RABIT : Jurnal Teknologi dan Sistem Informasi Univrab ISSN CETAK : 2477-2062
Volume 5 No. 2 | Juli 2020 : Hal :108-116 ISSN ONLINE : 2502-891X

PENGAMANAN M-COMMERCE MENGGUNAKAN ONE TIME PASSWORD METODE PSEUDO RANDOM NUMBER GENERATOR (PRNG)

[1)] Muhammad Fahrizal, [2)] Achmad Solichin
[1,2)]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2)]Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta
E-mail : *saya.masfahri@gmail.com, achmad.solichin@budiluhur.ac.id*

ABSTRAK
Mobile commerce atau *m-commerce* merupakan sistem perdagangan elektronik (*e-commerce*) yang menggunakan peralatan bergerak seperti telepon genggam, telepon pintar, PDA, dan notebook. Dengan pertumbuhan pengguna telepon pintar (*smartphone*) di seluruh dunia, banyak pemilik bisnis perdagangan elektronik yang juga menyediakan aplikasi m-commerce untuk mempermudah para pelanggannya dalam bertransaksi. Resiko keamanan merupakan salah satu kendala besar dalam perkembangan sistem perdagangan elektronik yang harus ditangani oleh penyedia aplikasi m-commerce. Oleh karena itu, pada penelitian ini diterapkan metode pengamanan aplikasi m-commerce menggunakan one time password (OTP) yang dibangkitkan dengan metode Pseudo Random Number Generator (PRNG). Penelitian ini juga melakukan modifikasi terhadap algoritme PRNG dengan melakukan tiga kali proses *bit shifting* dan menambahkan algoritme enkripsi. Hasil pengujian menunjukkan bahwa sistem dapat membangkitkan OTP yang selalu unik untuk setiap transaksi dengan rata-rata waktu pembangkitan hanya 0,3320455 detik. Hasil penelitian ini bermanfaat bagi pengembang aplikasi m-commerce untuk mengamankan aplikasinya.

Kata Kunci: keamanan e-commerce, m-commerce, one time password, PRNG

ABSTRACT
Mobile commerce or m-commerce is an electronic trading system (e-commerce) that uses mobile equipment such as mobile phones, smart phones, PDAs, and notebooks. With the growth of smartphone users throughout the world, many electronic commerce business owners also provide m-commerce applications to make it easier for their customers to make transactions. Security risk is one of the major safeguards in developing electronic commerce systems that must be approved by the m-commerce application provider. Therefore, in this research a security method for m-commerce applications is applied using a one-time password (OTP) generated by the Pseudo Random Number Generator (PRNG) method. This study also modified the PRNG algorithm by performing three bit shifting processes and adding encryption algorithms. The test results show a unique OTP system that can be published for each transaction with an average generation time of only 0.3320455 seconds. The results of this study are useful for m-commerce application developers to support their applications.

Keyword: *e-commerce security, m-commerce, one time password, PRNG.*

PENDAHULUAN

Beberapa tahun terakhir, terjadi perkembangan teknologi informasi dan internet di Indonesia mengalami peningkatan yang signifikan. Penetrasi internet di Indonesia tahun 2018 mencapai 64,8% dengan kenaikan sebesar 10,12% dibanding tahun sebelumnya [1]. Tingginya pengguna internet secara tidak langsung mendorong pertumbuhan berbagai model bisnis dan layanan digital seperti e-commerce, e-learning, e-banking, e-newspaper, dan e-money.

Biro Pusat Statistik telah melakukan survey perkembangan e-commerce di Indonesia pada tahun 2019. Walaupun secara umum usaha perdagangan di Indonesia masih menggunakan pola konvensional, namun berdasarkan survey yang telah dilakukan, jumlah transaksi penjualan melalui e-commerce selama tahun 2018 mencapai 17,21 trilliun rupiah [2]. Statistik tersebut menunjukkan bahwa perkembangan e-commerce di Indonesia memiliki peran yang cukup besar dalam menyokong perekonomian nasional.

Selain kemunculan e-commerce, seiring dengan meningkatkan penggunaan telepon pintar (*smartphone*), muncul konsep perdagangan berbasis telepon genggam yang disebut dengan *mobile commerce* atau *m-*

commerce. *Mobile commerce* merupakan sistem perdagangan elektronik (*e-commerce*) yang menggunakan peralatan bergerak seperti telepon genggam, telepon pintar, PDA, dan notebook [3]. Dengan pertumbuhan pengguna telepon pintar (*smartphone*) di seluruh dunia, banyak pemilik bisnis perdagangan elektronik yang juga menyediakan aplikasi m-commerce untuk mempermudah para pelanggannya dalam bertransaksi. Selain memberikan kenyamanan bagi pengguna, penyedia aplikasi m-commerce harus dapat memastikan bahwa pelanggan dapat bertransaksi dengan aman. Resiko keamanan merupakan salah satu kendala besar dalam perkembangan sistem perdagangan elektronik [2].

Beberapa ancaman keamanan yang sering terjadi pada e-commerce antara lain praktek penyalahgunaan kartu kredit (*carding*), serangan *denial of services (dos)*, *social engineering*, dan ancaman program seperti virus, worm, dan trojan [4]. Aplikasi m-commerce pun tidak luput dari ancaman keamanan. Sebuah penelitian yang mengkaji celah keamanan pada 5 (lima) aplikasi m-commerce besar di Indonesia menunjukkan bahwa masih terdapat beberapa celah keamanan yang perlu diwaspadai seperti *SSL Bypass* dan *permission* aplikasi yang membahayakan [5]. Selain itu, berdasarkan laporan dari RiskBased Security, pada kuartal pertama tahun 2020 jumlah pelanggaran terhadap data meningkat 58% dibanding kuartal yang sama di tahun 2019 [6]. Hal tersebut memberikan gambaran pentingnya pengamanan data digital.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan metode pengamanan berbasis *one time password (OTP)* yang dapat diterapkan pada aplikasi m-commerce . OTP merupakan password sesaat yang dibangkitkan pada saat pengguna melakukan login ke situs atau aplikasi [7]. Dengan demikian, selain memasukkan username dan password, pengguna diminta memasukkan sebuah password yang dibangkitkan oleh sistem. Penerapan OTP menjadikan situs atau aplikasi lebih aman dari serangan penyusup dan pihak-pihak yang tidak bertanggung jawab [7].

Salah satu kriteria penting dari OTP adalah tingkat ke-acak-an OTP [8], yang artinya OTP harus benar-benar teracak dan unik. Untuk menghasilkan OTP yang teracak dan unik, dapat digunakan beberapa metode seperti HMAC, Time-based OTP dan algoritme pengacakan PRNG [8]–[10]. Pada proses pembangkitan OTP juga dapat diterapkan algoritma enkripsi untuk meningkatkan keamanan [11]. Pada penelitian ini digunakan algoritme PRNG termodifikasi untuk membangkitkan OTP. Hasil penelitian ini dapat bermanfaat bagi pengembang aplikasi m-commerce untuk mengamankan aplikasinya.

One Time Password (OTP)

Kata sandi atau *password* merupakan kata kunci yang bersifat rahasia untuk melindungi berkas atau data dari akses tanpa izin. *Password* umumnya digunakan untuk otentikasi, otorisasi dan identifikasi. Otentikasi memastikan bahwa pengguna yang mengakses suatu layanan merupakan pengguna yang memang berhak mengakses layanan tersebut. Sementara itu, otorisasi merupakan proses mencari apakah orang yang sudah terotentikasi diijinkan untuk memanipulasi data tertentu. Menurut [10], dua pihak yang saling berkomunikasi harus dapat saling mengotentikasi satu sama lain untuk dapat memastikan sumber pesan. Otentikasi sumber pesan juga memberikan kepastian integritas data, karena dapat digunakan untuk memastikan apakah pesan sudah dimodifikasi atau belum.

One Time Password (OTP) merupakan sebuah algoritme yang menghasilkan kata sandi yang hanya dapat digunakan satu kali. Dibandingkan dengan password biasa OTP

dianggap lebih aman karena password terus berubah, yang berarti bahwa itu tidak rentan terhadap serangan ulangan atau password yang akan dicuri. Dalam konteks autentikasi, OTP biasanya digunakan sebagai mekanisme otentikasi tambahan oleh karena itu OTP sering disebut sebagai dua faktor otentikasi (*two-factor authentication*). Metode otentikasi utama tetap menggunakan username dan password, tetapi untuk dapat bertransaksi anda membutuhkan otentikasi tambahan, disitulah peran OTP [12].

Metode otentikasi ini tidak menggunakan kredensial yang berada dari suatu akun tertentu seperti password maupun username dan tidak pernah konstan, berbeda dengan kredensial login yang berada pada akun user yang tidak akan berubah kecuali user itu sendiri yang menginginkan agar dirubah. One Time Password memiliki keterbatasan, yaitu:

- Mempunyai masa aktif yang sementara.
- Bersifat dinamis
- Hanya dipakai dalam konteks yang sempit

Pseudo Random Number Generator

Random number generator merupakan suatu algoritme yang dirancang untuk menghasilkan suatu urutan nilai yang sulit ditebak polanya, sehingga urutan nilai tersebut dapat dianggap sebagai suatu keadaan acak (random). Menurut [10], bilangan acak yang dihasilkan oleh komputer, termasuk bilangan acak yang diterapkan dalam berbagai algoritme kriptografi, sebenarnya tidak benar-benar acak. Dengan kata lain dikenal dengan istilah bilangan acak semu. Bilangan acak tersebut dapat ditebak susunan atau urutan nilainya jika dapat diketahui algoritme yang digunakan. Dalam kriptografi, bilangan acak sering dibangkitkan menggunakan pembangkit bilangan acak semu atau *Pseudo Random Number Generator (PRNG)*.

PRNG merupakan sebuah algoritme yang menghasilkan suatu urutan nilai yang setiap hasil nilainya bergantung pada nilai yang dihasilkan sebelumnya. Luaran dari algoritme PRNG tidak betul-betul acak, hanya terlihat acak. Hal ini didukung oleh penelitian yang pernah dilakukan sebelumnya [13] yang mengulas beberapa algoritme PRNG. Tidak ada algoritma yang benar-benar dapat menghasilan bilangan acak secara sempurna tanpa ada perulangan selama pembangkit yang digunakan adalah komputer yang memiliki sifat deterministik [10].

Luaran dari pembangkit bilangan acak semu hanya mendekati beberapa dari sifat-sifat yang dimiliki bilangan acak. Walaupun bilangan tidak benar-benar acak hanya dapat dibangkitkan oleh perangkat keras pembangkit bilangan acak, melainkan oleh perangkat lunak komputer, akan tetapi bilangan acak semu banyak digunakan dalam beberapa simulasi ilmu fisika, matematika, biologi dan semacamnya. Beberapa penelitian juga masih menggunakan pembangkitan acak semu tersebut untuk berbagai keperluan [10], [13].

Saat ini terdapat beberapa algoritme pembangkit bilangan acak semu. Berikut ini beberapa diantara algoritme PRNG:

1) *Linear Congruential Generator* (LCG).
2) *Lagged Fibonacci Generators.*
3) *Linear Feedback shift registers.*
4) *Generalised Feedback Shift Registers.*
5) *Blum Blum Shub.*
6) *Mersenne Twister.*

Linear Congruential Generator (LCG)

Linear Congruential Generator merupakan salah satu jenis pembangkit bilangan acak semu. LCG merupakan salah satu algoritma yang bersifat rekrusif linear yang dikombinasikan dengan fungsi modulus [12]. Model matematis LCG dapat dihitung dengan menggunakan persamaan (1).

$$x_{n+1} = \big((a \times x_n) + b\big) \bmod m \quad (1)$$

yang mana x_{n+1} merupakan bilangan acak ke-n dari deretannya, x_n adalah bilangan acak sebelumnya, a adalah faktor pengali, b adalah penambahan bilangan, dan m adalah jumlah karakter / bilangan yang diinginkan.

METODE

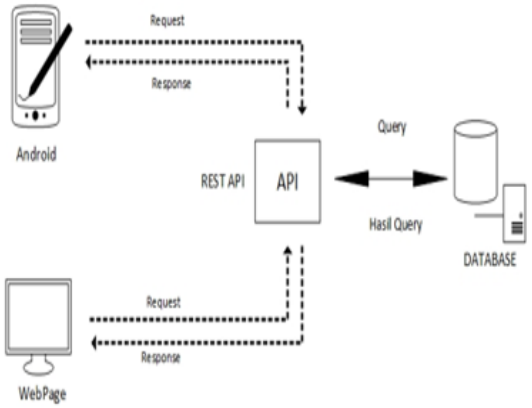
Analisis dan Penyelesaian Masalah

Pada penelitian ini, dikembangkan aplikasi m-commerce untuk FKM Interindo. Selama ini web FKM Interindo dikembangkan berbasis *Wordpress* dan belum disisipkan secara khusus untuk dibuka diperangkat *mobile-friendly*. Dengan pengembangan m-commerce, pelanggan dapat lebih praktis dan mudah dalam melakukan pembelian dan melihat status pemesanan. Namun demikian diperlukan autentikasi keamanan untuk melakukan *login* dan pendaftaran dikarenakan metode keamanan yang digunakan hanya menggunakan *username* dan *password*. Oleh karena itu diperlukan metode keamanan tambahan menggunakan pengaman tingkat kedua.

Tujuan adanya penelitian ini adalah menerapkan *Web Service* berbasis RESTful API (*Application Program Interface*) [14] serta meng-implementasi-kan keamanan pada *e-Commerce* menggunakan *One-Time Password* (OTP) agar ketika melakukan *login* dan pendaftaran pelanggan harus mem-validasi OTP apakah dia benar melakukan login atau pendaftaran atau tidak. Selain itu data akan sangat mudah diakses dengan bentuk data JSON oleh aplikasi *Client* berbeda *platform* seperti *Android* dan *Web*.

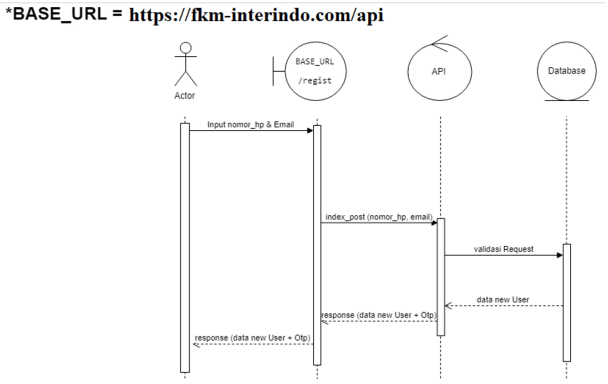
Arsitektur dan Diagram Sequence

Pada program ini terdiri dari rancangan layanan *web service* sebagai penyedia layanan bagi aplikasi lain, rancangan layar pada aplikasi klien *Android* dan *Web*. Serta spesifikasi basis data untuk mengakses data dan menyimpan data yang digunakan pada layanan *web service.*



Gambar 1. Arsitektur Aplikasi

Pada Gambar 1 ditampilkan proses aplikasi mengirimkan sebuah *request* (permintaan) berupa JSON (*JavaScript Object Notation*) ke API, selanjutnya *Web Service* mengeksekusi *query* untuk mengakses basisdata. Setelah proses peng-*query*-an selesai, W*eb Service* akan mengirimkan data atau *response* hasil permintaan (*Request*) kepada aplikasi.

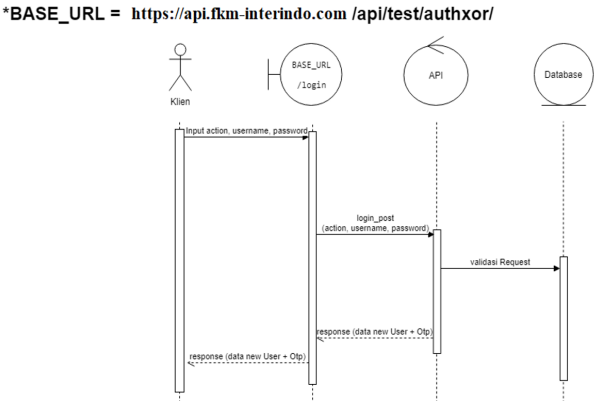


Gambar 2. Diagram Sequence bagian Registrasi

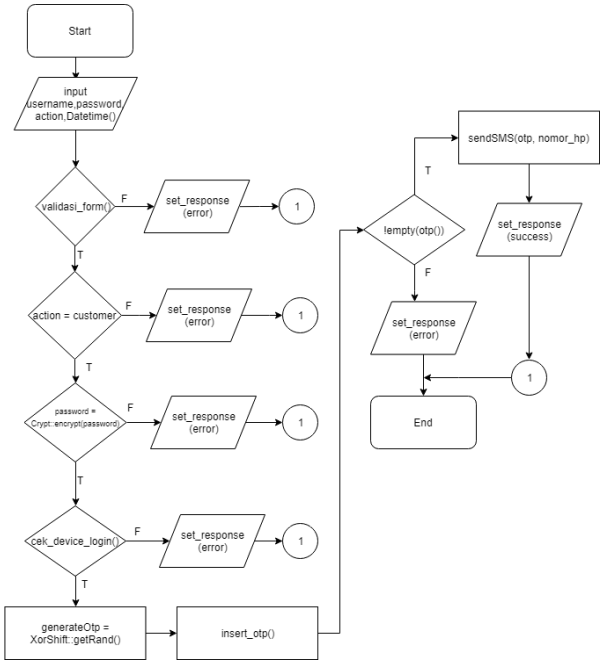
Pada sequence register (Gambar 2), dijelaskan alur untuk melakukan register di aplikasi Klien. Customer (Pelanggan) memasukan nomor Handphone dan Email, setelah itu request fungsi POST ke API, kemudian API memvalidasi nomor Handphone dan Email di basisdata lalu API memberi respon Customer baru yang sudah menjadi format JSON.

Pada diagram sequence login (Gambar 3) dijelaskan alur mengakses API dari Klien. Klien mengakses API login, Klien akan

mengirimkan request POST dengan beberapa parameter pada API, kemudian API meneruskan ke database, request data dari database, setelah itu API mengembalikan request data dan memberi respon *Customer* baru yang sudah menjadi format JSON.



Gambar 3. Diagram Sequence Bagian Login



Gambar 4. Flowchart Aplikasi

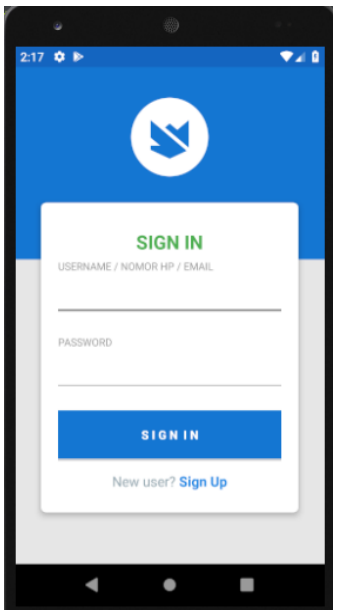
Flowchart dan Algoritme Web Service

Didalam menggambarkan urutan proses pada sistem digunakan flowchart untuk memperjelas alur proses. Gambar 4 merupakan flowchart alur proses login ke aplikasi m-commerce. Proses dimulai saat pengguna memasukkan username dan password melalui form login. Setelah data tervalidasi dan terverifikasi, sistem akan membangkitkan kode OTP yang akan dikirimkan ke pengguna melalui SMS.

HASIL

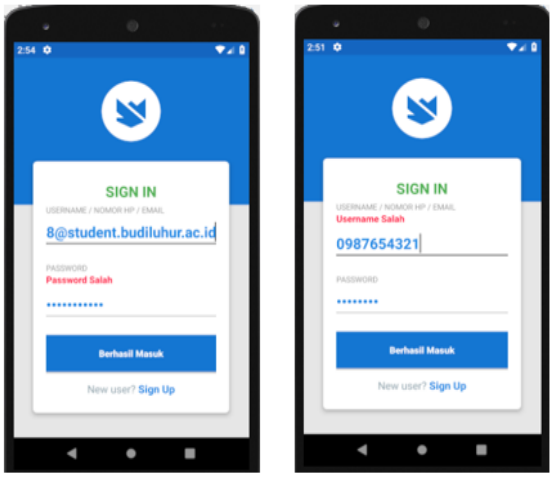
Tampilan Layar

Pada bagianini dijelaskan tampilan layar pada sitem aplikasi android dan *web* berbasis RESTful API dari tampilan awal hingga tampilan yang akan ditunjukan baik dari admin, Pelanggan. Gambar 5 merupakan tampilan layar aplikasi saat pertama kali dibuka. Aplikasi akan menampilkan form login yang dapat diisi menggunakan username dan password pengguna.



Gambar 5. Tampilan Form Login

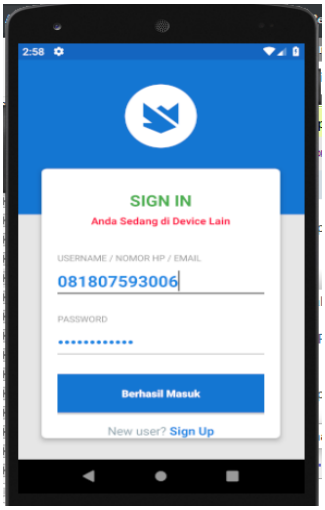
Apabila user mengisi field password dengan data yang salah, maka akan muncul notifikasi yang memberi tahu user bahwa data yang sudah diinputkan salah, seperti pada Gambar 6 bagian (a). Dan jika user mengisi field username dengan data yang salah, maka akan muncul notifikasi yang memberi informasi ke user bahwa data yang sudah diinputkan salah seperti terlihat pada Gambar 6 bagian (b).



(a) (b)

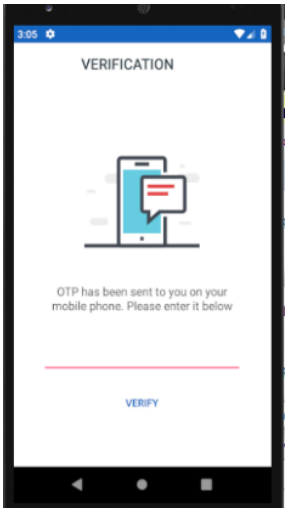
Gambar 6. Pesan Kesalahan Penginputan Username atau Password

Pesan kesalahan seperti terlihat pada Gambar 7 akan muncul jika user berusaha login ke aplikasi namun sudah login di aplikasi atau perangkat yang lain. User tidak dapat login di dua perangkat berbeda secara bersamaan.



Gambar 7. Pesan Kesalahan Login Ganda

Saat user berhasil melakukan Login, maka user akan diarahkan ke aktivitas Verifikasi OTP (Gambar 8) yang mana user harus memverifikasi OTP yang dikirimkan lewat SMS. Apabila user salah melakukan verifikasi OTP yang dikirimkan melalui SMS, maka user akan diberitahukan bahwa OTP salah.



Gambar 8. Permintaan Verifikasi OTP

Pengujian Algoritme OTP

Pengujian ini bertujuan untuk mengetahui seberapa unik OTP yang dihasilkan oleh algoritma pembangkitan OTP. Pengujian dilakukan dengan membangkitkan kode OTP sebanyak 200.000 kali, menggunakan kombinasi pengguna dan waktu login yang berbeda-beda. Tabel 1 menyajikan cuplikan hasil uji coba OTP yang menggunakan algoritma pembangkitan acak Pseudo Random Number Generator (PRNG).

Tabel 1. Cuplikan Hasil Pengujian Pembangkitan OTP

No	User	OTP	Waktu (detik)
1	081807593006	967489	0,000252
2	081807593007	965448	0,054763
3	081807593008	914223	0,088529
4	081807593009	912166	0,155939
5	081807593010	910141	0,221191
6	081807593011	908084	0,745041
7	081807593012	922379	0,712280
8	081807593013	920322	0,678369
..	..	..	..
N	..	..	..
		Rata-rata	0,3320455

Hasil pengujian algoritma OTP menunjukkan bahwa dari 200.000 kali pembangkitan kode OTP, tidak ditemukan angka OTP yang sama. Hal tersebut

menunjukkan bahwa algoritma pembangkitan OTP sangat baik untuk digunakan karena nilai OTP yang dihasilkan bersifat unik. Hasil pengujian ini menjadi salah satu kontribusi utama penelitian ini yang mana berhasil membuktikan bahwa penerapan algoritme pembangkitan OTP dengan PRNG dapat menghasilkan nilai OTP yang benar-benar unik.

Selain itu, dari sisi waktu pembangkitan nilai OTP, secara keseluruhan rata-rata waktu pembangkitan OTP hanya 0,3320455 detik. Dengan demikian, dapat disimpulkan bahwa algoritme pembangkitan OTP dapat menghasilkan OTP dengan sangat cepat.

Pengujian Aplikasi dengan Blackbox

Tabel 2 menampilkan hasil pengujian aplikasi dengan metode Blackbox. Secara fungsionalitas untuk web service 100% berhasil tervalidasi dapat berjalan dengan baik.

Tabel 2. Hasil Pengujian Aplikasi dengan Blackbox

Skenario Pengujian	Harapan	Luaran	Hasil
Login Dengan Mengkosongkan Username pada Login	Response akan memberikan message "Username tidak boleh kosong"	Response web service "Username Tidak Boleh Kosong"	Valid
Login Dengan Mengkosongkan Password pada Login	Response akan memberikan message "Password tidak boleh kosong"	Response web service "Password Tidak Boleh Kosong"	Valid
Login Dengan Mengisi Username dengan yang salah pada Login	Response akan memberikan message "Username Salah"	Response web service "Username Salah"	Valid
Login Dengan Mengisi Password salah dengan Username dengan Benar pada Login	Response akan memberikan message "Password Salah"	Response dari web service dengan message "Password Salah"	Valid
Cek OTP Dengan Mengkosongkan form OTP	Response akan memberikan pesan "OTP Tidak Boleh Kosong" dan OTP akan mengubah statusnya dari aktif ke tidak aktif	Response dari web service "OTP Tidak Boleh Kosong" dan OTP status menjadi expired	Valid
Cek OTP Dengan Menyalahkan OTP dengan yang ada di SMS	Response akan memberikan pesan "OTP Tidak Valid" dan OTP akan mengubah statusnya dari aktif ke tidak aktif	Response dari web service dengan message "OTP Tidak Valid" dan OTP status menjadi expired	Valid
Register Dengan Mengkosongkan Username pada Register	Response akan memberikan message "Username tidak boleh kosong"	Response dari web service dengan message "Username tidak boleh kosong"	Valid
Register Dengan Mengkosongkan Password pada Register	Response akan memberikan message "Password tidak boleh kosong"	Response dari web service dengan message "Password Tidak Boleh Kosong"	Valid

Kelebihan dan Kekurangan Aplikasi

Kelebihan Aplikasi

- Pelanggan dapat memesan produk dengan mudah melalui aplikasi Mobile.
- Pelanggan dipermudah untuk melihat semua produk FKM Interindo digenggaman.
- Pelanggan dapat mengecek status pemesanan melalui aplikasi Mobile.
- Pelanggan notifikasi via SMS apabila pesanan sudah sampai atau sudah diterima oleh Admin.
- Bersifat online.
- OTP yang digunakan tidak akan sama sebagaimana pengujian diatas

- Jika input kode verifikasi OTP tidak sesuai dengan akun pemilik maka user tidak akan mampu masuk ke dalam system web.
- Jika input kode verifikasi OTP melibihi dari 2 menit dari pengiriman pesan maka pelanggan harus melakukan Login kembali.

Kekurangan

- Untuk pemesanan masih dalam jangkauan Daerah Khusus Ibukota Jakarta.
- Pelanggan belum bisa memilih pengiriman produk lebih dari satu alamat.
- Proses login di aplikasi android membutuhkan waktu agak lama dikarenakan proses request fungsi POST ke database lamban.
- Pelanggan kadang tidak dapat notifikasi OTP apabila admin tidak mempunyai pulsa SMS.
- Apabila pelanggan gagal melakukan verifikasi OTP, maka pelanggan harus login ulang (Tidak Ada Re-send Code OTP).
- Hanya pelanggan yang menggunakan device Android yang dapat memesan

KESIMPULAN

Berdasarkan hasil pengujian terhadap metode maupun aplikasi yang dihasilkan pada penelitian ini, dapat disimpulkan bahwa metode pengamanan aplikasi menggunakan OTP dengan algoritme pembangkitan PRNG berhasil diterapkan. Aplikasi dapat membangkitkan OTP dengan cepat dengan rata-rata waktu pembangkitan hanya 0,3320455 detik. Kode OTP yang dihasilkan juga bersifat unik (acak sempurna) sehingga dapat memenuhi kriteria dasar sebuah OTP. Salah satu kontribusi utama penelitian ini adalah berhasil membuktikan bahwa penerapan algoritme pembangkitan OTP dengan PRNG dapat menghasilkan nilai OTP yang benar-benar unik dalam waktu yang cepat.

Sementara itu, berdasarkan pengujian fungsionalitas aplikasi menggunakan metode Blackbox dapat disimpulkan bahwa 100% dari fitur aplikasi dapat berjalan dengan baik. Penelitian ini dapat dikembangkan lebih lanjut dengan menerapkan beberapa metode pembangkitan OTP selain PRNG.

DAFTAR PUSTAKA

[1] C. M. Annur, "Survei APJII: Penetrasi Pengguna Internet di Indonesia Capai 64,8%," *Katadata.co.id*, 2019. [Daring]. Tersedia pada: https://katadata.co.id/berita/2019/05/16/survei-apjii-penetrasi-pengguna-internet-di-indonesia-capai-648.

[2] N. A. Rozama, A. L. Kusumatrisna, Z. Ilmiyah, T. Sutarsih, G. Siswayu, dan A. Syakilah, *Statistik E-Commerce 2019*. Jakarta: Badan Pusat Statistik, 2019.

[3] WikipediaID, "M-Dagang," *Wikipedia.org*, 2020. [Daring]. Tersedia pada: https://id.wikipedia.org/wiki/M-dagang. [Diakses: 20-Jun-2020].

[4] A. M. R. Wajong dan C. R. Putri, "Keamanan dalam Electronic Commerce," *ComTech*, vol. 1, no. 2, hal. 867–874, 2010.

[5] C. Hanifurohman dan D. D. Hutagalung, "Analisa Keamanan Aplikasi Mobile E-Commerce Berbasis Android Menggunakan Mobile Security Framework," in *Seminar Nasional Enhancing Innovations for Sustainable Development*, 2020.

[6] RiskBased Security, "2020 Q1 Report Data Breach QuickView," 2020.

[7] K. K. Kumbhare dan K. V. Warkar, "A Review on Noisy Password, Voiceprint Biometric and One-Time-Password," in *International Conference on Information Security & Privacy*, 2016, vol. 78, hal. 382–386.

[8] S. Ma *et al.*, "An Empirical Study of SMS One-Time Password Authentication in Android Apps," in *ACSAC '19: Proceedings of the 35th Annual Computer Security Applications Conference*, 2019, hal. 339–354.

[9] H. A. Chandra, Y. I. Wijaya, dan H. Budiman, "Algoritma One Time Password pada Sistem Informasi Penerimaan Siswa Baru Online SMP H.A. Johansyah.A Banjarmasin," *Technologia*, vol. 10, no. 4, hal. 207–211, 2019.

[10] D. V. S. Y. Sakti, N. Agani, dan M. Hardjianto, "Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android," *J. BIT*, vol. 13, no. 1, hal. 1–10, 2016.

[11] G. H. Editya dan S. Mulyati, "Aplikasi Mobile One Time Password Menggunakan Algoritma MD5 dan SHA1 untuk Meningkatkan Keamanan Website," *SKANIKA*, vol. 1, no. 2, hal. 618–623, 2018.

[12] A. Hangga dan E. Prabowo, "Modifikasi Linear Congruential Generator untuk Sistem Pengacakan Soal pada Computer Based Test (CBT)," *J. Tek. Elektro*, vol. 8, no. 2, hal. 47–49, 2016.

[13] S. Gharge, H. Brijwani, M. Pugrani, G. Sukhwani, dan D. Udherani, "Percon8 Algorithm for Random Number Generation," *Int. J. Eng. Res. Appl.*, vol. 4, no. 5, hal. 54–60, 2014.

[14] A. Solichin, M. A. Putra, dan K. Diniari, "RESTful Web Service Optimization with Compression and Encryption Algorithm," *2018 Int. Semin. Appl. Technol. Inf. Commun.*, hal. 333–337, 2018.