YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 3 Nomor 2 Edisi Mei 2018 (1-12)

21

PERANCANGAN SISTEM *INTERNET BANKING (IBANK)* MENGGUNAKAN *ONE-TIME-PASSWORD (OTP)* UNTUK PENGAMANAN TRANSAKSI (STUDI KASUS BANK MEGA, Tbk)

Andi Rosano[1], Nur Ali Farabi[2] , Aliffah Kusumaningrum[3]
Dosen AMIK Bina Sarana Informatika Jakarta, AMIK Bina Sarana Informatika Tangerang, AMIK Bina Sarana Informatika Tangerang
(Naskah diterima: 12 April 2018, disetujui: 27 April 2018)

Abstract

Internet Banking (IBank) has become a very popular banking service product today. In previous IBank system there are weaknesses that enable the theft of data that can ultimately lead to illegal transaction crimes. The use of the concept of financial transaction with One-Time-Password (OTP) is currently being implemented by several national banks to overcome the theft of passwords in line with the widespread development of the public using Internet and mobile phone technology (HP). The author conducts a field study at a private bank part of the system development to learn the implementation of IBank's OTP system use in a faster and safer banking transaction process.

Keywords: *financial transaction, One-Time-Password, safe.*

Abstrak

Internet Banking (IBank) sudah menjadi produk layanan perbankan yang sangat diminati saat ini. Pada sistem IBank terdahulu terdapat kelemahan yaitu memungkinkan terjadinya pencurian data yang pada akhirnya dapat menimbulkan kejahatan transaksi illegal. Penggunaan konsep pengamanan transaksi finansial dengan password sekali pakai atau One-Time-Password (OTP) pada saat ini diterapkan oleh beberapa bank nasional untuk mengatasi pencurian password sejalan dengan perkembangan masyarakat luas yang aktif menggunakan teknologi internet dan telepon bergerak (HP). Penulis melakukan studi lapangan pada sebuah bank swasta bagian pengembangan system untuk mempelajari implementasi penggunaan OTP sistem IBank pada proses transaksi perbankan yang lebih cepat dan aman.

Kata kunci: transaksi finansial, password sekali pakai, aman.

I. PENDAHULUAN

Perbankan sudah semakin banyak, selain terminal yang sudah dikenal yaitu kantor cabang dan cabang pembantu, mesin *ATM* (*automated teller machine*), kantor kas atau *kiosk*, *EDC* (*electronic data capture*) yang berada di toko/pedagang ditempat maupun yang bergerak, bank juga menyediakan fasilitas transaksi berbasis *internet banking (IBank)* dan telepon bergerak (*mobile phone*). Dengan penyediaan fasilitas *IBank*, diharapkan transaksi finansial dan non-finansial dapat dilakukan dari terminal lain selain cabang dan mesin *ATM*.

IBank adalah salah satu terminal pelayanan nasabah yang berbasis pada teknologi *internet* dan telepon bergerak (*mobile phone*). Sistem ini melayani beberapa transaksi yang dapat digolongkan menjadi 2 (dua), yaitu non-finansial terdiri dari informasi saldo, informasi transaksi, informasi nilai tukar mata uang, dan informasi lainnya. Golongan kedua adalah transaksi finansial terdiri dari pembayaran, transfer antar bank, dan pembelian.

Berdasarkan besarnya resiko yang melekat, golongan transaksi non-finansial tidak akan ada kerugian finansial pada nasabah apabila terjadi kegagalan transaksi, maka tingkat pengamanan transaksi cukup sampai pada *approval login*. Untuk transaksi finansial, selain *approval login* nasabah diharuskan melewati otentifikasi meng-gunakan *OTP* (*One-Time-Password*).

Pada tulisan ini akan dibahas perancangan sistem *IBank* yang memanfaatkan *OTP (one time password)* sebagai pengaman transaksional. Adapun teori yang menjadi dasar untuk perancangan implementasi *OTP* pada *IBank* adalah sebagai berikut :

A. Verifikasi Ganda Pengguna

Seorang pengguna *IBank* harus melalui 2 (dua) kali pemeriksaan untuk dapat mengakses sistem *IBank.* Yaitu tahap pertama adalah kebenaran *Login ID*, kedua kebenaran *password* dan jawaban salah satu dari 3 (tiga) pertanyaan verifikasi yang dibuat saat pengguna melakukan registrasi awal. Pemeriksaan ganda ini merupakan lapisan awal pengamanan sistim *IBank* (Musliyana, Zuhar, 2016).

Untuk transaksi yang termasuk transaksi finansial, konfirmasi dilakukan dengan memasukkan kode rahasia yang dibangkitkan oleh sistem securiti dan dikirim melalui *SMS (short message format)* yang dikirimkan oleh sistem *IBank* kepada pengguna melalui *handphone (HP)* yang sudah diregistrasi dan disimpan pada sistem *IBank*. Sehingga

dipastikan penerima kode rahasia atau *password* sekali pakai *(OTP)* adalah pengguna yang bersangkutan.

B. Replay Attack

Salah satu jenis serangan yang lazim ditemui pada jaringan komputer adalah *man-in-the middle attack (MITM).* Salah satu serangan yang dilakukan pada *IBank* dengan metode *MITM* adalah pencurian identitas autentikasi pengguna seperti *Login ID* dan *password* (Paterson, G., dkk,2009). Bila penyerang sudah berhasil mencuri identitas pengguna, penyerang dapat menggunakan ulang *(replay)* identitas tersebut untuk masuk ke sebuah sistem. Hal ini membuat penyerang hanya perlu mencuri identitas sekali saja untuk mendapat hak akses. Jenis serangan ini disebut *replay attack*. (Baskoro, Adin, P., 2016).

Algoritma *OTP*

Proses menghasilkan *password* sekali pakai menggunakan algoritma *One-Time-Password (OTP)* menggunakan suatu perhitungan yang ditunjukkan pada persamaan (1).

OTP = HMAC(K, T) …..... (1)

Keterangan :

- OTP *: One Time Password*.
- HMAC: *Keyed-hash Message Authentication Code* merupakan sebuah fungsi kriptografi yang dikombinasikan dengan *secret key*.
- K(Secret Key) : kode rahasia yang diambil dari kombinasi nomor *Hand Phone (HP)* dan nomor rekening yang disimpan pada *server sistem* sekuriti bank.
- T : jumlah *time-steps* antara eksekusi transaksi dan pembangkitan.

(Ungkawa, Uung; dkk, 2017)

Masa berlaku *OTP* yang dibangkitkan disetting atas dasar kebijakan bank dan bernilai *default* atau tetap (t). Pengguna harus melakukan *entry* nilai *OTP* yang dikirimkan melalui *SMS* yang dikirim ke *Handphone*-nya dalam waktu kurang dari t menit. Bila melebihi atau sama dengan t menit, maka *OTP* dianggap kadaluarsa dan tidak berlaku lagi.

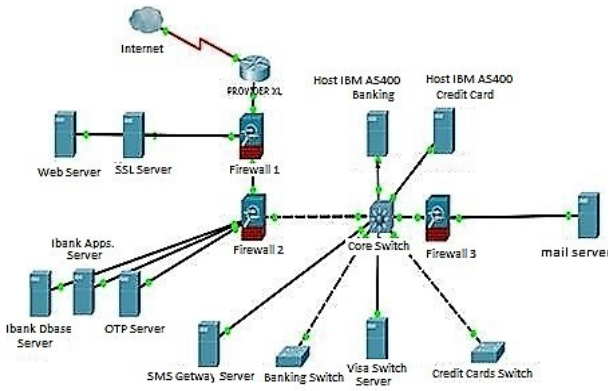
II. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah studi kasus pada sebuah bank swasta nasional , melakukan wawancara dan observasi pada bagian pengembangan sistem, infrastruktur, data komunikasi, *data center*, dan bagian operasional *Ibank* tersebut, survey pada pengguna *Ibank*, dan studi literatur.

Pengumpulan data dilakukan dengan studi dokumentasi file proyek pengembangan sistem, dokumen *SDLC* (*System Development Life Cycle*), wawancara dengan kepala divisi teknologi maupun kepala bagian, Observasi dilakukan pada bagian operasional *IBank* dan *ATM*, serta *data center*. Data transaksi diperoleh dari laporan akhir bulan dan akhir tahun sepanjang tahun 2016 dari bagian *operation division* dan *data center* bank, serta hasil pengisian kuesioner pengguna *IBank*.

A. Rancangan Perangkat Keras

Perangkat keras yang digunakan dapat dilihat pada gambar 1 dibawah ini.



Gambar 1. Topologi Sistem *IBank*
(IT Development Bank Mega2014)

Tersedia 2 sistem besar bank, yaitu sistem utama bank (*core banking system*) dan sistem kartu kredit (*credit card system*), keduanya menggunakan *minicomputer IBM400*. Dua mesin besar ini terhubung melalui *switch* utama (*core switch*) yang menjadi jembatan penghubung untuk seluruh sistem operasional yang ada, yaitu : *SMS getway, user bank switch, user credit card switch*, dan *Visa International switch*. Sedangkan sistem *IBank* yang merupakan *channel public* terhubung ke *firewall* 2 sebelum terkoneksi ke *switch* utama. *Firewall* utama yang terhubung ke *internet public network* melalui *switch provider* XL, merupakan gerbang utama memasuki lingkungan bank. *Website* bank terhubung ke *firewall* 3 di belakang *switch* utama.

B. Rancangan Paket Perangkat Lunak

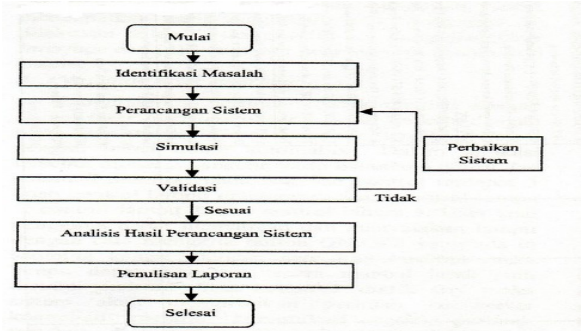
Sistem besar bank menggunakan *OS400* yang merupakan sistem operasi *minicomputer IBM AS400*. *Server* aplikasi sistem *IBank* menggunakan *Linux*, *Apache*, sedangkan *server database IBank* menggunakan *Oracle*. *Mail server* dan *SMS gateway server* menggunakan *Simple Mail Transfer Protocol (SMTP)*, *Post Office Protocol (POP3)*, . *IMAP (Internet Message Access Protocol)*, dan untuk pengaman jaringan disediakan 2 (dua) *firewall server* (Rosano, Andi, 2011).

Sistem sebenarnya juga terhubung ke jaringan internasional kartu kredit, jaringan

ATM Bersama dan jaringan *ATM* BCA (tidak perlu dicantumkan pada gambar).

C. Langkah-langkah Penelitian

Langkah-langkah penelitian yang diawali dengan identifikasi masalah yaitu mengidentifikasi permasalahan penelitian. Dari identifikasi tersebut akan didapat permasalahan yang nantinya akan diselesaikan dalam penelitian. Langkah selanjutnya adalah kegiatan perancangan sistem menggunakan teori dari tinjauan pustaka dan metodologi penelitian yang seiring dengan tema penelitian. Beberapa kajian tersebut berkaitan dengan : (1) perancangan arsitektur sistem *IBank* , (2) peralatan yang dipakai dalam perancangan. Kemudian yang dilakukan adalah perancangan sistem berdasar atas masalah yang muncul pada bagian identifikasi masalah. Langkah-langkah untuk menyelesaikan penelitian ini dijelaskan pada gambar 2 berikut.



Gambar 2. Langkah Penelitian

Hasil dari kegiatan perancangan sistem ini adalah prototype sistem *IBank* menggunakan *OTP* untuk pengamanan transaksi yang masih perlu diuji lagi dalam rangka mengoptimalkan kinerja sistem secara keseluruhan. Selanjutnya pengujian tersebut dilakukan pada bagian-bagian tertentu yang dianggap penting. Pengujian dilakukan sampai tercapai hasil yang terbaik berdasarkan analisis pengujian yang melibatkan beberapa pengguna sebanyak 20 (dua puluh) orang. Selanjutnya hasil pengujian ini menjadi dasar untuk mengoperasikan sistem *IBank* secara penuh.

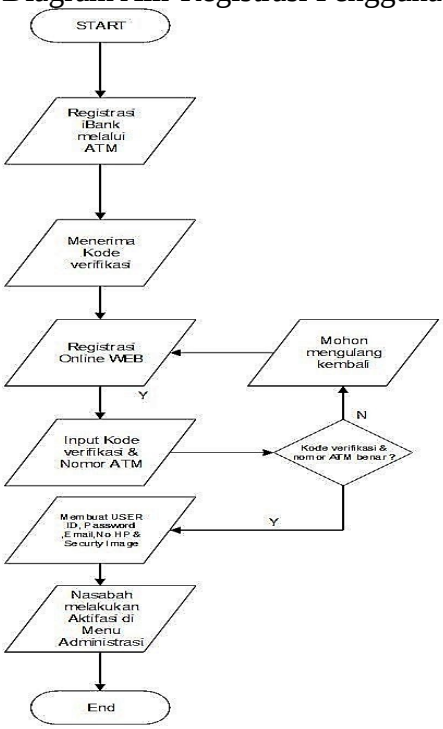
D. Rancangan Alur Proses Transaksi

OTP adalah *password* sekali pemakaian yang dibangkitkan oleh sistim keamanan bank yang diolah berdasarkan algoritma *OTP* dan komponen *secret key* dari pengguna *IBank,* dengan masa berlaku yang sudah ditentukan dalam satuan menit. *OTP* tidak berlaku lagi bila melewati batas waktu tersebut. *OTP* juga hanya berlaku untuk satu kali transaksi saja.

Untuk pembangkitan kunci rahasia (*secret key)*, pengguna *IBank* harus melakukan beberapa hal sebelum dapat bertransaksi, yaitu : 1) Memiliki rekening di bank dimaksud 2) Melakukan registrasi pemakai pada aplikasi *IBank* 3) Memiliki *Handphone* (*HP*) dengan nomor kontak resmi yang didaftarkan pada

sistem untuk konfirmasi transaksi 4) Memiliki alamat *email* resmi yang didaftarkan pada sistem. nasabah bank yang harus dikenal dengan baik dengan identitas yang jelas.

Diagram Alir Registrasi Pengguna



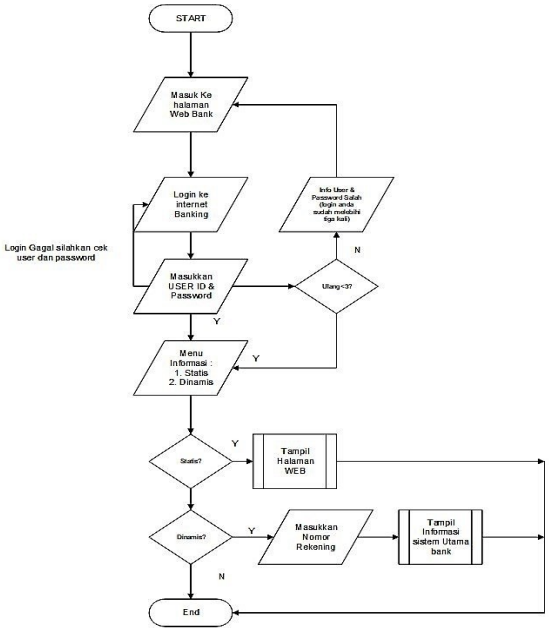
Gambar 3. Diagram Alir Registrasi Pengguna

(IT Development Bank Mega 2014)

Keterangan :

1. Pengguna memakai *ATM* bank untuk melakukan registrasi layanan *IBank*
2. Menerima struk *ATM* berisi kode verifikasi (*verification code*).
3. Melakukan registrasi secara *online* melalui *website* bank, *input* kode verifikasi, dan nomor kartu *ATM*
4. Membuat *User ID*, *Password*, mendaftarkan alamat *email*, nomor *HP* penerima *OTP*, serta memilih gambar pengaman (*security image*) dan pertanyaan pengaman (*security question*).
5. Melakukan aktivasi *OTP* melalui menu administrasi.
6. Proses registrasi selesai.

Diagram alir transaksi non-finansial dapat dilihat pada gambar berikut :



Gambar 4. Diagram alir transaksi non-finansial

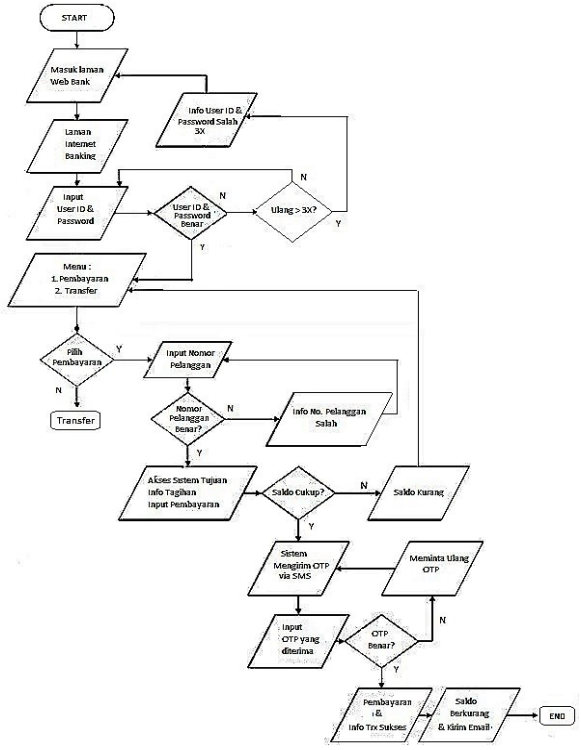
(IT Development Bank Mega 2014)

Keterangan :

1. Mengakses internet ke *website* bank
2. Memasukkan pilihan : *IBank*, masuk ke halaman *Login*
3. Memasukkan *User ID*, masuk ke halaman Verifikasi. Bila *User ID* salah maka gambar pengaman tidak sesuai dengan yang diregistrasikan

4. Memasukkan *password* dan menjawab pertanyaan (1 dari 3 kemungkinan pertanyaan yang muncul), untuk masuk ke menu informasi. Bila *password* salah muncul info *password* salah
5. Pilih menu informasi info, langsung tayang di *website*

Diagram alir transaksi finansial dapat dilihat pada gambar berikut :



Gambar 5. Diagram alir transaksi finansial (IT Development Bank Mega2014)

Keterangann :

1. Mengakses *internet* ke *website* bank
2. Memasukkan pilihan : *internet banking*, masuk ke halaman *Login*
3. Memasukkan *User ID*, masuk ke halaman Verifikasi. Bila *User ID* salah maka gambar pengaman tidak sesuai dengan yang diregistrasikan
4. Memasukkan *password* dan menjawab pertanyaan (1 dari 3 kemungkinan pertanyaan yang muncul), masuk ke menu transaksi. Bila *password* salah muncul info *password* salah
5. Pilih menu transaksi pembayaran atau transfer.
6. Untuk Pembayaran:pilih jenis pembayaran yang akan dilakukan, *input* nomor pelanggan, sistem *IBank* mengakses sistem institusi yang akan dibayar, informasi tagihan ditayangkan ke halaman *website*, pengguna *input* jumlah pembayaran dan nomor *HP* teregistrasi, sistem *IBank* mengakses sistem utama bank untuk mengecek saldo, kemudian sistem *IBank* mengakses sistem institusi yang akan dibayar dan meminta kode otentifikasi ke *OTP server*, sistem *SMS* bank mengirim *password* transaksi ke nomor *HP* teregistrasi, pengguna *input password* transaksi dan menekan '*ENTER*', bila *password* benar maka *IBank* melakukan

pembayaran sesuai perintah, pengguna mendapat jawaban transaksi berhasil dan saldo rekening pengguna di sistem utama bank berkurang sesuai jumlah pembayaran. Sistem *email* bank mengirim notifikasi transaksi ke *email* nasabah dan *SMS* ke nomor *HP* teregistrasi.

7. Untuk Transfer antar rekening : alur transaksi seperti pembayaran, hanya berbeda pada penerima dananya yaitu berupa nomor rekening di bank tujuan yang didahului dengan kode bank tujuan.

Jenis transaksi pada sistem *internet banking* terlihat pada tabel 1 berikut :

No.	MENU	RINCIAN	JENIS	OTP
1	Informasi	Saldo	Inquiry	Tidak
		Mutasi		
		Suku Bunga		
2	Pembayaran	Listrik Pascabayar	Transaksi	Ya
		Telepon Pascabayar		
		PAM		
		Kartu Kredit		
		Handphone Pascabayar		
		TV Berlangganan		
		Tiket		
		Internet		
3	Isi Ulang	Listrik Prabayar	Transaksi	Ya
		Handphone Prabayar		
		Prepaid Card		
4	Transfer	Rekening Satu Bank	Transaksi	Ya
		Rekening Bank Domestik		
		Rekening Luar Negeri		

Tabel 1 : JenisTransaksi *IBank* (Operation Division Bank Mega 2014).

III. HASIL PENELITIAN

Setelah dilakukan perancangan maka langkah selanjutnya adalah melakukan pengujian untuk mendapatkan hasil yang lebih baik. Pengujian ini dilakukan dalam 2 tahap yaitu (1) Pengujian Kemudahan Penggunaan Sistem dan (2) Pengujian kebergunaan (useability) sistem. Metode yang digunakan dalam pengujian ini adalah dengan menggunakan kuesioner. Dimana kuesioner dibagi kepada 20 (dua puluh) pengguna dari berbagai usia yang telah mengerti tentang internet banking dan telah biasa menggunakan internet. Pada awalanya pengguna diberi daftar tugas yang harus dilakukan terlebih dahulu seperti terlihat pada tabel 2 berikut :

No	Tugas
1	Membuka laman Internet Banking
2	Melakukan login awal
3	Melakukan verifikasi pemakai
4	Melakukan inquiry saldo - tanpa OTP
5	Melakukan inquiry transaksi - tanpa OTP
6	Melakukan transaksi pembayaran - dengan OTP
7	Melakukan transaksi transfer antar rekening - dengan OTP
8	Logout

Tabel 2 : Daftar Tugas Pengguna Internet Banking

A. Pengujian Kemudahan Penggunaan Sistem

Pengujian ini bertujuan untuk melihat apakah pengguna sistem internet banking dengan mudah bertransaksi dan tidak menemui kesulitan. Disain website internet banking telah dibuat sedemikian rupa sehingga mudah dipahami oleh pengguna atau nasabah. Petunjuk penggunaan sistem juga

telah dibuat dan dipublikasi dalam bentuk *leaflet* maupun dimuat pada laman informasi.

B. Pengujian Kebergunaan Sistem

Pengujian kebergunaan sistem perlu dilakukan dengan tujuan untuk mengetahui seberapa besar tingkat penerimaan terhadap sistem *internet banking* yang telah dibuat. Sehingga nantinya aplikasi tersebut dengan yakin dapat memenuhi kebutuhan pengguna atau nasabah, dan dirasakan kebergunaannya sebagai sarana bertransaksi bank dengan aman. Untuk memenuhi tugas yang diberikan maka pengguna yang mengunjungi laman situs akan menemukan laman awal situs bank dan terdapat menu untuk menuju *IBank* (gambar 5).

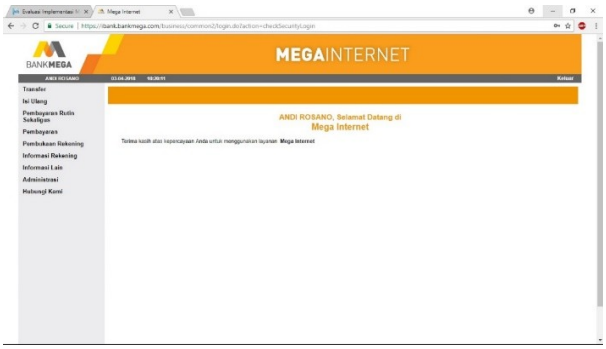
Gambar 6. Laman Awal Internet Banking

Halaman awal *IBank* yang ditampilkan ketika pengguna atau nasabah membuka alamat www.bankmega.com. Pengguna memilih memasuki menu Internet Banking dan menemukan laman *Login* (gambar 6), dan memasukkan *User ID* menuju laman verifikasi pengguna (gambar 7)

Gambar 7. Laman Login Internet Banking

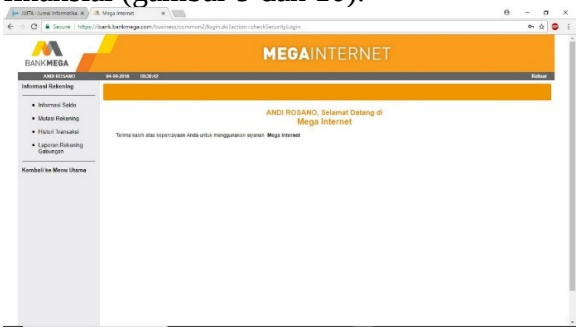
Gambar 8. Laman Verifikasi Internet Banking

Setelah melewati laman verifikasi pengguna akan menuju laman utama internet banking. Selanjutnya pengguna akan memilih sesuai kebutuhannya (gambar 8).



Gambar 9. Laman Utama Internet Banking

Pengguna dapat memilih submenu untuk transaksi Non-finansial maupun transaksi finansial (gambar 9 dan 10).



Gambar 10. Laman Submenu Transaksi Non-finansial

Gambar 11. Laman Submenu Transaksi Finansial

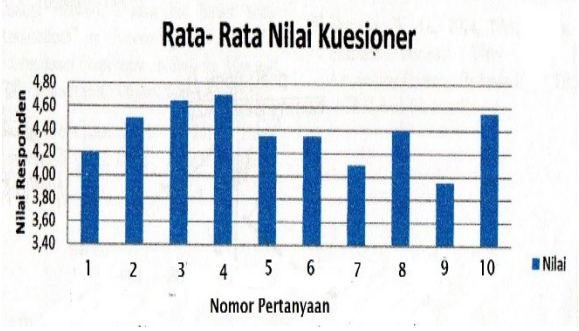
Selanjutnya setelah pengguna melaksanakan tugas yang diberikan, maka pengguna diminta untuk menjawab 10 (sepuluh) pertanyaan. Setiap pertanyaan mempunyai rentang nilai skala 5 *(Skala Likert)*. Pengguna cukup memberikan tanda silang atau centang pada masing-masing pertanyaan (tabel 3). Pertanyaan tersebut dibuat dengan tujuan untuk menunjukkan tingkat kemudahan dan kebergunaan sistem menurut sudut pandang pengguna. Dari 20 (dua puluh) responden yang telah menjawab pertanyaan didapat hasil rerata seperti pada tabel 4.

No.	Pertanyaan	Nilai Skala				
		1	2	3	4	5
1	Apakah proses registrasi internet banking mudah dilakukan?					
2	Apakah website internet banking informatif dan mudah dipahami?					
3	Apakah website internet banking mudah dibuka?					
4	Apakah proses login awal mudah dilakukan?					
5	Apakah verifikasi pengguna mudah dilakukan?					
6	Apakah mengakses informasi saldo mudah dilakukan?					
7	Apakah mengakses riwayat transaksi mudah dilakukan?					
8	Apakah proses transaksi pembayaran mudah dilakukan?					
9	Apakah proses transaksi transfer dana mudah dilakukan?					
10	Apakah proses transaksi dalam waktu kurang dari 3 menit?					

Tabel 3: Daftar Pertanyaan Pengguna Internet Banking

No.	Pertanyaan	Nilai
1	Apakah proses registrasi internet banking mudah dilakukan?	4.20
2	Apakah website internet banking informatif dan mudah dipahami?	4.50
3	Apakah website internet banking mudah dibuka?	4.65
4	Apakah proses login awal mudah dilakukan?	4.70
5	Apakah verifikasi pengguna mudah dilakukan?	4.35
6	Apakah mengakses informasi saldo mudah dilakukan?	4.35
7	Apakah mengakses riwayat transaksi mudah dilakukan?	4.10
8	Apakah proses transaksi pembayaran mudah dilakukan?	4.40
9	Apakah proses transaksi transfer dana mudah dilakukan?	3.95
10	Apakah proses transaksi dalam waktu kurang dari 3 menit?	4.35

Tabel 4 : Nilai Rerata Hasil Kuesioner



Gambar 12. Hasil Kuesioner

Dari hasil hasil kuesioner tabel 4 yang terlihat pada gambar 12, didapatkan bahwa, untuk pertanyaan (1). Apakah proses registrasi internet banking mudah dilakukan didapat hasil rata-rata nilai 4,20. Hal ini menunjukkan bahwa pengguna tidak menemui kesulitan untuk registrasi. Sedangkan untuk pertanyaan ke (2). Apakah website internet banking informatif dan mudah dipahami didapat hasil 4,50. Nilai tersebut juga menunjukkan aplikasi digunakan dengan mudah dan informatif. Selanjutnya untuk pertanyaan ke (3). Apakah website internet banking mudah dibuka didapat hasil 4,65 yang dapat diartikan aplikasi tersebut mudah sekali dibuka. Ke (4) untuk pertanyaan apakah proses login awal mudah dilakukan didapat hasil 4,70. Hal tersebut menunjukkan bahwa pengguna tidak menemui kesulitan sama sekali. Selanjutnya pertanyaan ke (5). Yaitu apakah verifikasi pengguna mudah dilakukan didapat hasil 4,35 yang menunjukkan pengguna dapat dengan mudah mengkases laman utama dengan mudah.

Kemudian untuk pertanyaan ke (6). Apakah mengakses informasi saldo mudah dilakukan didapat hasil 4,35 yang menunjukkan bahwa pengguna sangat mudah mendapatkan informasi saldo. Ke (7). Apakah mengakses riwayat transaksi mudah dilakukan didapat nilai 4,10 juga menunjukkan bahwa pengguna tidak ada masalah. Selanjutnya pada pertanyaan ke (8). Apakah proses transaksi pembayaran mudah dilakukan dengan nilai 4,40 dapat diartikan bahwa pemakaian *OTP* tidak menimbulkan masalah dalam bertransaksi finansial. Ke (9). Untuk pertanyaan apakah proses transaksi transfer dana mudah dilakukan, didapat nilai 3,95 yang menunjukkan bahwa transfer antar rekening mudah dan aman menggunakan OTP. Yang terakhir (10). Untuk pertanyaan apakah proses transaksi dalam waktu kurang dari 3 menit, didapat hasil 4,55 yang dapat diartkan bahwa transaksi sangat cepat tidak melebihi 3 (tiga) menit.

lV. KESIMPULAN

Dari hasil yang sudah didapat tersebut dapat disimpulkan dengan membuat rata-rata hasil bahwa hasil nya adalah 4,35 yang dapat disimpulkan bahwa pengguna internet banking sangat dimudahkan, dan penerapan *OTP (one time password)* untuk transaksi finansial di internet banking sangat mudah dan aman untuk digunakan.

DAFTAR PUSTAKA

Bank Mega. 2016. *Laporan Keuangan*.

Baskoro, Adin, P. 2017. *One-Time Password Berbasis Waktu dan Algoritma RSA sebagai Metode Autentikasi.* Makalah ke-2 IF4020 Kriptografi, Semester I Tahun 2016/2017. ITB Bandung 2017.

Dumais, Barry, M., & Schwartz, Morris (2009). *Principle of Computer Networks and Communications*. Pearson Prentice Hall.

IT Development Division. 2014. *Internet Banking Technical Reference.* Jakarta : Bank Mega.

IT Development Division. 2014. *Internet Banking SDLC (System Development Life Cycle) : System Design.* Jakarta : Bank Mega.

IT Development Division. 2015. *Internet Banking User Acceptance Test Report.* Jakarta : Bank Mega.

IT Operation Division. 2016. *Internet Banking Processing and Procedures Manual.* Jakarta : Bank Mega.

Musliyana, Zuhar. 2016. Peningkatan Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. Jurnal Rekayasa Elektrika, 12(1), 21-29. Retrieved from, http*://www.jurnal.unsyiah.ac.id/JRE/article/view/2896/vol_12*

Operation Division. 2016. *Standard Operation Procedure : Internet Banking.* Jakarta : Bank Mega.

Paterson, G., Kenneth, & Stebila, Douglas. 2009. *One-time-password-authenticated key exchange. Retrieved from* (https*://eprint.iacr.org/2009/430.pdf*, diakses 12 Desember 2017).

Rosano, Andi. 2011. *Efisiensi Biaya dan Optimalisasi Data Rate Pada Jaringan System Banking Online (Studi Kasus : PT Bank Mega, Tbk).* Tesis tidak diterbitkan. Jakarta : MTE UMB Jakarta.

Ungkawa, Uung; Amelia, D., Irma; Ramadhan, P.,Kurnia. 2017. *Implementasi Algoritma Time-Based One Time Password Dalam Autentikasi Token Internet Banking. Retrieved from* (http*://lib.itenas.ac.id/kti/wp-content/uploads/2017/10/Jurnal-Putra.pdf*)