metode baru yang diadopsi pada beberapa sistem perbankan yang bertujuan untuk menangkal serangan otomatis terhadap sesi atau halaman konfirmasi pada *website*. Metode ini mengharuskan pengguna yang sah untuk memasukkan informasi yang ditampilkan dalam gambar atau audio secara acak dan sulit bagi program otomatis (robot otomatis) untuk mengenali dan memproses gambar atau audio tersebut sebagai input konfirmasi.
h. *Short Message Service* (SMS):
   Short Message Service (SMS) merupakan metode yang diterapkan pada *Internet Banking* untuk memberitahu nasabah bank tentang transaksi yang sedang dilakukan melalui SMS. SMS ini menyediakan saluran otentikasi kedua untuk transaksi perbankan, dimana sistem *Internet Banking* mengirimkan kepada pengguna (nasabah bank) satu set karakter melalui SMS yang harus diinformasikan untuk otoritas konfirmasi pada proses transaksi melalui *Internet Banking*.
i. *Device Identification*:
   Device Identification biasanya diterapkan bersama-sama dengan *Device Registering* tetapi juga digunakan sebagai solusi yang berdiri sendiri dalam sistem *Internet Banking* yang bertujuan untuk memfasilitasi akses nasabah bank. Model identifikasi ini didasarkan pada karakteristik fisik dari perangkat yang digunakan oleh nasabah bank dengan cara mengidentifikasi asal usul dan riwayat informasi perangkat tersebut.
j. *Positive Identification*:
   Positive Identification adalah suatu model di mana nasabah bank diminta untuk memasukkan beberapa informasi rahasia yang hanya diketahui nasabah tersebut

dalam rangka untuk mengidentifikasi dirinya. Hal ini diterapkan sebagai metode otentikasi kedua.

k. *Pass-Phrase*:
   Pass-Phrase ini adalah model keamanan berdasarkan informasi yang dimiliki oleh nasabah bank. Hal ini biasanya digunakan sebagai metode otentikasi kedua dalam transaksi yang melibatkan pergerakan uang.

l. *Transaction Monitoring*:
   Saat ini pada sistem *Internet Banking*, masing-masing bank menggunakan teknik yang berbeda-beda. Mulai dari teknik kecerdasan buatan, analisis riwayat transaksi dan metode lain yang digunakan untuk mengidentifikasi pola-pola penipuan dalam transaksi perbankan sebagai pendekatan untuk pemantauan transaksi perbankan.

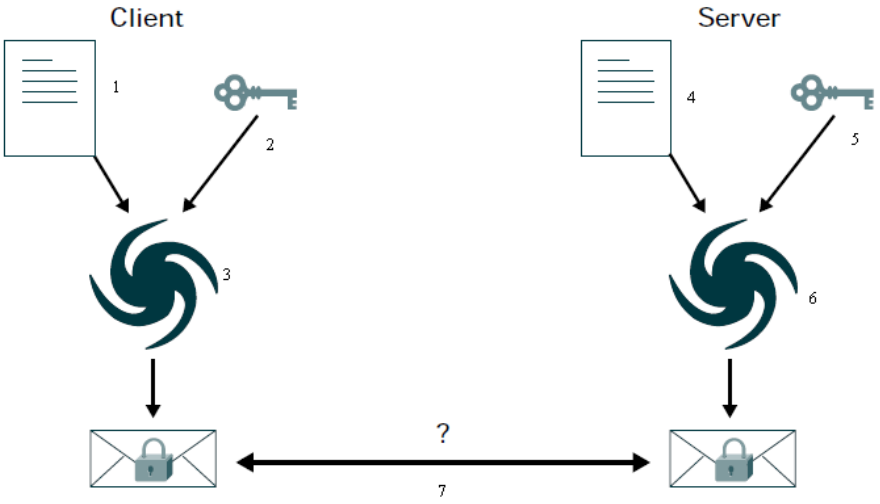
11. SSL dan *Token*

Secure Socket Layer (SSL) dan *Token* (*One-Time Password Tokens*) merupakan bagian dari model keamanan yang sering digunakan dalam sistem *Internet Banking* oleh bank terutama bank-bank yang ada di Indonesia.

a. *Secure Socket Layer* (SSL):
   Secure Socket Layer (SSL) merupakan bagian terpenting dari *Digital Certificates* dimana *Digital Certificates* salah satu model keamanan *Internet Banking*. SSL merupakan protokol standar *web* yang digunakan untuk menjaga keamanan web dengan cara mengenkripsi komunikasi data antara pengguna dengan *website* yang diakses. *Enkripsi* merupakan proses pengacakan data sehingga data tidak bisa dibaca oleh pihak lain. Kemudian proses mengembalikan data yang acak menjadi data asli disebut dengan *dekripsi*. Lalu lintas data melalui sambungan SSL akan selalu di enkripsi sehingga akan menghindari risiko sabotase atau pencurian data. Misalnya data *username, password* dan data-data penting lainnya.
   Secara umum *website* yang menggunakan SSL ini bisa dilihat dari alamat atau *Uniform Resource Locator* (URL) yang digunakan yakni dengan menggunakan https (https://) atau bisa dilihat icon gembok yang terdapat pada *toolbar address web browser* yang digunakan misalkan *google chorme*, *safari* sedangkan pada *mozilla firefox* tidak ada gambar gembok tapi muncul adalah nama perusahaan atau nama banknya. SSL biasanya digunakan mulai dari halaman *login* sampai masuk ke sistem *Internet Banking*. Setiap *website* yang menggunakan SSL dapat dilihat legalitas dan informasi sertifikat SSL dengan cara mengklik gambar gembok atau nama perusahaan yang terdapat pada *toolbar address web browser*. Isi dari sertifikat SSL antara lain menerangkan informasi mengenai:
   1) Pihak yang menggunakan sertifikat SSL yaitu perusahaan atau bank (Alamat website, nama perusahaan atau bank dan alamat).
   2) Pihak ketiga yang mengeluarkan sertifikat SSL.
   3) Versi, nomor seri dan masa berlaku sertifikat SSL.
   4) Algoritma enkripsi yang digunakan.

   SSL mempunyai cara kerja tersendiri dimana dalam SSL terdapat suatu tanda tangan digital (*digital signature*). Tanda tangan digital tersebut digunakan untuk memastikan integritas data. Setiap data yang dipertukarkan melalui SSL memiliki tanda tangan digital yang melekat pada SSL tersebut. Tanda tangan digital tersebut juga digunakan untuk memproses data menggunakan algoritma enkripsi, hash dan informasi kunci publik yang ada pada komputer client dan server. Data yang telah

melalui proses hash dengan menggunakan kunci publik tidak dapat dikembalikan seperti semula, karena proses hash merupakan proses enkripsi satu arah. Kemudian data yang telah dihash baik dari komputer client maupun komputer server akan dicocokan (*checksum*), jika data cocok berarti saluran akses ke website aman, jika tidak cocok berarti sudah terjadi kerusakan atau kebocoran data (lihat Gambar 1)[12].



Gambar 1. *Digital Signatures*

Dari Gambar 1 dapat dijelaskan bahwa:

1) Komputer client mengirim suatu data.
2) Komputer client mempunyai data dan sebuah kunci publik.
3) Komputer client melakukan proses *hash* antara data dan kunci publik.
4) Komputer server mengambil data secara acak.
5) Komputer server mengambil kunci publik yang tersimpan di server.
6) Komputer server melakukan proses hash antara data dan kunci publik.
7) Komputer client membandingkan data yang telah hash miliknya dengan data yang telah dihash milik komputer server. Jika kedua data sama maka data tidak rusak dan saluran SSL aman.

b. *Token* (*One-Time Password Tokens*):

Token merupakan alat otentikasi kedua dari sistem Internet Banking yang berfungsi menghasilkan password untuk dipakai sebagai verifikasi transaksi Internet Banking dimana bentuk dari *token* tersebut seperti kalkulator (lihat Gambar 2). Sebelum menggunakan *token* harus dimasukkan password untuk membuka *token*, jadi *token* menggunakan password sebelum menghasilkan password sehingga keamanan lebih terjamin. Jadi *token* dapat disebut sebagai alat otentikasi. Sedangkan otentikasi secara garis besar dapat dibagi dalam empat metode yaitu[13]:

1) *Something You Know*:

   Ini adalah metode otentikasi yang paling umum. Cara ini mengandalkan kerahasiaan informasi, contohnya adalah password atau PIN. Cara ini berasumsi bahwa tidak ada seorangpun yang mengetahui rahasia itu kecuali pemilik akses yang asli.

[12] Cisco, 2002, *White Paper: Introduction to Secure Sockets Layer*, Cisco System, h. 3

[13] Rizki Wicaksono, "Menggunakan Mesin Pencari Google dengan kata kunci Cara Kerja Token" dalam http://www.ilmuhacking.com/web-security/memahami-cara-kerja-token-internet-banking/. Diakses tanggal 18 Oktober 2012

2) *Something You Have*:
   Cara ini biasanya merupakan faktor tambahan untuk membuat otentikasi menjadi lebih aman. Cara ini mengandalkan barang yang sifatnya unik contohnya adalah kartu magnetik/*smartcard*, *hardware token*, *USB token* dan sebagainya. Cara ini berasumsi bahwa tidak ada seorangpun yang memiliki barang tersebut kecuali pemilik aslinya.
3) *Something You Are*:
   Ini adalah metode yang paling jarang diapakai karena faktor teknologi dan manusia juga. Cara ini mengandalkan keunikan bagian-bagian tubuh pemilik akses asli yang tidak mungkin ada pada orang lain seperti sidik jari, suara, sidik retina atau sidik bibir. Cara ini berasumsi bahwa bagian tubuh pemilik akses seperti sidik jari, sidik retina atau sidik bibir, tidak mungkin sama dengan orang lain.
4) *Something You Can*:
   Cara ini diasumsikan bahwa tidak ada orang lain di dunia ini yang bisa melakukan itu selain pemilik akses yang asli. Sebagai contoh tanda tangan di atas materai. Memang otentikasi dengan tanda tangan dibangun di atas asumsi bahwa tidak ada yang bisa menuliskan tanda tangan kecuali pemilik tanda tangan. Walaupun pada kenyataannya ada saja orang yang bisa meniru tanda tangan orang lain dengan sangat baik. Namun dengan menyadari fakta tersebut, tanda tangan di atas kertas tetap diakui sebagai bukti otentik atas siapa pemilik tanda tangan.

Gambar 2. *Token*[14]

Merujuk dari metode otentikasi maka Internet banking menggunakan dua metode otentikasi dengan mengombinasikan antara *"something you know"* berupa password dengan *"something you have"* berupa *token*. Pada umumnya ada dua mode pemakaian *token* Internet Banking[15]:

1) *Mode Challenge/Response (C/R)*:
   Ini adalah mode yang paling sering dipakai ketika bertransaksi. Dalam mode ini server memberikan informasi berupa sederetan angka. Angka tersebut harus dimasukkan kedalam mesin *token* untuk mendapatkan jawaban (*response*) berupa angka yang tampil pada *token*. Kemudian angka yang muncul pada *token* dimasukan ke dalam form yang terdapat pada *website* Internet Banking. *Token* akan mengeluarkan kode berupa angka yang

[14] Affriyuddin. "Menggunakan Mesin Pencari Google Image dengan kata kunci Token" dalam http://ekonomi.kompasiana.com/moneter/2012/05/09/bank-di-internet-atau-internet-banking/. Diakses tanggal 18 Oktober 2012

[15] *Ibid.*

berbeda-beda walaupun dengan informasi kode atau angka yang sama secara periodik tergantung waktu informasi dimasukkan ke dalam *token*.

2) *Mode Self Generated (Response Only)*:
Dalam mode ini server tidak memberikan informasi apapun. *Token* bisa langsung mengeluarkan sederetan angka tanpa harus memasukkan informasi dari server. Seperti mode C/R, *token* juga mengeluarkan kode yang berbeda-beda secara periodik tergantung waktu ketika *token* diminta untuk menghasilkan kode.

Sebenarnya jawaban yang diberikan oleh *token* baik dalam mode C/R maupun *Self Generated* tidak lain adalah password juga. Namun berbeda dengan password yang digunakan untuk login, password yang dihasilkan *token* memiliki keterbatasan untuk alasan keamanan yaitu[16]:

1) Hanya boleh digunakan sekali:
Ini disebut dengan OTP (*One Time Password*). Setelah suatu password dipakai, maka password yang sama tidak bisa lagi dipakai untuk kedua kalinya. Dengan cara ini tidak ada gunanya menyadap *password* yang dihasilkan *token* karena *password* tersebut tidak bisa dipakai lagi. Namun bila *password* tersebut di-*intercept* (dicegat) sehingga tidak pernah sampai ke server, maka *password* tersebut masih dapat digunakan karena *password* tersebut dianggap server belum pernah dipakai walaupun hal ini kecil sekali kemungkinannya terjadi. Jadi intinya semua *password* yang dihasilkan dari *token* sudah ada dan tersimpan diserver.
2) Hanya boleh digunakan dalam rentang waktu yang terbatas:
Password yang dihasilkan *token* memiliki waktu yang sangat terbatas, mungkin antara 3 sampai 6 menit bila waktunya habis maka *password* itu tidak bisa lagi digunakan, walaupun belum pernah dipakai.
3) Hanya boleh digunakan dalam konteks sempit:
Password yang dihasilkan *token* hanya bisa dipakai dalam suatu transaksi dalam konteks sempit, contohnya password yang dipakai untuk transaksi mengisi pulsa tidak dapat digunakan untuk melakukan transfer dana.

12. Perbandingan *Internet Banking*

Di Indonesia perbankan yang menggunakan sistem Internet Banking sudah banyak terutama bank-bank besar seperti bank BUMN dan Swasta. Tetapi dalam makalah ini hanya membandingkan empat sistem Internet Banking untuk personal atau individu yaitu BNI Internet Banking, Mandiri Internet, BSMNet Banking dan Klikbca.

a. BNI Internet Banking:

BNI Internet Banking merupakan layanan perbankan online yang diberikan Bank Negara Indonesia (BNI). Alamat website BNI Internet Banking personal adalah: https://ibank.bni.co.id/directRetail/ibank. Adapun komponen layanan BNI Internet Banking adalah sebagai berikut:

1) Tampilan:
Tampilan atau antar muka halaman login BNI Internet Banking terdiri dari *user id* dan *password* (lihat Gambar 3). Setiap nasabah yang ingin menggunakan layanan BNI Internet Banking haruslah mendaftarkan diri

[16] *Ibid.*

melalui *customer service*, BNI ATM dan BNI Internet Banking. Setelah melakukan pendaftaran maka nasabah akan mendapatkan *user id* dan *password* dimana *user id* dan *password*, nasabah sendiri yang menentukan.

Gambar 3. Halaman Login BNI Internet Banking Personal

2) Fasilitas:
BNI Internet Banking terdapat beberapa jenis fasilitas antara lain:
   a) Transaksi non finansial:
      - Informasi saldo
      - Informasi mutasi rekening
   b) Transaksi finansial:
      - Transfer dana antar Rekening BNI
      - Transfer dana ke bank lain (kliring dan RTGS)
      - Pembayaran tagihan (Kartu Kredit, Telkom, Kartu Halo, Kartu Xplor, Matrix, StarOne, Listrik PLN)
      - Pembelian voucher prabayar (Telkomsel, Indosat, XL, Esia, Fren, Telkom flexi dan 3)
      - Pembelian tiket airline (Garuda Indonesia, Lion Air, Mandala)
      - Pembayaran biaya pendidikan (UGM, ITB, USU dan lain-lain)
   c) Fasilitas Administrasi:
      - Registrasi BNI eSecure
      - Aktifasi BNI eSecure
      - Ganti Alamat Email
      - Ganti Password
      - Daftar Rekening
      - Daftar Pembayaran
      - Download Receipt Transaksi.
3) Keamanan:
BNI Internet Banking memiliki fitur keamanan yang dapat mengamankan transaksi perbankan secara online yaitu sebagai berikut:
   a) Menggunakan *user id* dan *password*.

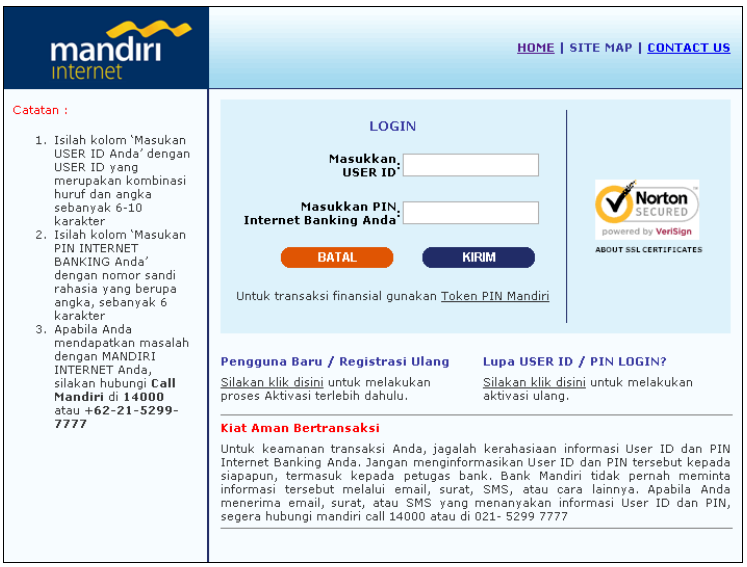
b) Dalam pengamanan website, BNI Internet Banking menggunakan SSL dan algoritma yang berlapis yaitu:
   - Algoritma enkripsi *Advanced Encryption Standard* (AES) 256 bit dengan model *Cipher Block Chainning* (CBC)
   - Algoritma hash *Secure Hash Algorithm* (SHA1)
   - Algoritma kunci publik *Rivest Shamir Adleman* (RSA) 1024 bit.

c) Sertifikat SSL dikeluarkan oleh VeriSign Secured.
d) Menggunakan *token* (lihat Gambar 2. bagian tengah) sebagai otentikasi kedua atau verifikasi untuk transaksi yang diberi nama BNI e-Secure.
e) *Auto Logoff* jika nasabah lupa keluar dari sistem.
f) Seluruh aktifitas nasabah akan tercatat oleh sistem.

b. Mandiri Internet:

Mandiri Internet merupakan salah satu layanan perbankan dari Bank Mandiri yang digunakan secara online. Alamat website Mandiri Internet personal atau perorangan adalah: https://ib.bankmandiri.co.id/retail/Login.do?action=form&lang=in_ID. Adapun komponen layanan Mandiri Internet adalah sebagai berikut:

1) Tampilan:
   Tampilan atau antar muka halaman login terdiri dari *user id* dan PIN (lihat Gambar 4). Setiap nasabah yang ingin menggunakan layanan Mandiri Internet haruslah mendaftarkan diri melalui *customer service*, ATM Mandiri dan Mandiri Internet.



Gambar 4. Halaman Login Mandiri Internet

2) Fasilitas:
   Mandiri Internet mempunyai beberapa jenis fasilitas yang dapat digunakan nasabah secara online antara lain:
   a) Transfer Dana:
      - Transfer antar Rekening Mandiri (dengan berita atau tanpa berita)

- Transfer antar Bank Domestik (Kliring dan RTGS
- Transfer Terjadwal

b) Pembayaran (Telkom & Telepon CDMA, Telepon GSM, Internet, Kabel TV, Kartu Kredit, Listrik, Pajak, PAM, Angsuran, Asuransi, Pendidikan, Kereta Api, Tour & Travel, Airlines, Multi Payment, Auto Debit dan lain-lain).
c) Pembelian (Pulsa GSM dan CDMA)
d) Kartu Mandiri Prabayar (History Kartu, Isi Ulang Kartu, Daftar Kartu)
e) Aplikasi Online (Penempatan Deposito, Tabungan Rencana Mandiri)
f) Informasi Rekening dan Kartu Kredit:
    - Rek. Tabungan & GIRO (Posisi Saldo, Histori Transaksi, Daftar Rekening)
    - Rek. Deposito
    - Rek. Tabungan Rencana Mandiri
    - Rek. Pinjaman
    - Kartu Kredit (Informasi Kartu Kredit Mandiri, Pendaftaran e-Billing)
g) Aktifitas Transaksi
h) Fungsi Administrasi (pendaftaran rekening tujuan mandiri sms dan mandiri call, rubah alamat email, ganti password)
i) Personalisasi (transaksi favorit, bahasa).

3) Keamanan:
Mandiri Internet memiliki fitur keamanan yaitu sebagai berikut:
a) Menggunakan *user id* dan PIN.
b) Dalam pengamanan website, Mandiri Internet menggunakan SSL dan algoritma yang berlapis yaitu:
    - Algoritma enkripsi *ARC4* atau *ARCFOUR* (RC4) 128 bit
    - Algoritma hash *Secure Hash Algorithm* (SHA1)
    - Algoritma kunci publik *Rivest Shamir Adleman* (RSA) 2048 bit.
c) Sertifikat SSL dikeluarkan oleh VeriSign Secured (Norton Secured).
d) Menggunakan *token* (lihat Gambar 2. bagian sebelah kiri) sebagai verifikasi transaksi yang diberi nama Token PIN Mandiri.
e) *Auto Logoff* (*Session Time Out*) jika nasabah lupa *log-out* atau keluar dari sistem.
f) Seluruh aktifitas nasabah akan tercatat oleh sistem.

c. BSMNet *Banking*:

BSMNet Banking merupakan salah satu layanan perbankan dari Bank Syariah Mandiri yang digunakan untuk transaksi perbankan secara online. Alamat website BSMNet Banking personal adalah: https://bsmnet.syariahmandiri.co.id/cms/. Adapun komponen layanan BSMNet Banking adalah sebagai berikut:

1) Tampilan:
Tampilan atau antar muka halaman login terdiri dari user id dan password (lihat Gambar 5). Setiap nasabah yang ingin menggunakan layanan BSMNet Banking haruslah mendaftarkan diri melalui *customer service*.

Gambar 5. Halaman Login BSMNet Banking

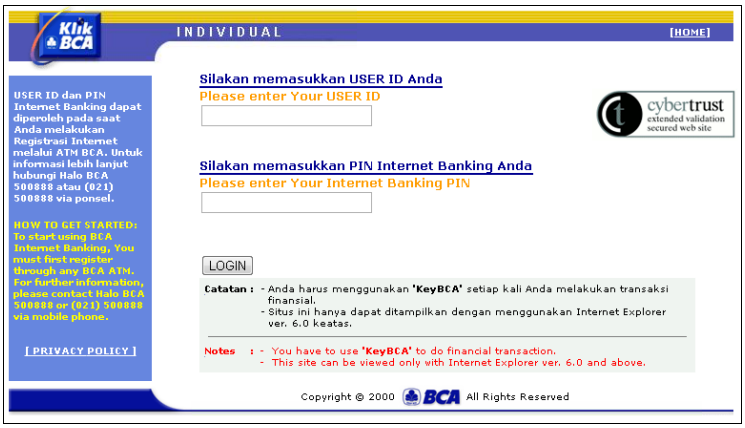
2) Fasilitas:
   Pada BSMNet Banking terdapat beberapa jenis fasilitas antara lain:
   a) Informasi data rekening Nasabah (tabungan, deposito, giro, pembiayaan)
   b) Cetak data mutasi transaksi
   c) Pemindahbukuan antar rekening BSM
   d) Transfer uang antar bank secara real time melalui jaringan ATM Bersama dan Prima-BCA
   e) Pembayaran tagihan (telpon, listrik dan lain-lain).
3) Keamanan:
   BSMNet Banking memiliki fitur keamanan yaitu sebagai berikut:
   a) Menggunakan *user id* dan *password*.
   b) Dalam pengamanan website menggunakan SSL dan algoritma yang berlapis yaitu:
      - Algoritma enkripsi *Advanced Encryption Standard* (AES) 256 bit dengan model *Cipher Block Chainning* (CBC)
      - Algoritma hash *Secure Hash Algorithm* (SHA1)
      - Algoritma kunci publik *Diffie Helman* (DHE) dan *Rivest Shamir Adleman* (RSA) 1024 bit.
   c) Sertifikat SSL dikeluarkan oleh VeriSign Secured.
   d) Menggunakan *keycode* (PIN Otoritas) sebagai otentikasi kedua untuk transaksi.
   e) *Auto Logoff* jika nasabah lupa keluar dari sistem.
   f) Seluruh transaksi nasabah akan tercatat pada sistem.

d. Klikbca:

Klikbca merupakan salah satu layanan perbankan dari Bank Central Asia (BCA). Alamat website klikbca individual adalah: https://ibank.klikbca.com/. Adapun komponen layanan klikbca adalah sebagai berikut:

1) Tampilan:

Tampilan atau antar muka halaman login terdiri dari *user id* dan PIN (lihat Gambar 6). Setiap nasabah yang ingin menggunakan layanan klikbca haruslah mendaftarkan diri melalui *customer service*, ATM BCA dan klikbca.



Gambar 6. Halaman Login Klikbca

2) Fasilitas:

Pada klikbca terdapat beberapa jenis fasilitas antara lain:

a) Pembelian (Pulsa isi ulang, Tiket, Saham)
b) Pembayaran (Kartu kredit, Telepon, Handphone, Internet, Asuransi, Pinjaman, Pajak, Listrik/PLN, Air/PAM, Pendidikan)
c) Transfer Dana (Antar Rekening BCA, BCA Virtual Account, Bank Lain Dalam Negeri)
d) Informasi Rekening (Informasi Saldo, Mutasi Rekening, Deposito)
e) Informasi Kartu Kredit (Informasi Saldo, Transaksi, Tagihan)
f) Informasi Kredit Konsumer (Informasi Pinjaman, History Pembayaran Pinjaman)
g) Informasi Produk Investasi (Saldo Reksadana)
h) Informasi Lainnya (Informasi Kurs, Nomor Kupon Gebyar Tahapan BCA)
i) Status Transaksi
j) History Transaksi
k) Administrasi (Ganti PIN, Ubah Bahasa, Hapus Daftar Transfer, Hapus Daftar Pembayaran, Ubah Alamat Email, Registrasi Inquiry Kartu Kredit BCA, Hapus Inquiry Kartu Kredit BCA, Registrasi KeyBCA, Tambah Koneksi KeyBCA, Hapus Koneksi KeyBCA, Hapus Koneksi KeyBCA, Aktivasi KeyBCA, Aktivasi BCA KlikPay)
l) E-mail (Inbox, Outbox, Berita Baru).

3) Keamanan:

Klikbca memiliki fitur keamanan yaitu sebagai berikut:

a) Menggunakan *user id* dan PIN.

b) Dalam pengamanan website menggunakan SSL dan algoritma yang berlapis yaitu:
    1. Algoritma enkripsi *ARC4* atau *ARCFOUR* (RC4) 128 bit
    2. Algoritma hash *Secure Hash Algorithm* (SHA1)
    3. Algoritma kunci publik *Rivest Shamir Adleman* (RSA) 2048 bit.
c) Sertifikat SSL dikeluarkan oleh Cybertrust SureServer.
d) Menggunakan *token* (lihat Gambar 2. bagian sebelah kanan) sebagai otentikasi kedua untuk transaksi yang diberi nama KeyBCA.
e) *Auto Logoff* jika nasabah lupa *log-out.*
f) Seluruh aktifitas nasabah akan tercatat oleh sistem.

13. Mencegah Kejahatan *Internet Banking*

Dalam melakukan transaksi secara online ada kemungkinan dibayang-bayangi oleh kejahatan online terutama dalam melakukan transaksi perbankan menggunakan layanan Internet Banking. Untuk mencegah kejahatan online terutama untuk layanan Internet Banking ada beberapa cara, antara lain sebagai berikut:

a. Menggunakan komputer pribadi, diusahakan jangan mengunakan komputer umum seperti diwarnet atau rental karena biasanya diwarnet sering ditemui komputer yang sudah terpasang perangkat lunak *key logger* yang digunakan untuk merekam *user id* dan *password*.
b. Memastikan komputer yang digunakan terbebas dari virus atau *malware* terutama virus trojan dan virus berbahaya lainnya yang sering mengincar data-data penting sewaktu online, dengan cara memasang antivirus dan mengupdate antivirus secara berkala karena virus selalu berkembang setiap harinya.
c. Selalu memastikan alamat *website* Internet Banking yang digunakan adalah benar dan *website*nya menggunakan SSL atau https:// yang aktif. Kemudian pastikan juga informasi sertifikat SSL sama dengan informasi *website* Internet Banking yang bersangkutan. Karena banyak sekali penipu di Internet menggunakan alamat-alamat Internet Banking palsu mirip dengan alamat Internet Banking aslinya atau yang disebut dengan istilah *phising*. Sebaiknya sebelum masuk ke *website* Internet Banking masuk dulu ke *website* utama dari bank tersebut.
d. Sebaiknya menggunakan *web browser* terbaru dan mengupdate web browser secara berkala, karena kemungkinan ada fitur-fitur dari Internet Banking tidak terbaca oleh *web browser* lama atau *web browser* terbaru bisa memblokir pengambilan data-data penting oleh *malware*.
e. Selalu melakukan *log-out* atau keluar dari sistem Internet Banking walaupun meninggalkan komputer cuma sebentar. Karena ada kemungkinan pihak-pihak yang tidak bertanggung jawab menggunakan sistem sewaktu meninggalkan komputer walaupun sistem Internet Banking sudah menggunakan *auto logoff*.
f. Setelah menggunakan Internet Banking sebaiknya selalu menghapus atau membersihkan *history* pada *web browser*. Karena setiap *web browser* akan selalu menyimpan data-data sewaktu *online* pada *cache* sehingga *cache* tersebut dapat disalahgunakan oleh pihak-pihak yang tidak diinginkan.
g. Jangan memberitahu pihak lain tentang *user id* dan password Internet Banking apalagi ditulis dan ditempel di meja kerja. Kemudian jangan menggunakan

password yang mudah ditebak seperti: nama, tanggal lahir, nama isrti, nama anak dan lain-lain. Selalu mengganti *password* secara berkala.

h. Jangan mudah percaya dengan *email* yang mengatasnamakan *administrator* bank dan memberi embel-embel hadiah setelah itu memberi *link* alamat *website* dan menyuruh mengklik *link* tersebut kemudian memasukan *user id* dan *password* Internet Banking serta data pribadi lainnya. Karena *link* tersebut bisa jadi mengandung alamat *website* palsu, sehingga data-data yang dimasukan direkam oleh pengirim *email* dan data-data tersebut dapat disalahgunakan.

14. Keuntungan & Kerugian *Internet Banking*

Setiap fasilitas yang diberikan oleh suatu produk atau layanan selalu mempunyai keuntungan dan juga terdapat kerugian. Begitu juga dari layanan Internet Banking mempunyai keuntungan dan kerugian.

a. Keuntungan:
    1) Merpermudah nasabah dalam melakukan aktivitas perbankan tanpa perlu pergi ke bank kecuali dalam hal setoran tunai atau penarikan tunai.
    2) Aktivitas perbankan dapat dilakukan kapan dan dimana saja selama ada akses internet.
    3) Mempermudah nasabah dalam membawa uang tunai dalam jumlah yang besar sewaktu akan melakukan transfer. Sehingga dapat melindungi nasabah dari kejahatan perampokan.
    4) Mempermudah nasabah dalam melakukan pembayaran tagihan tanpa perlu datang ke tempat pembayaran tagihan.
    5) Mempermudah nasabah dalam melakukan pembelian tiket dan pulsa tanpa perlu datang ke *counter* penjualan tiket dan pulsa.
    6) Keamanan sistem Internet Banking berlapis, mulai dari *user id* dan *password* kemudian *website* menggunakan SSL dengan algoritma yang berlapis serta adanya otentikasi kedua untuk verifikasi transaksi seperti: *token* atau *keycode*.

b. Kerugian:
    Sedangkan kerugian dari Internet Banking sangat kecil kemungkinannya, walaupun ada, mungkin itu disebabkan dari kelalaian nasabah itu sendiri yang tidak melakukan cara-cara pencegahan kejahatan Internet Banking yang telah dijelaskan sebelumnya. Sebagai contoh: nasabah bank tidak sengaja memberikan *user id* dan *password* Internet Bankingnya kepada pihak lain ataupun *user id* dan *password*nya diambil (disadap) oleh pihak lain. Pihak lain tersebut hanya bisa melakukan transaksi non finansial seperti melihat informasi saldo dan informasi mutasi rekening dan lain-lain. Sedangkan untuk melakukan transaksi finansial seperti: transfer, pembelian tiket, pembelian pulsa dan membayar tagihan atau yang lainnya tidak bisa dilakukan karena harus menggunakan otentikasi kedua untuk melakukan transaksi tersebut yaitu menggunakan *token* ataupun *keycode*.

15. Kesimpulan dan Saran

Adapun kesimpulan dan saran yang dapat diberikan dari makalah ini adalah sebagai berikut:

a. Fasilitas layanan Internet Banking yang diberikan kepada nasabah dari beberapa bank yang dibandingkan pada umumnya sama. Hanya beberapa fasilitas saja yang berbeda tetapi tidak terlalu prinsipil. Sedangkan untuk tampilan *website* dari keempat sistem Internet Banking termasuk *user friendly* (mudah digunakan).
b. Setiap bank selalu memberikan layanan terbaiknya untuk nasabahnya mulai dari kemudahan, kenyamanan dan terutama keamanan dalam bertransaksi. Dari empat sistem Internet Banking yang telah dibandingkan dapat disimpulkan bahwa semuanya memberikan kemudahan, kenyamanan dan keamanan. Terutama dari segi keamanan, terbukti pada keempat sistem Internet Banking yang telah dibandingkan semua menggunakan keamanan yang berlapis-lapis sehingga serangan atau kejahatan terhadap sistem Internet Banking mereka dapat terjaga dan aman.
c. Setiap nasabah harus selalu memperhatikan dan melakukan tindakan pencegahan kejahatan Internet Banking karena penipuan melalui Internet selalu meningkat, sehingga dengan adanya tindakan pencegahan nasabah dapat melakukan transaksi perbankan online secara benar dan aman.
d. Nasabah harus teliti sebelum menggunakan layanan Internet Banking terutama masalah keamanan dari layanan Internet Banking tersebut. Untuk keamanan Internet Banking minimal harus ada komponen-komponen keamanan sebagai berikut:
    1) *User id* dan *password*.
    2) *Website* Internet harus menggunakan SSL dan algoritma yang berlapis.
    3) Otentikasi kedua, sebaiknya menggunakan *token*.
    4) Sistem dilengkapi dengan *Auto Logoff*.
    5) Semua aktifitas tercatat oleh sistem.

16. Daftar Pustaka

Ahmad Kaleem dan Saima Ahmad, *"Bankers' Perceptions of Electronic Banking in Pakistan"*, dalam Journal of Internet Banking and Commerce, Vol. 13, no.1, April 2008, Lahore Pakistan, 2008.

Affriyuddin. http://ekonomi.kompasiana.com/moneter/2012/05/09/bank-di-internet-atau-internet-banking/. Diakses tanggal 18 Oktober 2012.

Candid Wüest, *White Paper: Symantec Security Response: "Phishing In The Middle Of The Stream" - Today's Threats To Online Banking*. Dublin: Symantec. 2005.

Cisco, *White Paper: Introduction to Secure Sockets Layer*, Cisco System, 2002.

David Whiteley, *E-Commerce: Strategy, Technologies And Applications*, London: MC. Graw-Hill. 2000.

Elisha Menson Auta, *"E-Banking In Developing Economy: Empirical Evidence From Nigeria"*, dalam Journal of Applied Quantitative Methods", Vol. 5 No. 2 Summer 2010, Abuja Negeria, 2010.

Laerte Peotta dkk, *"A Formal Classification Of Internet Banking Attacks And Vulnerabilities"* dalam International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 1, Februari 2011. Brazil: Electrical Engineering Department, University of Brasilia. 2011.

Mahmood Shah dan Steve Clarke, *E-Banking Management: Issue, Solutions and Strategies*, London: IGI Global. 2009.

Mary J. Cronin, *Banking and Finance on the Internet*, Canada: John Wiley & Sons, 1998.

Matt Bishop, *Introduction to Computer Security*, New Jersey: Prentice Hall PTR, 2004.

Nong Ye, *Secure Computer and Network - Systems Modeling, Analysis and Design*, England: John Wiley & Sons Ltd., 2008.

Praphul Chandra, *Bulletproof Wireless Security - GSM, UMTS, 802.11 and Ad Hoc Security*, USA: Newnes Elsevier Inc., 2005.

Rizki Wicaksono, http://www.ilmuhacking.com/web-security/memahami-cara-kerja-token-internet-banking/. Diakses tanggal 18 Oktober 2012.

Thomas P. Vartanian, Robert H. Ledig dan Lynn Bruneau, *21st Century Money, Banking And Commerce*, Washington: Fried, Frank, Harris, Shriver & Jacobson. 1998.