Prosiding Seminar Nasional Sistem Informasi
dan Teknik Informatika
pp. 36-53, 2021

ISSN xxxx-xxxx online

Implementasi *One Time Password* dengan Metode Advanced Encryption Standard

Oesman Hendra Kelana[1*], Paulus Lucky Tirma Irawan[2] dan Patricia Meiliana Halim

[1, 2]Teknik Informatika Universitas Ma Chung, Villa Puncak Tidar N-01 Malang 65151

Correspondence: Oesman Hendra Kelana (oesman.hendra@machung.ac.id)
Received: *15 Agustus 2021* – Revised: *10 September 2021* - Accepted: *1 November 2021*

Abstrak. Teknologi yang terus berkembang membutuhkan tingkat keamanan yang tinggi, terutama dalam menjaga password. Untuk mengatasi password yang harus diubah dalam jangka waktu tertentu, digunakanlah One-Time Password (OTP). OTP sudah berhasil diimplementasikan dalam berbagai kasus perbankan menggunakan token. Penelitian ini bertujuan untuk mengimplementasikan OTP dalam smartphone, terutama Android yang diharapkan dapat menggantikan fungsi token yang sudah ada. Metode yang digunakan untuk membangkitkan OTP dalam penelitian ini adalah metode AES (Advanced Encryption Standard). Aplikasi berbasis Android yang dihasilkan dapat menggantikan fungsi token yang ada saat ini. Selain itu, dalam mengimplementasikan algoritma kriptografi AES untuk OTP berdasarkan challenge, aplikasi ini menggunakan secret number yang akan bertambah seiring dengan jumlah pembangkitan OTP.

Kata kunci: One-Time Password, Advanced Encryption Standard, Android, token, challenge

Citation Format: Kelana, O.H., Irawan, P.L.T, & Halim, P.M. (2021). Implementasi *One Time Password* dengan Metode Advanced Encryption Standard. *Prosiding Seminar Nasional Sistem Informasi dan Teknik Informatika (SAMA SISI)*, 36-53.

Prosiding Seminar Nasional Sistem Informasi dan Teknik Informatika
pp. 36-53, 2021
ISSN xxxx-xxxx online

PENDAHULUAN

Keamanan merupakan hal yang penting dalam perkembangan teknologi saat ini. Teknologi yang semakin berkembang, memungkinkan terjadinya penyadapan informasi. Untuk mencegah terjadinya penyadapan informasi diperlukan proses otentikasi menggunakan sandi atau password. Pada hakikatnya, sebuah password atau sandi hanya boleh diketahui oleh pemiliknya saja, namun password itu sendiri masih dapat disadap oleh orang lain. Salah satu cara untuk mengamankan password agar tidak diketahui orang lain adalah dengan melakukan perubahan password secara berkala, namun pengguna akan mengalami kendala dalam mengingat password yang baru secara terus menerus.

Berbagai penelitian telah dilakukan untuk mengatasi permasalahan di atas, salah satunya adalah penelitian tentang One-Time Password (OTP). Sesuai dengan namanya, OTP akan menghasilkan password yang akan berlaku satu kali dalam setiap transaksi sehingga dapat juga disebut password sekali pakai (Kalaikavitha & Gnanaselvi 2013). Pembangkitan OTP dapat dilakukan dengan membangkitkan serangkaian angka acak, melainkan hal ini memiliki kelemahan karena membutuhkan database yang besar.

OTP tidak dapat berdiri sendiri tanpa adanya metode algoritma kriptografi. Algoritma kriptografi dapat meningkatkan keamanan informasi seperti otentikasi (authentication), mencegah penyangkalan (nonrepudiation), dan menjaga kerahasiaan (confidentiality). Metode OTP telah diimplementasikan oleh sejumlah bank di dunia, termasuk Indonesia, sebagai metode untuk pengamanan transaksi online banking.

Implementasi OTP dalam transaksi online banking menggunakan alat tambahan berbentuk seperti kalkulator kecil yang disebut security token (disebut juga token). Token adalah kumpulan klaim atau informasi tentang pemilik dan dapat digunakan untuk menyatakan ikatan antara rahasia atau kunci otentikasi dan keamanan (Jammes, Mensch & Smit 2005). Namun, penggunaan token juga memiliki kelemahan. Sebuah token didesain secara unik, sehingga setiap pihak yang mengembangkan model pengamanan ini kemungkinan besar memiliki jenis token yang berbeda satu sama lain, sekalipun secara garis besar memiliki fungsi dan bentuk fisik yang tidak jauh berbeda. Selain itu, penggunaan token cenderung tidak praktis bagi pengguna layanan dikarenakan dibutuhkan *n* buah token fisik yang berbeda untuk n buah layanan dari penyedia layanan yang berbeda.

Seiring dengan berkembangnya peralatan teknologi yang ada saat ini, penggunaan telepon genggam pintar atau biasa disebut smartphone meningkat. Smartphone adalah tren

Prosiding Seminar Nasional Sistem Informasi dan Teknik Informatika
pp. 36-53, 2021
ISSN xxxx-xxxx online

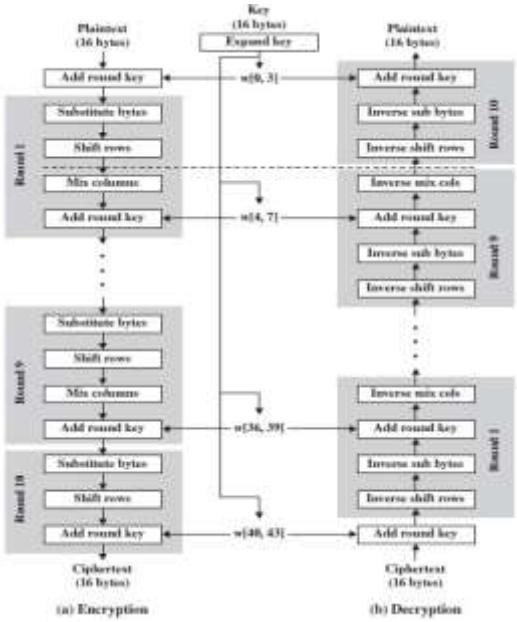
dari komunikasi terpadu yang mana mengintegrasikan telekomunikasi dan layanan internet ke dalam sebuah alat dikarenakan smartphone telah menggabungkan portabilitas telepon genggam dengan kemampuan komputasi dan jaringan dari komputer PC (Guo, Wang & Zhu 2004).

Dalam penelitian ini, metode OTP akan diimplementasikan ke dalam smartphone menggunakan algoritma kriptografi Advanced Encryption Standard (AES). Algoritma AES merupakan algoritma cipher yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia (Yuniati, Indriyanta & C 2009). Selain itu, algoritma AES juga dapat diimplementasikan ke dalam aplikasi yang membutuhkan keamanan data yang cukup tinggi. Bahkan dalam hal membangkitkan OTP, algoritma AES lebih mudah beradaptasi dan lebih cepat performansinya dibandingkan dengan OTP yang menggunakan algoritma hash function (Park et al. 2008).

METODE PELAKSANAAN

Advanced Encryption Standard

AES (*Advanced Encryption Standard*) memiliki blok masukan dan keluaran serta kunci. Terdapat tiga varian kunci dalam AES, yaitu AES 128 bit, 192 bit, dan 256 bit. Terdapat sepuluh putaran dalam algoritma AES, yang ditunjukkan pada Gambar 1.



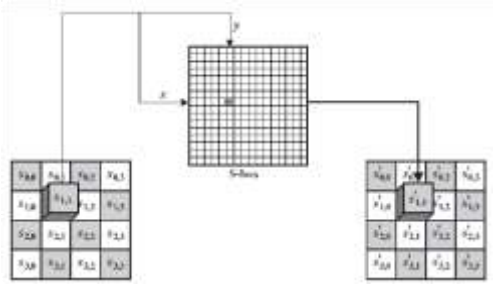
Gambar 1. Proses enkripsi dan dekripsi AES (Stallings, 2017)

Pada awal algoritma ini, *plaintext* atau teks yang akan dienkripsi terlebih dahulu dilakukan operasi XOR dengan *key* sebagai transformasi awal. Setiap putaran terdiri dari subtitusi *byte*, pergeseran baris, *mix columns* (kecuali pada putaran terakhir), dan diakhiri dengan XOR dengan *key* yang telah di-*expand*. Hasil akhir dari algoritma ini adalah *ciphertext* atau teks yang telah dienkripsi.

AES berorientasi dalam *byte* sehingga lebih efisien dalam implementasi algoritma ke dalam *software* dan *hardware*. Dalam algoritma AES, terdapat tiga parameter, yaitu *plaintext*, *ciphertext*, dan *key*. *Plaintext* merupakan sebuah *array* yang berisi data masukan dan berukuran 16 atau 24 atau 32 *byte*. Ukuran dari *plaintext* bergantung pada jenis algoritma AES apa yang digunakan.

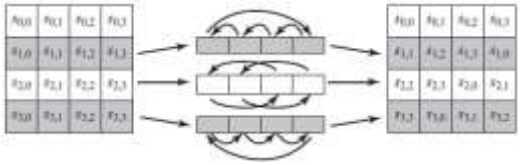
Ciphertext merupakan sebuah *array* yang berisi hasil enkripsi data dan berukuran sama dengan *plaintext*. Karena AES merupakan algoritma simetris dalam kriptografi, maka jumlah key yang digunakan hanya satu dan berukuran sama dengan *plaintext*.

Subtitusi *byte* adalah proses transformasi *byte* dimana setiap elemen dipetakan dengan menggunakan tabel subtitusi (*S-box*). Proses subtitusi *byte* ditunjukkan dalam Gambar 2.



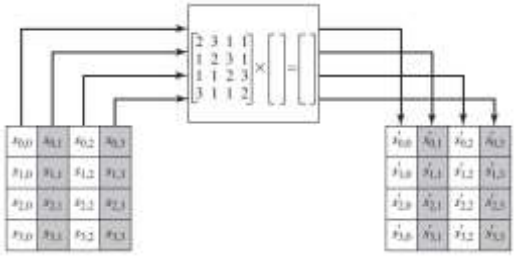
Gambar 2. Proses subtitusi *byte* (Stallings, 2017)

Pada transformasi pergeseran baris (*shift rows*), terjadi sebuah proses perputaran atau pergeseran *bit* yang diterapkan pada baris dua hingga empat. Proses pergeseran baris ditunjukkan pada Gambar 3.



Gambar 3. Proses pergeseran baris (*shift rows*) (Stallings, 2017)

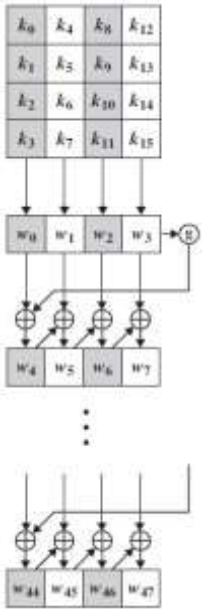
Proses *Mix Columns* adalah proses mengkalikan setiap elemen dengan elemen tetap. Proses *Mix Columns* ditunjukkan pada Gambar 4.



Gambar 4. Proses *mix columns* (Stallings, 2017)

Proses *expand key* untuk setiap putaran ditunjukkan pada Gambar 5.

Dalam setiap proses expand key, key akan dibagi menjadi 4 kolom. Khusus untuk kolom pertama, akan dilakukan fungsi g untuk meng-expand key. Fungsi *g* ditunjukkan pada Gambar 6.

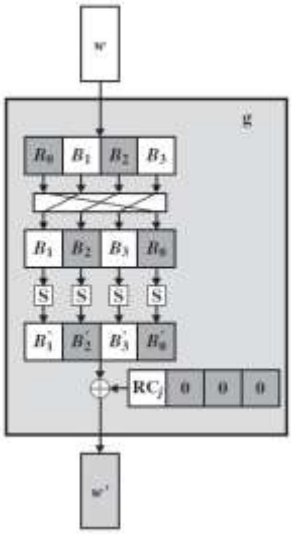


Gambar 5. Proses expand key (Stallings, 2017)

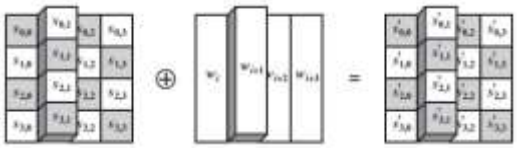
Dalam fungsi *g*, nilai dari setiap kolom akan dilakukan shift row atau pergeseran baris sebanyak 1 kali ke kiri, lalu hasilnya akan dimasukkan ke dalam S-Box. Hasil dari S-Box akan di-XOR dengan nilai round konstanta. Hasil dari proses expand key akan di-

ISSN xxxx-xxxx online

XOR dengan hasil dari mix column dan dinamakan proses Add Round Key yang ditunjukkan pada Gambar 7.



Gambar 6. Fungsi *g* pada proses expand key (Stallings, 2017)



Gambar 7. Proses *add round key* (Stallings, 2017)

One-Time Password

One-Time Password (OTP) adalah *password* yang hanya dapat digunakan untuk satu kali login (*password* sekali pakai). OTP digunakan agar attacker yang ingin menggunakan *password* yang telah dipakai masuk dalam sistem, tidak dapat masuk karena *password* yang digunakan sudah tidak valid lagi. Untuk membangkitkan sebuah OTP, algoritma yang digunakan menggunakan metode random sehingga hasil OTP tidak dapat ditebak polanya. Terdapat tiga jenis OTP yang ditunjukkan sebagai berikut.

1. Berdasarkan waktu (*timesynchronization*). Pada jenis ini, OTP yang dibangkitkan hanya berlaku selama waktu tertentu.
2. Berdasarkan *password* sebelumnya Dengan menggunakan algoritma matematis, *password* yang baru dibangkitkan berdasarkan *password* yang lama.

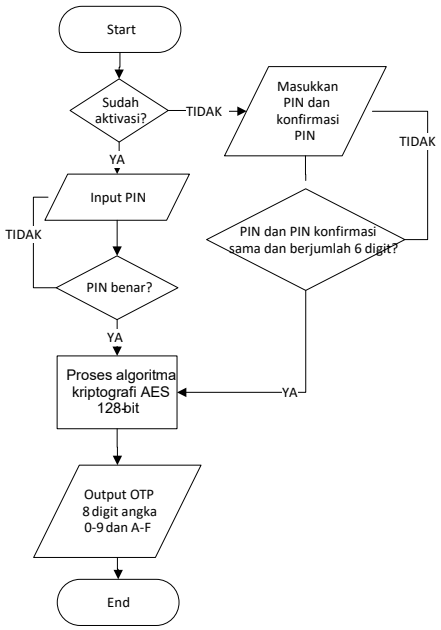
ISSN xxxx-xxxx online

3. Berdasarkan *challenge* Masih menggunakan algoritma matematis, *password* yang baru dibangkitkan berdasarkan pemilihan angka secara acak oleh server atau berdasarkan *counter* (Kalaikavitha & Gnanaselvi 2013).

Perancangan Sistem

Diagram Alir Aplikasi

Berikut akan diberikan diagram aplikasi yang dirancang oleh penulis:

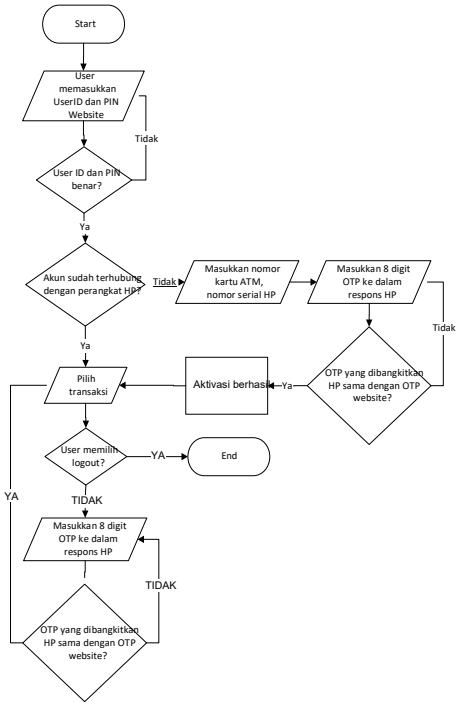


Gambar 8. Diagram alir proses aplikasi.

ISSN xxxx-xxxx online

Diagram Alir Website

Berikut akan diberikan diagram *website* simulasi yang dirancang oleh penulis:

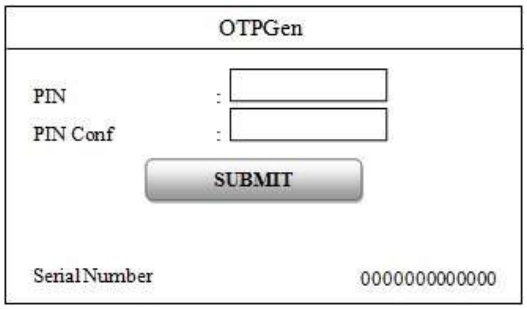


Gambar 9. Diagram alir simulasi *website.*

Desain Antarmuka

Desain Antarmuka Aplikasi

Berikut akan dijelaskan tentang gambaran desain antarmuka dari aplikasi yang dihasilkan oleh penulis:

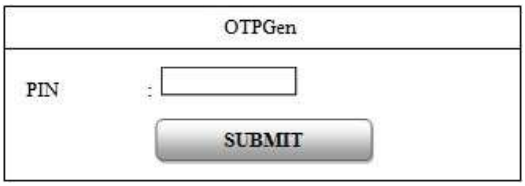


Gambar 10. Tampilan awal.

Tampilan awal pada Gambar 10 akan meminta pengguna untuk memasukkan pin baru pada perangkat. Apabila pin dan pin konfirmasi telah sama dan berjumlah 6 digit,

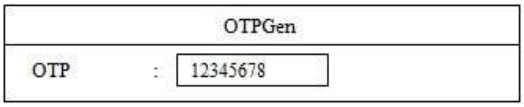
ISSN xxxx-xxxx online

maka pin tersebut akan disimpan ke dalam *database* bersama dengan nomor serial perangkat yang tertera pada aplikasi. Tampilan ini hanya akan muncul ketika pengguna baru pertama kali menggunakan aplikasi ini



Gambar 11. Tampilan masukan PIN.

Tampilan Gambar 11 menunjukkan tampilan ketika pengguna menjalankan program apabila perangkat telah diaktivasi. Pengguna diminta untuk memasukkan PIN sesuai dengan PIN yang dimasukkan pada saat program diaktivasi.

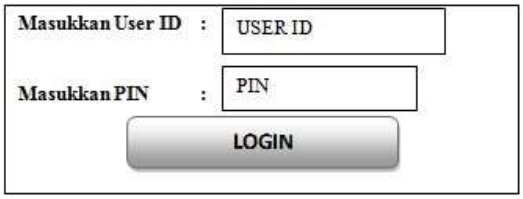


Gambar 12. Tampilan keluaran OTP.

Gambar 12 menunjukkan tampilan keluaran dari aplikasi. Keluaran yang dihasilkan, diletakkan pada sebuah *textView*. Apabila pengguna telah memasukkan kode OTP pada *website*, aplikasi akan secara otomatis berakhir dan kembali pada gambar 9 untuk melakukan inputan PIN kembali apabila pengguna ingin melakukan transaksi kembali.

Desain Antarmuka Website Simulasi

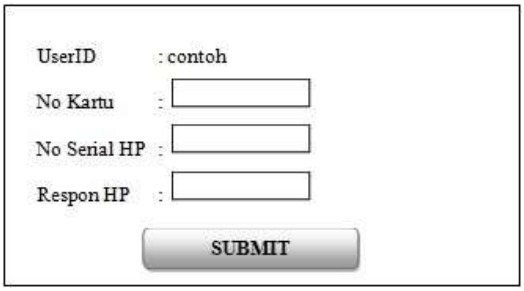
Berikut akan dijelaskan tentang gambaran desain antarmuka dari *website* simulasi yang dihasilkan oleh penulis:



Gambar 13. Tampilan login *website.*

ISSN xxxx-xxxx online

Pada saat pengguna membuka *website*, pengguna diminta untuk memasukkan user id dan PIN seperti yang ditampilkan pada Gambar 11. Setelah memasukkan login dengan benar, maka akan muncul tampilan menu dari *website*. Apabila *website* belum terhubung dengan perangkat manapun, pengguna diminta untuk memasukkan nomor kartu ATM, nomor serial HP dan respon HP seperti yang diperlihatkan pada Gambar 14 agar dapat melakukan transaksi.



Gambar 14. Tampilan aktifasi *website.*

Pada tampilan ini, pengguna diminta untuk memasukkan nomor kartu ATM, nomor serial HP, dan OTP dari perangkat Android yang dimasukkan ke dalam respon HP. UserID yang ditampilkan pada *website* merupakan user ID yang digunakan untuk masuk ke dalam *website* (*login*). Nomor kartu ATM berjumlah 16 digit dan tertera pada kartu ATM pemilik, sedangkan nomor serial HP berupa IMEI, ESN, atau SerialID dari perangkat yang digunakan.

Gambar 15. Tampilan transaksi transfer.

Pada Gambar 15, pengguna diminta untuk memasukkan OTP yang telah dibangkitkan dari perangkat untuk dicocokkan dengan *database*. Apabila cocok, maka transaksi telah berhasil.

ISSN xxxx-xxxx online

HASIL DAN PEMBAHASAN

Uji Coba

Pada penelitian ini, aplikasi diujicobakan ke dalam perangkat *smartphone* Lenovo S890 dengan spesifikasi sebagai berikut:

1. sistem operasi Android v4.1.1 (*Jelly Bean*),
2. prosesor *Dual-core* 1.2 GHz,
3. memori 1GB,
4. Internet

Tampilan Aplikasi

Aplikasi ini dilengkapi dengan *web service* sehingga memerlukan koneksi Internet dan semua data yang digunakan maupun data yang didapat dari aplikasi disimpan di dalam *database* yang berada pada halaman *web* http://otpsimulator.besaba.com/.

Pada saat aplikasi dijalankan, akan tampak tampilan *splash screen* berupa gambaran loading aplikasi dan nama aplikasi seperti yang ditunjukkan pada gambar 16. Proses ini berlangsung selama 6 detik. Pada aktivitas ini, aplikasi melakukan pengecekan apakah pada perangkat pernah diaktifasi sebelumnya. Apabila Android belum diaktifasi sebelumnya, maka setelah beberapa detik, tampilan akan berubah ke tampilan menu aktifasi. Apabila Android telah diaktifasi, tampilan akan menuju ke tampilan menu penginputan pin.

Gambar 16. Tampilan menu *Splash Screen.*

ISSN xxxx-xxxx online

Gambar 17. Tampilan menu aktifasi

Pada tampilan menu aktifasi, pengguna diminta untuk memasukkan 6 digit angka yang berfungsi sebagai PIN aplikasi. Apabila jumlah angka yang dimasukkan tidak berjumlah 6 dan atau masukkan pin dan pin konfirmasi (pin_conf) tidak sama, pengguna akan diminta untuk memasukkan kembali PIN. Selain meminta masukkan berupa pin, pada tampilan menu aktifasi juga ditampilkan nomer serial telepon genggam. Nomor serial ini mengikuti tipe telepon genggam, yaitu IMEI pada tipe GSM, ESN pada tipe CDMA, atau Serial ID pada perangkat yang tidak menyediakan fungsi telepon di dalamnya (*tablet*). Nomor serial ini digunakan untuk menghubungkan perangkat dengan *website* simulasi. *Website* ini bertujuan untuk memeriksa apakah OTP yang telah dibangkitkan masih valid atau tidak.
Apabila pengguna memasukkan pin dan pin konfirmasi sesuai dengan ketentuan, maka aplikasi akan memasukkan nomor serial dan pin yang telah dibuat ke dalam *database* melalui layanan *web service* yang ditunjukkan pada Gambar 18.

Gambar 18. Tampilan memasukkan PIN ke *database*

ISSN xxxx-xxxx online

Jika di dalam database telah terdapat nomor serial yang sama dengan nomor serial pengguna, maka masukkan pin akan ditumpuk dan disesuaikan dengan pin yang terakhir dimasukkan (hal ini dapat terjadi apabila pengguna telah melakukan aktifasi sebelumnya menggunakan perangkat tersebut dan menghapus data yang tersimpan pada aplikasi). Setelah aplikasi berhasil memasukkan data ke dalam *database*, maka aplikasi akan menampilkan OTP_Aktifasi yang dibangkitkan sebagai *password* aktifasi yang menjadi penghubung *website* dengan aplikasi. Waktu yang diperlukan untuk membangkitkan OTP dan memasukkan ke dalam *database* seperti pada gambar 18 bergantung pada kecepatan Internet perangkat. Pada perangkat yang digunakan untuk uji coba, waktu yang diperlukan selama 2-3 detik.

Gambar 19. Tampilan menu OTP_Aktifasi

Gambar 19 menunjukkan tampilan menu OTP_Aktifasi yang dibangkitkan menggunakan algoritma AES. Tampilan menu OTP_Aktifasi menampilkan serial number pada bagian bawah aplikasi. Keluaran yang dihasilkan berjumlah 8 digit yang terdiri dari angka 0-9 dan A-F. Keluaran akan ditampilkan dalam *TextView* dan langsung dimasukkan ke dalam *database*. Keluaran ini akan menjadi input pada aktifasi *website* sebagai Respon HP. Dalam membangkitkan OTP, digunakan juga *secret number* yang berfungsi untuk pembeda antara satu OTP yang dibangkitkan dengan OTP sebelumnya. *Secret number* akan otomatis bertambah jumlahnya seiring dengan jumlah OTP yang telah dibangkitkan. Hasil OTP yang telah dibangkitkan tidak memiliki batas waktu, sehingga dapat digunakan kapan saja, tetapi akan tidak berlaku (tidak valid) apabila pengguna membangkitkan kembali OTP pada perangkat.

ISSN xxxx-xxxx online

Gambar 20. Tampilan menu penginputan PIN

Pada gambar 20, pengguna diminta untuk memasukkan PIN yang telah didaftarkan pada saat aktifasi. Apabila PIN yang dimasukkan salah, pengguna diminta untuk memasukkan kembali PIN yang benar. Setelah PIN yang dimasukkan benar, maka akan ditampilkan menu OTP yang dibangkitkan menggunakan algoritma AES.

Gambar 21. Tampilan menu OTP

Tampilan menu OTP pada Gambar 21 menampilkan keluaran OTP berupa 8 digit yang terdiri dari angka 0-9 dan huruf A-F yang akan dimasukkan ke dalam *website* sebagai pengecekan untuk kevalidan OTP. OTP ini akan berlaku satu kali dan tidak dapat digunakan kembali. Tampilan menu OTP sedikit berbeda dengan tampilan OTP_Aktifasi. Yang membedakan dari kedua tampilan tersebut adalah ada dan tidaknya nomor serial perangkat. Hal ini dimaksudkan, nomor serial akan muncul ketika perangkat belum tersambung dengan *website* penyedia layanan.

Prosiding Seminar Nasional Sistem Informasi dan Teknik Informatika
pp. 36-53, 2021
ISSN xxxx-xxxx online

Tampilan Website Simulator

Dalam melakukan simulasi pengecekan OTP, dibuatlah sebuah *website* untuk menghubungkan antara *website* dengan aplikasi.

Gambar 22. Tampilan awal *website.*

Pada tampilan awal *website*, pengguna diminta untuk memasukkan User ID dan PIN yang telah diberikan oleh pihak penyedia layanan. Untuk membuat User ID yang baru, pengguna harus mendaftar ke penyedia layanan untuk meminta User ID dan PIN. Setelah memasukkan User ID, pengguna harus menghubungkan User ID dengan perangkat bergerak untuk dapat melakukan transaksi.

Gambar 23. Tampilan menu utama.

Tampilan menu utama *website* merupakan informasi akun yang dimiliki pengguna. Pada bagian kanan atas, terdapat nama pengguna sebagai pengingat bahwa Anda masuk sebagai *user* yang tertulis. Pada Gambar 23, dapat dilihat nomor kartu dan nomor serial masih kosong dan menu *Payment* dan menu *Transfer* tidak aktif. Hal ini dikarenakan pengguna belum melakukan aktifasi *website* untuk menghubungkan antara *website* dan perangkat. Untuk dapat melakukan transaksi, pengguna harus melakukan aktifasi yang dapat dilakukan dengan cara memilih menu *Activation*.

Gambar 24. Tampilan menu *Activation.*

Untuk melakukan aktifasi pada *website*, pengguna diminta untuk memasukkan 16 digit nomor yang tertulis pada kartu ATM, nomor serial HP, dan respon HP. Nomor serial HP merupakan nomor identitas pada telepon genggam, yaitu IMEI pada tipe GSM, ESN pada tipe CDMA, atau Serial ID pada perangkat yang tidak menyediakan fungsi telepon di dalamnya (*tablet*). Nomor serial ini dapat dilihat pada bagian bawah aplikasi saat dijalankan, atau dapat juga dilihat pada *Settings – About phone – Status – IMEI/ ESN/ Serial number Information*. Respon HP merupakan 8 digit yang terdiri dari angka 0 – 9 dan huruf A – F yang dihasilkan dari pembangkitan OTP melalui aplikasi pada perangkat. Setelah akun *website* telah diaktifasi dan terhubung dengan perangkat, pengguna dapat melakukan transaksi berupa *Payment* dan *Transfer* dan menu *Activation* akan tidak aktif karena aktifasi hanya dapat dilakukan satu kali. Apabila pengguna telah berganti perangkat dan ingin kembali menggunakan perangkat untuk akun yang sama, pengguna harus menghubungi penyedia layanan untuk me-*reset* akun. Kedua transaksi ini akan meminta inputan berupa OTP yang dibangkitkan melalui perangkat yang telah terhubung.

Gambar 25. Tampilan menu *Payment.*

Pada menu pembayaran atau *Payment*, pengguna dapat memilih untuk membayar PLN, PDAM, atau Telepon. Lalu pengguna diminta untuk mengisikan nomor pelanggan sesuai

ISSN xxxx-xxxx online

dengan jenis pembayaran yang diinginkan beserta dengan jumlah pembayarannya, dan pengguna harus memasukkan 8 digit OTP yang dibangkitkan melalui perangkat.

Gambar 26. Tampilan menu *Transfer.*

Pada menu transfer dana, pengguna diminta untuk memasukkan nomor rekening tujuan beserta dengan jumlah dana yang ingin ditransfer, dan pengguna harus memasukkan 8 digit OTP yang dibangkitkan melalui perangkat.

KESIMPULAN

Berdasarkan hasil penelitian, diambil kesimbulan:

1. Fungsi token yang biasa dapat digantikan dengan menggunakan aplikasi di perangkat begerak, sehingga lebih praktis dan tidak memerlukan peralatan tambahan.
2. Pengimplementasian algoritma kriptografi Advanced Encryption Standard (AES) untuk One Time Password (OTP) berdasarkan challenge menggunakan secret number akan menambah kerahasiaan (confidensialitas) OTP yang dibangkitkan.

UCAPAN TERIMA KASIH

Penelitian ini mendapatkan hibah pendanaan dari Ma Chung Research Grand 2020. Terima kasih untuk dukungan LPPM Universitas Ma Chung dalam membantu terlaksananya penelitian ini.

DAFTAR PUSTAKA

Guo, C. Wang, H.J. & Zhu, W. (2004), Smart Phone Attacks and Defences, *HotNets III, ACM SIGCOMM*, Sandiego.

Jammes, F., Mensch, A. & Smit, H. (2005), Service-Oriented Device Communications Using the Device Profile for Web Services, ICS, *ASM International Conference Proceeding Series, ACM New York*, New York.

ISSN xxxx-xxxx online

Kalaikavitha E.. & Gnanaselvi J. (2013), Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology. *Research Inventy: International Journal of Engineering and Science,* 2(10), 14-17.

Park, S.D., Na, J.C., Kim, Y.H. & Kim, D.K. (2008)., Efficient OTP (One Time Password) Generating using AED-based MAC, *Journal of Korea Multimedia Society,* 11(20), 1-8.

Stalling, W. (2017), *Pearson. Cryptography and Network Security. Principles and Practice. 7th. Ed*. Edinburgh.

Yuniati, V, Indriyanta, G. (2009), Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jenis File, *Jurnal Informatika.* 5(1), 22-31.