Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur

Eristya Maya Safitri[1], Adelia Sefri Larasati[2], Syahroni Rizki Hari[3]

[1,2,3] Sistem Informasi, Universitas Pembangunan Nasional Jawa Timur
[1]maya.si@upnjatim.ac.id
[2]adelialarasati16@gmail.com
[3]syahronirizki098@gmail.com

***Abstrak*— Teknologi Informasi sejak lama telah dipandang sebagai penggerak dan pendukung strategi khususnya dalam dunia Perbankan karena hampir seluruh transaksi melibatkan penggunaan tekologi informasi, oleh sebab itu keamanan teknologi informasi perlu dikelola dengan baik untuk menghindari risiko yang mungkin terjadi. Risiko-risiko ini berkaitan dengan pencurian data informasi nasabah dan internal perusahaan. Risiko yang mungkin terjadi harus ditangani mulai sekarang agar tidak menimbulkan kerugian dalam penggunaan teknologi informasi. Mengontrol keamanan sistem informasi merupakan salah satu cara untuk melindungi data perusahaan dari salah satu risiko yaitu dari pihak yang tidak berwenang. Jika Pihak yang tidak berwenang dapat mengakses data perusahaan maka data perusahaan dalam status terancam karena dapat disalahgunakan. Pengamanan sistem informasi pada perbankan sangat diperlukan untuk memberikan akses ke pengguna yang sah, membatasi pengguna yang tidak sah dan mengontrol aktivitas mencurigakan. Tujuan penulisan ulasan literatur ini yaitu mengulas tentang keamanan informasi perbankan di lingkup *i-Banking*.**

***Kata Kunci*—Teknologi Informasi, Akses Kontrol, E-banking**

I. PENDAHULUAN

Bank adalah perusahaan yang mengelola uang yang diperoleh dari nasabah dalam bentuk tabungan dan menyalurkannya lagi kepada nasabah dalam bentuk pinjaman atau tabungan. Jika sebuah bank mengalami kegagalan, dampak yang ditimbulkan dapat meluas mempengaruhi nasabah dan lembaga-lembaga yang menyimpan dananya atau menginvestasikan modalnya di bank, dan akan menciptakan dampak yang sangat luas secara domestik maupun pasar internasional [1]. Keberadaan Teknologi Informasi (TI) menjadi bagian penting dalam proses bisnis perbankan karena hampir seluruh transaksi melibatkan penggunaan TI. Penggunaan TI telah menjadi hal yang fundamental dalam bisnis perbankan, digunakan sebagai media untuk melakukan berbagai transaksi *multichanel* untuk melakukan transaksi perbankan. Selain menjadi tulang punggung transaksi[2], TI telah mampu meningkatkan kinerja pegawai dan meningkatkan kepercayaan pada pelanggan untuk melakukan transaksi.

Sejalan dengan literatur lain, beberapa penelitian yang diungkapkan oleh Fristak dan Ward mengungkapkan tentang penggunaan TI dalam perbankan yang mampu meningkatkan efisiensi dalam operasional serta mampu menghasilkan *benefit* yang besar bagi bank yang menerapkan sistem informasi perbankan [3]. *Internet Banking (I- Banking)* merupakan salah satu pemanfaatan TI didunia perbankan. Bank bisa dikatakan semakin kuat untuk mengebankan *I-Banking* karena kemajuan internet yang banyak digunakan oleh nasabah bank [4]. Kondisi ini merupakan potensi yang bagus bagi perbankan untuk mengembangkan layanan berbasis internet. Kondisi seperti ini menciptakan daya tarik sektor perbankan yang dapat mengundang nasabah baru.

Perkembangan teknologi yang cepat dapat menimbulkan berbagai masalah terhadap keamanan data pada perusahaan perbankan dalam pengelolan *E-Banking*. Pertahanan dari sistem informasi sering disebut dengan pengendalian dan keamanan sistem informasi (information systems control and security) yang didefinisikan sebagai penjagaan terhadap fasilitas dan proses komputer dari gangguan-gangguan yang disengaja maupun tidak disengaja yang dapat menyebabkan perubahan, kerusakan atau pencurian sumber-sumber daya sistem informasi secara tidak sah .

Keamanan sistem informasi merupakan suatu subsistem dalam suatu organisasi yang bertugas mengendalikan resiko terkait dengan sistem informasi berbasis komputer. Keamanan sistem informasi merupakan sebuah aplikasi prinsip- prinsip pengendalian internal yang secara khusus digunakan untuk mengatasi masalah-masalah dalam sistem informasi[5]. Bodnar dan William (2004) menyatakan ada enam metode yang dapat digunakan untuk melakukan kecurangan sistem informasi, yaitu : manipulasi input, mengubah program, perubahan file secara langsung, pencurian data, sabotase, dan penyalahgunaan atau pencurian sumber daya informasi[5].

Pada *paper* ini penulis akan mengulas tentang keamanan sistem informasi perbankan pada sistem *i-banking* dari pihak bank dan nasabah.

II. METODE PENELITIAN

Metode yang digunakan dalam pengerjaan paper ini menggunakan metode Studi Literatur. Teknik Studi Literatur ini dilakukan dengan melakukan pencarian terhadap berbagai sumber tertulis, baik berupa buku-buku, arsip, majalah, artikel, dan jurnal, atau dokumen-dokumen yang relevan dengan permasalahan yang dikaji. Sehingga informasi yang didapatkan dari studi kepustakaan ini dijadikan rujukan untuk memperkuat argumentasi-argumentasi yang ada. Hasil dari mempelajari berbagai literatur ini akan digunakan untuk

mengulas dan membahas tentang Keamanan Sistem Informasi yang ada pada E-Banking.

Dalam pengumpulan studi literatur kami menggunakan Google sebagai mesin pencari utama dan dua *database* jurnal online yang dapat diakses secara penuh yakni Science Direct dan IEEE. Semua jurnal yang sudah diteliti dengan baik nantinya akan menjadi sebuah informasi untuk menjadi topik pembahasan.

III. HASIL DAN PEMBAHASAN

Layanan perbankan untuk transaksi keuangan banyak diberikan oleh bank dengan tujuan utama memberikan kemudahan nasabah dalam bertransaksi. Selain pelayananan di kantor bank, terdapat layanan menggunakan *internet banking* dan juga ATM [2]. Saat ini nasabah lebih memilih bertransaksi melalui *delivery channel alternatif* seperti ATM, *Internet Banking*, SMS Banking, bukan lagi melalui antri di bank [3]. Dengan semakin banyaknya transaksi berbasis online maka memicu meningkatnya penggunaan *delivery channel alternative*, contohnya seperti Internet Banking yang semakin sering digunakan oleh masyarakat. Penulis akan meneliti keamanan sistem informasi dari *internet banking* yang digunakan dalam dunia perbankan.

A. Aspek Keamanan

Menurut Dony Ariyus, keamanan komputer meliputi beberapa aspek diantaranya :

1. **Authentication,** Agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi.
2. **Integrity**, Keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh yang berhak dalam perjalanan informasi tersebut**.**
3. **Non-repudiation**, Non- repudiation merupakan hal yang bersangkutan dengan si pengirim. Si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. **Authority,** Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
5. **Confidentiality,** Confidentiality merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses**.**
6. **Privacy,** Privacy merupakan lebih mengarah pada data yang sifatnya pribadi.
7. **Availability,** Aspek ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.
8. **Access control,** Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. [5]

Menurut Budi Rahardjo mengungkapkan bahwa aspek keamanan yang harus dijaga dari internet Banking adalah:

1. **Confidentiality,** Aspek confidentiality memberi jaminan bahwa data-data tidak dapat disadap oleh pihak-pihak yang tidak berwenang. Serangan terhadap aspek ini adalah penyadapan nama account dan PIN dari pengguna Internet Banking.
2. **Integrity,** Aspek integrity menjamin integritas data, dimana data tidak boleh berubah atau diubah oleh pihakpihak yang tidak berwenang. Salah satu cara untuk memproteksi hal ini adalah dengan menggunakan checksum, signature, atau certificate
3. **Authentication,** Authentication digunakan untuk meyakinkan orang yang mengakses servis dan juga server (web) yang memberikan servis. Mekanisme yang umum digunakan untuk melakukan authentication di sisi pengguna biasanya terkait dengan: - Sesuatu yang dimiliki (misalnya kartu ATM, chipcard) - Sesuatu yang diketahui (misalnya userid, password, PIN, TIN) - Sesuatu yang menjadi bagian dari kita (misalnya sidik jari, iris mata)
4. **Non-repudiation,** Aspek non-repudiation menjamin bahwa jika nasabah melakukan transaksi maka dia tidak dapat menolak telah melakukan transaksi. Hal ini dilakukan dengan menggunakan digital signature yang diberikan oleh kripto kunci publik (public key cryptosystem). Mekanisme konfirmasi (misal melalui telepon) juga merupakan salah satu cara untuk mengurangi kasus.
5. **Availability,** Aspek availability difokuskan kepada ketersediaan layanan. Jika sebuah bank menggelar layanan Internet Banking dan kemudian tidak dapat menyediakan layanan tersebut ketika dibutuhkan oleh nasabah, maka nasabah akan mempertanyakan keandalannya dan meninggalkan layanan tersebut [6].

B. Keamanan Pada *Enthernet Banking*

Dalam usaha pengamanan data nasabah, diperlukan kerjasama antar pihak Bank dan pihak nasabah untuk menjaga sistem keamanan dalam bertransaksi menggunakan jasa layanan yang diberikan oleh pihak manajemen bank. Berikut adalah usaha yang dapat dilakukan pihak bank untuk meningkatkan keamanan sistem pada bank:

1. **Sistem Cryptography,** Sistem ini menggunakan angka-angka yang dikenal dengan kunci *(key)*.Sistem ini disebut juga dengan sistem sandi.Ada dua tipe *cryptography,* yaitu simetris dan asimetris. Pada sistem simestris menggunakan kode kunci yang sama bagi penerima dan pengirim pesan. Kelemahan dari *cryptography simestris* adalah kunci ini harus dikirim pada pihak penerima dan halini memungkingkan seseorang untuk mengganggu di tengah jalan.Sistem*cryptography asimetris* juga mempunyai kelemahan yaitu jumlah kecepatan pengiriman data menjadi berkurang karena adanya tambahan kode.Sistem ini biasanya digunakan untuk mengenali nasabah da melindungi informasi finansial nasabah .

2. **Firewall**, Firewall merupakan sistem yang digunakan untuk mencegah pihak- pihak yang tidak diijinkan untuk memasuki daerah yang dilindungi dalam unit pusat kerja perusahaan. *Firewall* berusaha untuk mencegah pihak-pihak yang mencoba masuk tanpa ijin dengan cara melipatgandakan dan mempersulit hambatan-hambatan yang ada. Namun, yang perlu diingatkan adalah bahwa sitem *firewall* ini tidak dapat mencegah masuknya virus atau gangguan yang berasala dari dalam perusahaan itu sendiri[7]

Dalam usaha pengamanan data nasabah pun peran nasabah dalam melakukan tindakan keamanan akun pribadi juga sangat diperlukan. Berikut adalah usaha yang dapat dilakukan pihak nasabah untuk meningkatkan keamanan sistem pada bank:

1. ***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
2. ***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
3. ***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 [8].
4. ***Username dan Password,*** Pengamanan paling umum yang dapat dilakukan oleh Nasabah adalah *Username* dan *Password*. Sebelum nasabah dapat mengakses akun miliknya, nasabah harus memasukan beberapa karakter pengaman akunnya. *Username* dan *Password* terdiri dari beberapa karakter, tergantung dari pihak bank penyedia layanan. Beberapa bank juga menyediakan persyaratan khusus dalam penentuan jumlah karakter maupun jenis karakter yang digunakan untuk *Username* dan *Password*. Berikut adalah contoh syarat *username* dan *password* yang telah ditetapkan oleh bank BCA dana Bank Syariah Mandiri [9].

Tabel 1. Persyaratan Keamanan Akses Login

Bank	Username	Password
Klik BCA	12 Karakter (8 Alfabet + 4 Numerik)	6 Karakter Numerik
BSMNNetBanking	8 Karakter Numerik	4 Karakter Numerik

C. Jenis Serangan Pada E-Banking

Terdapat serangan -serangan *hacker* yang biasanya dilakukan untuk merusak sistem keamanan bank. Serangan ini dilakukan baik dari sisi sistem bank yang tersedia maupun pola penggunaan nasabah dalam menggunakan layanan. Dalam usaha pengamanan yang dilakukan, diperlukan juga pemahaman kemungkinan risiko tertinggi baik dilihat dari tingkat keseringan jaringan maupun tingkat pengaruh atas dampak yang dihasilkan dari risiko berikut. Berikut adalah daftar risiko serangan dari sisi sistem layanan bank [7] :

1. **Brute force attack,** atau dalam bahasa Indonesia disebut juga dengan serangan brute force ini adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci password yang memungkinkan atau istilah gampangnya mungkin menggunakan Random password atau password acak. Pendekatan inipada awalnya merujuk pada sebuah program.
2. **Denial of service (DoS) attack,** merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya(denial of servis). Cara untuk melumpuhkan dapat bermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi hang atau crash, tidak berfungsi, atau menurunnya kinerja sistem karena beban CPU menjadi tingi. komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia.
3. **Virus, worm, Trojan,** Menyebarkan virus, worm, maupun Trojan dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban.

Dalam usaha pengamanan yang dilakukan, diperlukan juga pemahaman kemungkinan risiko tertinggi dari sisi pola penggunaan layanan oleh nasabah, baik dilihat dari tingkat keseringan jaringan maupun tingkat pengaruh atas dampak yang dihasilkan dari risiko. Berikut adalah daftar risiko serangan dari sisi penggunaan sistem oleh nasabah[7] :

1. ***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[8].

2. ***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
3. ***Typo Site,*** Pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika ada seseorang korban salah mengetikan alamat dan sirus palsu buatannya. Jika hal ini terjadi maka pelaku akan mudah memperoleh informasi *user* dan *password* korbannya dan dapat dimanfaatkan untuk merugikan korban[7].
4. ***Interception,*** Pihak yang tidak berhak berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan.

D. Kesalahan yang Dilakukan Nasabah

Meskipun berbagai cara pengamanan telah dilakukan, baik dari pihak bank maupun dari pihak nasabah sendiri, data nasabah tetap dapat dicuri jika nasabah sendiri sebagai pemilik akun melakukan kesalahan-kesalahan dalam mengakses akun miliknya. Berikut ini beberapa kesalahan yang sering dilakukan oleh nasabah[10]:

1. **Password Yang Mudah Ditebak,** PIN, Password atau Kata Sandi merupakan langkah pengamanan pertama yang dihadapi oleh nasabah ketika hendak mengakses akun. Seringkali nasabah mengabaikan pentingnya menggunakan kata sandi yang aman. Beberapa nasabah lebih sering menggunakan kombinasi karakter yang mudah mereka ingat seperti, 123456, 000000, abcdef, atau bahkan tanggal lahir mereka. Hal dihindari karena penggunaan kata sandi tersebut mudah ditebak orang
2. **Jaringan Internet Yang Tidak Aman,** Tidak memperhatikan jaringan internet yang digunakan oleh nasabah juga menjadi salah satu kelalaian dari nasabah. Informasi yang kita miliki dapat dengan mudah dicuri oleh orang lain jika kita menggunakan jaringan internet yang tidak aman. Kita perlu waspada dalam menggunakan jaringan internet apalagi ketika kita berbagi jaringan internet dengan orang lain. Disamping itu, penggunaan VPN tidak disarankan terutama penggunaan VPN yang tidak dapat dipertanggungjawabkan keamanannya.
3. **Anti Virus Yang Kadaluarsa,** Perangkat yang kita miliki tentunya harus memiliki software anti virus yang dapat menjamin keamanan perangkat kita agar tidak terjangkit virus yang dapat mencuri data pribadi kita. Hampir semua anti virus dapat dijamin perlindungannya, tapi anti virus yang telah kadaluarsa tidak dapat menjamin lagi keamanan dari penggunanya. Hal ini disebabkan karena anti virus tersebut tidak mendapatkan update terbaru tentang virus atau bahkan anti virus tidak dapat bekerja lagi jika telah melewati tanggal kadaluarsa
4. **Jarang Memeriksa Akun,** Akun yang jarang diperiksa juga dapat diserang oleh hacker. Nasabah yang tidak memeriksa lagi akunnya tidak akan mendapatkan *update* atau perkembangan terbaru dari akunnya. Hal ini juga dapat menyebabkan nasabah tidak mengetahui hal-hal apa saja yang telah terjadi pada akunnya, entah itu dana masuk ke rekening, ataupun penarikan dana yang tidak diketahui oleh nasabah sendiri.

E. Cara Pengamanan yang Perlu Dilakukan Nasabah

Dari ulasan terkait kesalahan yang sering dilakukan nasabah, maka berikut adalah cara pengamanan yang perlu dilakukan nasabah untuk meningkatkan keamanan pada akun sistem e-banking yang digunakan.

1. **Pastikan Situs,** Pastikan nasabah mengakses situs yang benar. Seringkali beberapa upaya yang dilakukan oleh pencuri adalah dengan mengirim pesan penipuan yang mencantumkan alamat website yang dibuat mirip dengan alamat asli milik bank yang ditiru
2. **Ganti Password Secara Berkala**, Gunakan kata sandi maupun PIN yang tidak mudah ditebak, dan usahakan jangan menggunakan tanggal lahir untuk PIN. Selain itu, pastikan juga untuk mengganti kata sandi secara berkala untuk menghindari jika kata sandi telah diketahui oleh pihak yang tidak

berkepentingan

3. **Gunakan Jaringan yang Aman,** Gunakan selalu jaringan internet milik pribadi ketika mengakses I-banking. Hindari penggunaan jaringan yang digunakan bersama ketika hendak mengakses I-banking. Pastikan juga jaringan yang digunakan bebas dari intervensi dari pihak lain.
4. **Anti Virus Terupdate**, Pastikan anti virus yang dimiliki oleh perangkat sudah terupdate secara berkala. Anti virus yang telah diupdate memiliki informasi terbaru mengenai virus yang mungkin bisa menyerang atau mencuri informasi

IV. KESIMPULAN

Perkembangan *Internet banking* di Indonesia akan meningkat pesat sejalan dengan perkembangan teknologi, permintaan pasar, letak geografis dan jumlah penduduk. Penataan operasi *internet banking* diperlukan untuk menghindari permasalahan dimasa mendatang serta memudahkan pengawasan yang dilakukan oleh bank indonesia.

Hal tersebut diperkuat dengan adanya informasi dari hasil dan pembahasan kami mengenai beberapa masalah keamanan internet banking diatas, seperti misalnya: DNS Hijacking, Phishing, dll. Selain itu, terdapat juga kesalahan yang dilakukan nasabah yang menyebabkan juga masalah keamanan internet banking seperti Jarang mengupdate akun dan memberi password yang mudah ditebak. Selain itu dengan usaha untuk meningkatkan *Awareness* (Baik dari manajemen hingga nasabah), membuat policy/prosedur yang baik dan mengevaluasi sistem secara berkala. Beberapa hal yang perlu dilakukan oleh nasabah untuk meningkatkan pengamanan akun e-banking pribadi antara lain:

a. Hindari untuk mengakses *Internet Banking* dari tempat-tempat umum, seperti, warnet, dll. Karena aspek keamanannya sangat minimalis.
b. Meminimalisir terjadinya proses phishing dengan menggunakan perangkat yang memiliki Firewall dan Antivirus.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada tim dalam menyelesaikan jurnal dengan tepat waktu dan menghasilkan kualitas studi literatur yang baik.

REFERENSI

[1] Subsom, P, dan Limwiriyakul, S, 2011. *A Comparative Analysis of Internet Banking Security in Thailan : A Customer Perspective*. pp 260-272.

[2] Pratiwi, 2016. JUTISI. *Penerapan Sistem Biometrik pada Nasabah Pengguna ATM (Studi kasus IKPIA Perbanas Jakarta)*, 5 (2), pp. 1042–1047

[3] O. Andriyani, H. Cangara, dan S. Rhiza S, 2014. J. Komun. KAREBA. *Penggunaan Teknologi Informasi Online Dalam Kecepatan Pelayanan Dan Pengamanan Pada Bank BCA Makassar (Sebuah Studi Komunikasi Organisasi),* 3(1), pp. 58–67

[4] Ronny, 2017. *Enam Kekuatan Layanan Jasa Internet banking Tinjauan Dari Presepsi Nasabah*. Surabaya

[5] ***Bodnar, George, H. and Hopwood, William, S. 2004.*** **Accounting Information Systems*. Ninth Edition. Upper Saddle River. New Jersey 07458: Pearson Education Inc. hal 614.***

[6] Ariyus, Dony, 2006. *Computer Security*. Andi Offset: Yogyakarta.

[7] Annisya, Rialda dan Hastuti, Maynina Norshela. 2012. *Security System Layanan Internet Bankinh PT. Bank Mandiri (Persero) Tbk.* Jakarta

[8] Hendarsyah, Decky, 2019. *Keamanan Layaan Internet Banking Dalam Transaksi Perbankan.* Sekolah Tinggi Ilmu Ekonomi (STIE) Syariáh Bengkalis

[9] Purnama, Benni, dan Wijaya, Ibnu Sani, dan Yani, Herti, *STUDI LAYANAN INTERNET BANKING DITINJAU DARI ASPEK KEAMANAN SISTEM INFORMASI (Studi kasus KlikBCA dan BSMNetbanking)*

[10] Rahardjo, Budi, 2001. *Aspek Teknologi dan Keamanan Dalam Internet Banking, Materi Seminar Internet Banking di Banking Research and Regulation Directorate, Bank Indonesia, "Internet Banking : Implementasi dan Tantangan Kedepan.* Jakarta.