PENERAPAN METODE *SMART AUTHENTICATION* DALAM LAYANAN *E-BANKING* MENGGUNAKAN *TWO CHANNEL AUTHENTICATION* DAN *QR-CODE* PADA PERANGKAT *MOBILE* ANDROID

Ryandi Yusuf[1)], Egi Anggriawan[2)]
Sekolah Tinggi Sandi Negara
Jl. Haji Usa, Ciseeng, Bogor, 16330
Telp : (0251) 8541742, Fax : (0251) 8541720
E-mail : ryandi.yusuf@lemsaneg.go.id[1)] egi.stsn@gmail.com[2)]

Abstrak

E-banking merupakan salah satu layanan perbankan yang menerapkan teknologi dan informasi yang mengalami kemajuan yang pesat, karena E-banking memberikan layanan mobilitas dan fleksibilitas sehingga nasabah mampu mengakses layanan perbankan secara cepat, mudah dan real-time. Oleh karena itu, keamanan menjadi faktor penting dalam menjaga kenyamanan nasabah pada layanan E-banking. Saat ini E-banking masih menggunakan teknik otentikasi yang menggunakan kerahasiaan user ID dan password. Selain itu juga terdapat juga penambahan token security. Akan tetapi teknik otentikasi tersebut saat ini me jadi sangat rentan seiring berkembangnya serangan yang bersifat langsung seperti phising dan man-in-the-middle/browser. Two channel authentication muncul sebagai salah satu solusi yang menawarkan jaminan perbaikan keamanan atas lemahnya keamanan pada teknik single factor authentication. Selain itu, saat ini berkembang pula penerapan QR-code untuk layanan berbasis smart authentication yang menjamin kecepatan proses otentikasi pada transaksi di layanan internet banking. Dari hasil penerapan kedua teknik tersebut mampu memberikan perlindungan keamanan pada layanan internet banking.

Kata kunci: *E-banking, phising, two channel authentication, QR-code.*

Abstract

E-banking is one of the banking service that applies technology and information which is progressing rapidly, because E-banking services on mobility and flexibility so that customers are able to access the banking service efficiently, easily and real-time. Because of that, security is the important factor to keep the customer's convenience on E-banking service. Nowadays, E-banking is still using the authentication technique that uses the user ID's confidentiality and password. There's also an additional token security other than that. However, that authentication technique is becoming very vulnerable lately as the direct attacks develop into things such as phising and man-in-the-middle/browser. Two channel authentication exists as one of the solution that offers security repair guarantee for the security's weakness on single factor authentication technique. Also, the QR-Code application has developed for smart authentication basic service that guarantees the authentication processing speed for transaction in internet banking service. From the application of both technique, we are able to give security protection for internet banking service.

Key word: *E-banking, phising, two channel authentication, QR-code.*

1. PENDAHULUAN

E-banking merupakan bagian dari sistem perbankan secara elektronik yang terpengaruh oleh perkembangan teknologi informasi. *E-banking* menawarkan kenyamanan secara fleksibilitas dan mobilitas yang tinggi sehingga dapat diakses dengan mudah, cepat dan kapan saja selama 24 jam secara *realtime*. Selain itu *E-banking* dapat diakses baik dari *notebook*, komputer, *smartphone*, *tablet*, dan PDA.
Saat ini sebagian layanan *E-banking* masih menerapkan sistem primitif *single factor authentication* yang hanya berdasarkan kerahasiaa *user* ID dan PIN [2]. Penambahan kekuatan yang dilakukan bank yaitu dengan pembangkitan nilai acak (OTP) oleh *token*[3]. Teknik otentikasi seperti *single factor authentication* tidak bisa menghindari serangan langsung seperti *phising, malware* dan *in-the-middle/browser* (MITM) [1], atau jenis

serangan saat ini yaitu sinkronisasi *token* [7]. Salah satu kerawanan yang muncul yaitu saat nasabah mengakses layanan *E-banking* dengan menggunakan akses *internet* publik seperti pada hotel, bandara, tempat makan ataupun *cafe* yang tanpa diketahui keamanan yang dijamin. Selain itu untuk serangan menggunakan *malware* tanpa disadari nasabah mencuri informasi rahasia miliknya. Selain itu, serangan terhadap nilai acak menggunakan *token* saat ini menjadi sangat rentan untuk diserang. Serangan terbaru yang berhasil dilakukan yaitu dengan teknik *phising* dan *malware* (disebut juga sinkronisasi *token*) dengan berpura-pura meminta nasabah menginputkan *response* yang dihasilkan oleh *token* untuk menebak kemungkinan nilai pembangkitan yang dilakukan selanjutnya [7].

Saat ini banyak berkembang metode otentikasi yang mampu menjamin kerahasiaan data milik nasabah. Salah satunya yaitu dengan menerapkan metode *two channel authentication* dan QR-*code*. *Two channel authentication* menerapkan prinsip *two factor authentication* dengan menjamin keamanan terhadap serangan langsung seperti *phising*, sedangkan QR-*code* menerapkan prinsip *smart authentication* yang menjamin kecepatan terhadap otentikasi, selain itu QR-*code* juga memberikan jaminan keamanan yaitu apabila seseorang akan menghitung nilai QR-code maka diperlukan perangkat khusus untuk dapat membacanya sehingga tidak sembarang pihak dapat membaca nilai yang ada pada QR-*code*.

Dalam skema otentikasi yang diajukan, kita asumsikan bahwa nasabah telah mendaftarkan nomor telepon selularnya dan telah melakukan instalasi terhadap aplikasi QR-*code reader* di telepon selular miliknya pada tahap register. Skema otentikasi yang diusulkan menjamin otentikasi pengguna dengan membangkitkan QR-*code* pada sistem *login* yang diperkuat dengan PIN milik nasabah. Lalu penerapan QR-*code* sebagai pengganti dari fungsi *token* yang digunakan oleh bank secara konvensional pada proses transaksi finansial. QR-*code* disini berfungsi sebagai pembangkit bilangan acak sekali pakai (selanjutnya disebut OTP) untuk metode *challenge-reponse protocol* yang dibangkitkan pada kedua pihak (*user* dan *server*). OTP yang dihasilkan merupakan bilangan semu acak yang telah diuji kekuatannya secara kriptografi [8]. Lalu nasabah akan menerima SMS berisi kode verifikasi untuk menerapkan teknik *two channel authentication* pada proses transaksi finansial. Dalam penelitian ini juga digunakan algoritma AES untuk mengenkripsi nilai *response* saat dikirimkan oleh *user*, sehingga mampu menjamin kerahasiaan nilai *response* dari pihak yang berada ditengah jalur komunikasi antara *user* dan *server*. AES dipilih karena dianggap sebagai algoritma yang aman dan menjadi standar yang ditetapkan oleh NIST (*National Institute of Standard and Technology*) untuk penggunaan algoritma simetrik standar [9].

2. KAJIAN YANG TERKAIT

2.1 *Two Channel Authentication*

Saat ini kebanyakan sistem otentikasi masih mengusulkan penerapan *single factor authentication* seperti *password*, *passphrase*, dan nomor PIN untuk otentikasi pengguna [1]. Sudah tidak disangsikan lagi, metode seperti ini sudah tidak lagi menjamin keamanan terhadap serangan dengan teknik langsung seperti *man-in-the-middle* dan *phising*, dimana penyerang mampu mendapatkan informasi rahasia milik target seperti *user* ID, *password* atau PIN tanpa diketahui. Oleh sebab itu penerapan metode otentikasi baru dengan menjamin keamanan terhadap serangan model langsung menjadi satu kebutuhan yang harus terpenuhi untuk dapat melawan serangan pada sistem otentikasi yang terus berkembang [1].

Two channel authentication (TCA) saat ini menawarkan solusi perbaikan keamanan dari *single factor authentication.* Teknik seperti ini bekerja seperti teknik *two factor authentication* tapi menggunakan jaringan yang berbeda dan independen (contohnya jaringan *web* dikombinasikan dengan jaringan *mobile/*GSM) [1]. Teknik TCA mampu memberikan perlindungan terhadap kebocoran informasi yang mungkin terjadi pada teknik *single factor authentication*. Untuk dapat mendapatkan informasi rahasia milik target, maka penyerang harus menyerang semua jaringan yang digunakan oleh target.

2.2 QR-*Code*

QR-*code* atau disebut juga dengan *Quick Response code* [3-6]. QR-*code* merupakan perkembangan dari bentuk otentikasi *bar code*. Sebelumnya untuk beberapa teknik otentikasi yang digunakan yaitu *user* ID, *password, bar code, finger prints, face identity.* Akan tetapi untuk *usern* ID dan *password* saat ini sudah tidak lagi menjamin keamanan, sedangkan *bar code* memiliki keterbatasan penyimpanan yaitu hanya 20 digit. Oleh karena itu, *bar code* tidak bisa digunakan untuk menyimpan *password* yang sangat kompleks [5].

QR-*code* merupakan sebuah *bar code* berbentuk dua dimensi, sehingga mereka dapat dibaca dari segala arah di 360. QR-*code* dapat menyimpan hingga 4296 karakter alfanumerik[5]. Jadi QR-*code* memiliki kapasitas penyimpanan yang jauh lebih banyak dari *bar code*. Keuntungan lain dari QR code adalah dapat dibaca setelah sebagian kerusakan.

Gambar 1. Asitektur QR-code [5].

Berikut merupakan keuntungan dan kerugian menerapkan metode QR-*code* menurut [5], yaitu:

a. Keuntungan penggunaan QR-*code*:
   1. QR-*code* adalah dua dimensi dan dapat dibaca di segala arah (dengan sudut 360 derajat).
   2. Kapasitas penyimpanan QR-*code* adalah hingga 4296 karakter alfanumerik.
   3. QR-*code* dapat dibaca jika terdapat sebagian kerusakan hingga 30%.
   4. Sangat mudah untuk memindai dengan perangkat berbasis kamera.
   5. QR-*code* tidak terbaca oleh orang tanpa menggunakan alat pemindai.
   6. QR-*code* dapat menyimpan data yang disimpan dalam satu dimensi kode bar di sepersepuluh ruang.
   7. Hal ini dapat menangani berbagai jenis data seperti angka dan abjad.
b. Kerugian penggunaan QR-*code*:
   1. Hanya dapat dibaca menggunakan suatu perangkat tertentu (pemindai QR-*code*).

2.3 *One-Time Password*

One time password merupakan teknik autentikasi yang hanya berlaku untuk satu kali penggunaan [8]. OTP menjamin keamanan terhadap serangan *replay*, dimana penyerang yang berhasil mendapatkan nilai OTP yang sudah digunakan tidak mungkin dapat digunakan kembali.

OTP menggunakan algoritma pembangkitan dengan sifat semu acak yang telah diuji secara kiptografi [8]. Berikut merupakan metode-metode yang digunakan pada pembangkitan OTP menurut [8], yaitu:

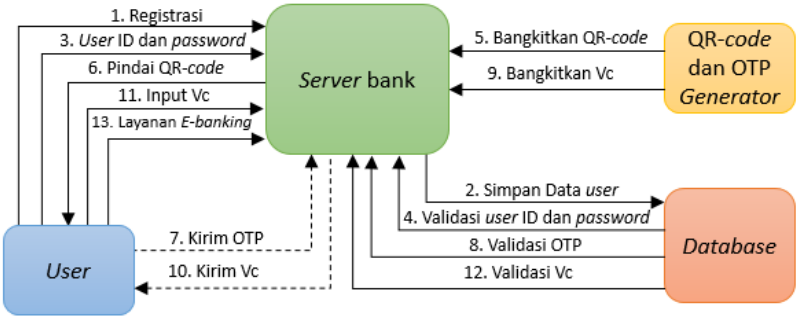
a. Berdasarkan sinkronisasi waktu, metode seperti ini digunakan untuk otentikasi antara *client* dan *server* karena hanya berlaku untuk waktu yang singkat.
b. Berdasarkan suatu algoritma matematika yang menggunakan masukkan nilai OTP sebelumnya untuk mendapatkan nilai OTP baru.
c. Berdasarkan suatu nilai *challenge* dimana OTP dihasilkan dari suatu algoritma matematika yang mengkombinasikan pengetahuan terhadap nilai rahasia *challenge* (contoh metode seperti ini diterapkan pada otentikasi untuk suatu transaksi atau *counter*).

2.4 *Advanced Encryption Standard* (AES)

AES atau *advanced encryption standard* merupakan algoritma enkripsi simetrik yang mampu menggunakan kunci bevariasi yaitu 128, 192, dan 256 bit untuk melakukan proses enkripsi dan dekripsi dengan ukuran blok 128 bit [9]. AES merupakan standar yang ditetapkan oleh NIST (*National Institute of Standard and Technology*) untuk penggunaan algoritma simetrik standar. AES terdiri dari *round-round* yang memiliki proses yang sama dan hanya berbeda pada *round* terakhir. Setiap *round* pada AES memiliki empat komponen utama yaitu, *Subbytes*, *ShiftRows*, *MixColumn*, dan *AddRoundKey* [9].

3. SKEMA OTENTIKASI YANG DIUSULKAN

Skema otentikasi yang kami ajukan akan mengembangkan dua aplikasi *E-banking* yang menjamin keamanan data nasabah. Dari sisi *sever* bank kami menggunakan pemrograman berbasis *web* dan dari sisi nasabah sebagai pengguna kami menggunakan perangkat android sebagai pemindai QR-*code* yang dibangkitkan *server* bank dan juga menerima kode verifikasi yang dikirimkan *server* bank sebagai langkah terakhir pada tahapan otentikasi melalui layanan SMS.



Gambar 2 Skema sistem otentikasi yang diajukan

Penjelasan mengenai skema otentikasi pada Gambar 2, yaitu:

1. Nasabah (selanjutnya disebut pengguna) melakukan proses registrasi untuk dapat mengaktifkan layanan *E-banking* dengan mendatangi bank dan mengisi formulir yang telah disediakan bank. Pada proses registrasi nasabah akan mendaftarkan nomor telepon selularnya dan melakukan instalasi aplikasi pemindai QR-code pada *smartphone* android miliknya.
2. Bank akan menyimpan semua informasi mengenai pelanggan ke dalam *database* bank termasuk *password* dan nilai rahasia yang akan digunakan untuk melakukan perhitungan OTP. *Database server* akan dienkripsi untuk melindungi data nasabah.
3. Pengguna melakukan proses *login* untuk dapat mengakses layanan *E-banking* menggunakan komputer milik nasabah. Pengguna menginputkan *user* ID dan *password*. *User* ID dan *password* merupakan suatu *request* untuk meminta membangkitkan QR-*code.*
4. *Database server* bank akan melakukan validasi terhadap *user* ID dan *password* pengguna.
5. QR-*code* akan dibangkitkan dan langsung muncul di layar komputer pengguna. Tahapan pembangkitan QR-*code* akan dijelaskan lebih lanjut pada bagian selanjutnya.
6. Pengguna memindai QR-*code* menggunakan aplikasi pemindai QR-*code* yang telah diinstal pada proses registrasi awal.
7. QR-*code* yang telah dipindai menggunakan aplikasi pemindai QR-*code* akan menghitung nilai OTP. Nilai OTP tersebut akan dienkripsi menggunakan algoritma AES-128, lalu mengirimkan nilai OTP tersebut kepada *server bank*.
8. *Database server* bank akan melakukan validasi terhadap nilai OTP.
9. *Server* bank akan membangkitkan kode verifikasi (V_C) sebagai tahap akhir otentikasi menggunakan jaringan GSM pada layanan SMS. Kode verifikasi berupa 6 digit angka acak yang dibangkitkan menggunakan OTP *generator*.
10. Kode verifikasi dikirimkan ke telepon selular pengguna menggunakan layanan SMS pada jaringan GSM.
11. Pengguna memasukkan kode verifikasi ke *web E-banking* yang ada di komputer pengguna.
12. *Database server* bank akan melakukan validasi terhadap kode verifikasi.
13. Setelah melakukan tahap otentikasi, maka pengguna dapat menggunakan layanan *E-banking* yang disediakan.

Untuk proses transaksi perbankan, skema otentikasi yang kami usulkan dalam melakukan perhitungan nilai *challenge-response* akan menggunakan QR-*code*. Aplikasi pemindai QR-*code* pengguna akan menggantikan fungsi *token* pada umumnya. Proses pembandingan dan pembangkitan kode verifikasi memiliki langkah yang sama seperti pada Gambar 2. Untuk nilai QR-*code* yang dibangkitkan memiliki waktu toleransi yang berlaku yaitu selama 60 detik. Jika pengguna telah melewati waktu toleransi saat memindai maka *server* akan menampilkan pemberitahuan bahwa pengguna telah melewati waktu yang ditentukan. Hal tersebut berfungsi untuk mencegah siapa saja melakukan *brute force* terhadap QR-*code*. Jika pengguna ingin meminta QR-*code* baru maka pengguna hanya perlu melakukan *refresh* terhadap halaman *web*. Berikut merupakan tampilan aplikasi yang kami bangun sebagai simulasi dari proses yang kami ajukan:

Gambar 3 Tampilan login pada website bank untuk layanan E-banking

Gambar 4 Tampilan menu login pada aplikasi pemindai QR-code milik pelanggan

Gambar 5 Tampilan menu utama pada aplikasi pemindai QR-code milik pelanggan

Gambar 6 Tampilan aplikasi pemindai saat memindai QR-code dari website E-banking

4. ANALISIS KEAMANAN

Penerapan metode otentikasi primitif dengan mengandalkan kerahasiaan *user* ID dan *password* ssat ini sudah tidak lagi menjamin keamanan terhadap serangan langsung seperti *phising*, *malware* dan *man-in-the-middle* [1]. Alasan ini berlaku jika sistem tidak bisa menjamin bahwa transaksi yang dilakukan adalah benar dilakukan oleh pihak yang sah. Salah satu kasus terbaru yang menyerang keamanan *E-banking* yaitu dengan teknik *phising* (sinkronisasi token). Penyerang berhasil membobol dana nasabah pada 3 bank besar di Indonesia yang masih menerapkan metode otentikasi primitif [7].

Berbeda halnya dengan menerapkan teknik otentikasi menggunakan TCA dan QR-*code*, keamanan akan dijamin dengan penggunaan dua jaringan komunikasi (GSM dan *web*) dimana penyerang tidak akan memperoleh akses penuh terhadap akun *E-banking* nasabah. Untuk melakukan serangan tehadap akun *E-banking* nasabah maka yang diperlukan oleh penyerang yaitu:

1. Mengintip *user* ID dan *password* milik pengguna yang diperlukan untuk *login* ke *website* bank;
2. Memindai QR-*code* yang dibangkitkan oleh *website* bank dengan menebak algoritma, nomor rekening pengguna, *password* dan kunci yang digunakan sama dengan milik pengguna;
3. Mencuri *smartphone* tanpa diketahui pengguna dan memotong akses dengan menebak *password* aplikasi pemindai; dan
4. Mengetahui *password* pribadi dari *smartphone* pengguna untuk mengetahui SMS berisi kode verifikasi yang diterima.

Metode otentikasi menggunakan TCA dan QR-*code* dikatakan aman terhadap serangan langsung seperti *phising*, *malware* dan *man-in-the-middle* karena menerapkan metode *challenge-response protocol*. Perhitungan nilai

response akan berbeda jika menggunakan *token*, yang mana nilai *challenge* akan ditampilkan di layar dan memberikan kesempatan penyerang untuk menghitung kemungkinan nilai *response* yang muncul selanjutnya [7]. Sementara jika menggunakan metode yang kami usulkan maka nilai *challenge* akan dirubah menjadi QR-*code* untuk menghindari penyerang dengan mudah menghitung nilai *response.* Selain itu pada sisi pengguna, aplikasi diperkuat dengan nilai *password* untuk melindungi aplikasi tersebut dari pihak lain dan kode verifikasi sebagai langkah akhir otentikasi yang dikirimkan melalui layanan SMS kepada telepon selular nasabah.
Serangan langsung yang berkembang saat ini yaitu teknik serangan dengan mencari celah terhadap kecerobohan pengguna. Dengan maksud bahwa serangan yang memanfaatkan kecerobohan pengguna terhadap kerahasiaan informasi seperti *user* ID, *password* dan *response token* lebih mudah dilakukan tetapi memberikan dampak serangan yang berbahaya. Akan tetapi dengan penerapan skema otentikasi yang kami ajukan maka serangan tidak memberikan pengaruh terhadap keamanan. Contohnya yaitu teknik seperti *phising* menggunakan *key logger* tidak dapat melakukan serangan yang efektif karena tidak dapat merekam nilai yang tersembunyi dibalik QR-*code.* Ataupun jika skenario terburuk dari kebocoran algoritma atau aplikasi pemindai QR-*code* berhasil di *break* total maka penyerang masih membutuhkan sebuah kode verifikasi untuk mendapatkan akses terhadap akun *E-banking* nasabah. Dengan kata lain bagi penyerang yang ingin menyerang harus memperoleh semua akses yang disyaratkan.

5. KESIMPULAN

Tulisan ini memberikan suatu alternatif keamanan terhadap penggunaan layanan *E-banking*. Dengan perkembangan yang pesat terhadap penggunaan layanan *E-banking* maka setidaknya pihak bank mampu memberikan rasa nyaman dengan menyediakan keamanan terhadap dana nasabah yang disimpan di bank. Namun saat ini kenyataannya penerapan *single factor authentication* dengan mengandalkan kerahasiaan *user ID* dan *password* masih diterapkan. Sehingga memberikan celah untuk berkembangnya teknik serangan langsung seperti *phising, malware,* dan *man-in-the-middle* terhadap sistem keamanan pada layanan *E-banking.* Penerapan QR-*code* dan TCA yang kami ajukan dinilai mampu menahan serangan langsung seperti teknik *phising, malware* dan *man-in-the-middle* (contohnya sinkronisasi *token*). Kelemahan dari sistem otentikasi yang kami ajukan yaitu langkah yang diterapkan lebih banyak dibandingkan dengan teknik *single factor authentication,* akan tetapi langkah-langkah tersebut untuk memperkuat pengamanan layanan *E-banking* menjadi lebih baik. Perbandingan yang dilakukan dengan skema yang ada saat ini yaitu dari segi aspek keamanan, kenyamanan dan kecepatan perhitungan *challenge-response.*

6. REFERENSI

[1] Al-Fairuz, M., Renaud, K., 2010. *Multi-Channel, Multi-Level Authentication For More Secure eBanking*. University Of Glasgow. UK.

[2] Kumar, S., Temkar, R., Raj, N., 2013. QR Code Based Secure OTP Distribution Scheme for Authentication in Net-Banking. *International Journal of Information Science and Intelligent System,* Vol.2, *Issue* 4, pp 115-121.

[3] Gandhi, A., et.al., 2014. Advanced Online Banking Authentication System Using One Time Passwords Embedded in Q-R Code. *International Journal of Computer Science and Information Technologies,* Vol.5 (2), 2014, pp 1327-1329.

[4] Yoo, S., Shin, S., Ryu, D., 2013. *The 7th International Conference on Information Security and Assurance: An effective Two Factor Authentication Method using QR code.* Cebu, Philippines 26-28 April 2013. Tasmania, Australia.

[5] Shamal, S., Monika, K., Neha., 2014. Secure Authentication for Online Banking Using QR Code. *International Journal of Emerging Technology and Advanced Engineering,* Vol.4, *Issue* 3, 2014, pp 778-781.

[6] Murkute, J., et.al., 2013. Online Banking Authentication System Using QR-code and Mobile OTP. *International Journal of Engineering Research and Applications,* Vol.3, *Issue* 2, 2013, pp 1810-1815.

[7] Muzakki, K., 2015. Dana Nasabah Rp 130 M Dibobol. *Koran SINDO*, 16 April. 1. 2b.

[8] Kalaikavitha, E., Gnanaselvi, J., 2013. Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology. *International Journal of Engineering and Science,* Vol.2, Issue 10 (April 2013), pp 14-17.

[9] Federal Information Processing Standards. 2001. *Advanced Encryption Standard* (AES) [Online] (Updated 26 Nov 2001). Available at: http://www.csrc.nist.gov [Accessed 26 April 2015]

[10] Stranberger, G., Froihofer, L., Goeschka, K., 2009. *International Conference on Availability, Reliability and Security: QR-TAN: Secure Mobile Transaction Authentication.* Fukuoka, Japan 16-19 March 2009. Austria.