AINET Jurnal Informatika

e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653

DESAIN DAN IMPLEMENTASI TIME BASED ONE TIME PASSWORD UNTUK MENINGKATKAN KEAMANAN OTENTIKASI PADA WEBSITE TOP UP GAMING

Muhyiddin A. M. Hayat*[1], Reski Abbas[2], Rizki Yusliana Bakti[3]
[1,2,3]Informatika, Teknik, Universitas Muhammadiyah Makassar
e-mail[1]: muhyiddin@unismuh.ac.id

Abstract

This study aims to determine the working system of website login security using Time Based One Time Password (TOTP) properly. Second, so that in carrying out login activities on the Web, users are protected from attacks that can harm Personal Information. The research was conducted by creating a game voucher top up website and then an authentication system was applied, namely TOTP. From the initial stages of the application, namely entering the email and password in accordance with the database on the website page. Then the website will generate a generated code which will be used as a TOTP code. Then, the verification code is sent to email and WhatsApp. Then the user enters the verification code. The results of this study indicate that other users cannot enter or login if they do not have a verification code that is automatically generated by the system and sent to email and WhatsApp.

Keywords*: Login; Password; authentication; TOTP; website.*

Abstrak

Penelitian ini bertujuan untuk Mengetahui sistem kerja dari pengamanan *login Website* menggunakan *Time Based One Time Password* (TOTP) dengan baik. Kedua, Agar dalam melakukan aktivitas *Login* pada *Web, user* terhindar dari serangan-serangan yang dapat membahayakan Informasi Pribadi. Penelitian dilakukan dengan membuat sebuah website top up voucher game kemudian diterapkan sistem autentikasi yaitu TOTP. Dari tahapan awal aplikasi yaitu memasukan *email* dan *password* yang sesuai dengan database pada halaman *website*. Lalu pada *website* tersebut akan menghasilkan kode generate yang akan digunakan sebagai kode TOTP. Kemudian, kode verifikasi dikirimkan ke *email* dan *WhatsApp*. Lalu *user* memasukan kode verifikasi. Hasil dari penelitian ini menunjukkan bahwa Pengguna lain tidak dapat masuk atau *login* apabila tidak memiliki kode verifikasi yang dibuat otomatis oleh system dan dikirimkan ke email dan *WhatsApp*

Kata Kunci : *Login*; *Password*; autentikasi; *TOTP*; *website*

1. Pendahuluan

Jaringan komputer yang saling berhubungan membentuk internet. Akibatnya, salah satu faktor utama yang perlu dipertimbangkan dengan keberadaan sistem jaringan internet adalah keamanannya, karena data atau informasi menjadi sangat rentan terhadap serangan dari pihak yang tidak berwenang ketika ada banyak orang yang terhubung ke jaringan [1].

Peretas menggunakan berbagai teknik untuk menemukan *username* dan *password* dari sebuah akun (*account)*. *Sniffing* adalah salah satu metode di mana peretas dapat mempelajari informasi akun seseorang. *Sniffing* adalah bentuk *cybercrime* dimana pelaku mengambil *username* dan *password* orang lain, baik secara sadar maupun tidak sadar. Pelaku kemudian dapat memakai akun korban untuk merusak atau menghapus data milik korban [2].

Sistem informasi berbasis web dibangun di atas jaringan komputer yang saling terhubung. Hal ini memungkinkan siapa saja dengan mudah mengakses semua data dan informasi. Tidak hanya oleh mereka yang berkepentingan, tetapi juga oleh mereka yang ingin mencuri data dan informasi dari sistem (*hacker*). Akibatnya, sistem harus dapat menentukan apakah individu yang akan memanfaatkannya merupakan pihak yang berkepentingan atau tidak. Pengguna harus mengidentifikasi dirinya ke sistem, yang kemudian harus memeriksa apakah identifikasi itu asli atau tidak.

One Time Password (OTP) adalah teknik keamanan yang melibatkan perubahan *password* secara teratur. OTP adalah jenis otentikasi dimana *password* hanya digunakan sekali. Secara umum, OTP digunakan untuk memenuhi persyaratan proses otentikasi *server* dan *user* [3].

Algoritma *Time-Based One Time Password (TOTP)* adalah salah satu algoritma yang memiliki kemampuan untuk menghasilkan *password* sekali pemakaian. Algoritma TOTP menghasilkan *password* yang memiliki masa berlaku terbatas dan selalu diperbarui setelah jangka waktu tertentu. *Secret key* digabungkan dengan *current time* dalam teknik TOTP, yang kemudian di-hash menggunakan algoritma enkripsi SHA256 [4].

2. Metode Penelitian

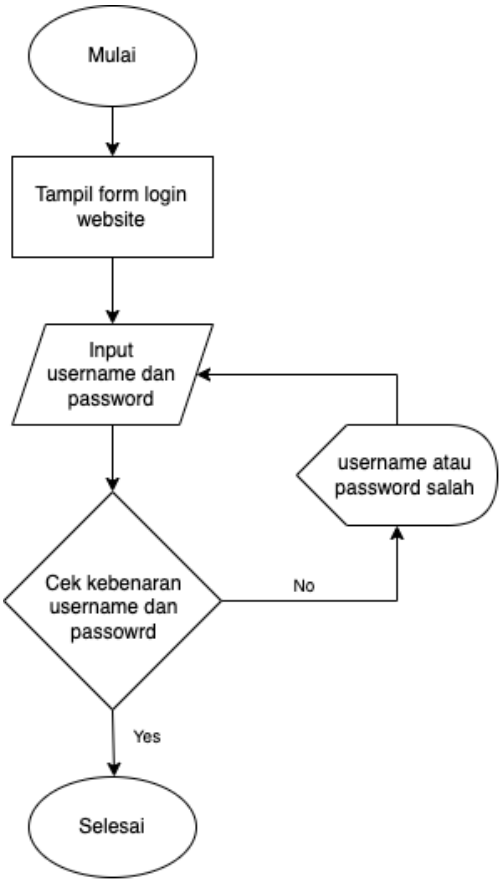
Ada dua jenis *One-Time Password*, yaitu HOTP (HMAC *based* OTP) dan TOTP (*Time-based* OTP). Kata sandi sekali pakai, juga dikenal sebagai OTP, biasanya digunakan untuk transaksi *online* atau pendaftaran akun. Kode OTP terdiri dari kombinasi nomor unik dan rahasia yang dihasilkan secara acak. Kode OTP ditujukan untuk keamanan, dan OTP dianggap lebih aman karena *password* terus berubah [6].

Secure Hash Algorithm (SHA), adalah fungsi hash satu arah yang dibuat oleh NIST dan umumnya digunakan bersama dengan DSS atau disebut *Digital Signature Standard*. SHA juga dapat didasarkan pada MD4 yang dibuat oleh seseorang bernama Ronald L. Rivest dari MIT. Keamanan pada SHA biasanya terletak pada desain SHA yang dibuat sedemikian rupa sehingga jika secara komputasi tidak mungkin menemukan pesan yang sesuai dengan *message digest* yang diberikan [7].

2.1. Perancangan Sistem

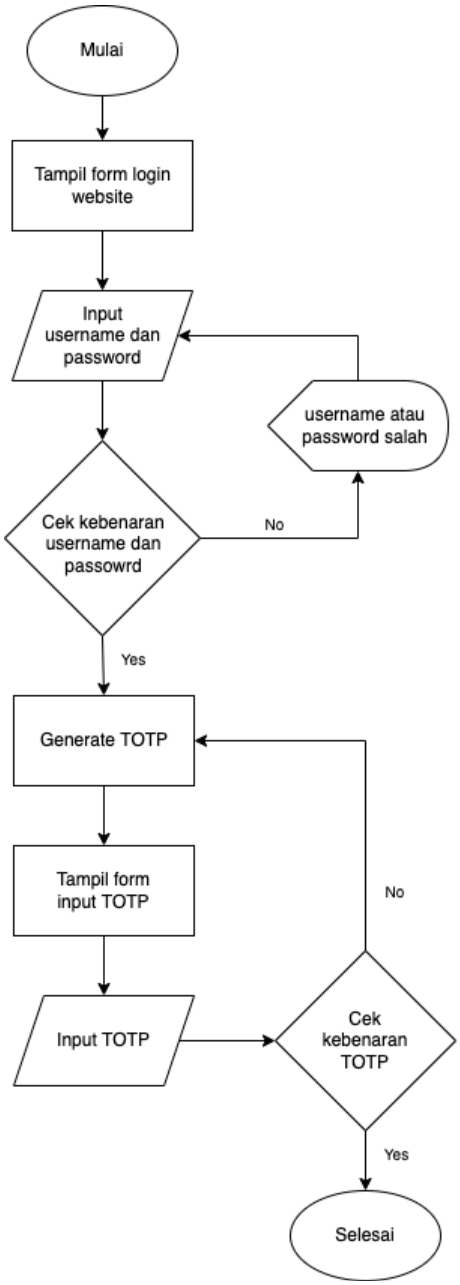
Perancangan adalah suatu proses untuk membuat dan mendesain sistem yang baru. Berdasarkan pengertian diatas dapat disimpulkan bahwa perancangan sistem adalah sebuah proses setelah analisis dari siklus pengembangan sistem untuk merancang suatu system [5]

Berikut ini merupakan rancangan *flowchart* dan algoritma pemrograman. Terdiri dari Halaman *Login* dan Halaman Verifikasi OTP yang merupakan halaman inti dari program ini. Pada Halaman Login terdapat inputan *username* dan *password*. Sedangkan pada Halaman Verifikasi OTP, terdapat inputan kode OTP dan tombol kirim ulang. Berikut *flowchart* dan algoritmanya :



Gambar 1. Flowchart login website sebelum penerapan TOTP

Proses dari login website sebelum penerapan TOTP, Tampil *form login*, kemuadian *user* menginput *username dan password*, lalu system akan memeriksa kebenaran *username* dan *password* tersebut Jika *username* dan *password* salah, maka ditampilkan pesan kesalahan kemudian *input* Kembali *username* dan *password*, jika *username* dan *password* benar, maka proses selesai

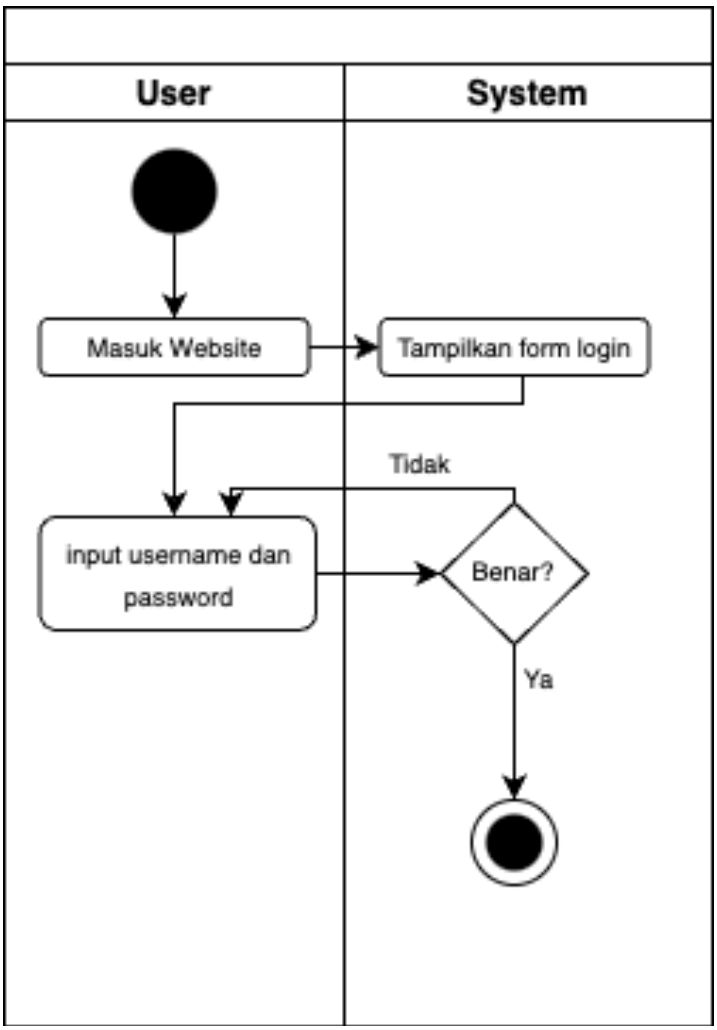


Gambar 2. Flowchart login website penerapan TOTP

Algoritma proses login website dengan TOTP, Tampil *form login*, kemuadian *user* menginput *username dan password*, Jika *username* dan *password* salah, maka ditampilkan pesan kesalahan kemudian *input* Kembali *username* dan *password*, jika *username* dan *password* benar, kemudian system akan menggenerate TOTP, lalu user akan menginput TOTP,setelah itu proses cek TOTP, jika TOTP benar maka proses selesai, apabila salah maka TOTP degenerate Kembali.

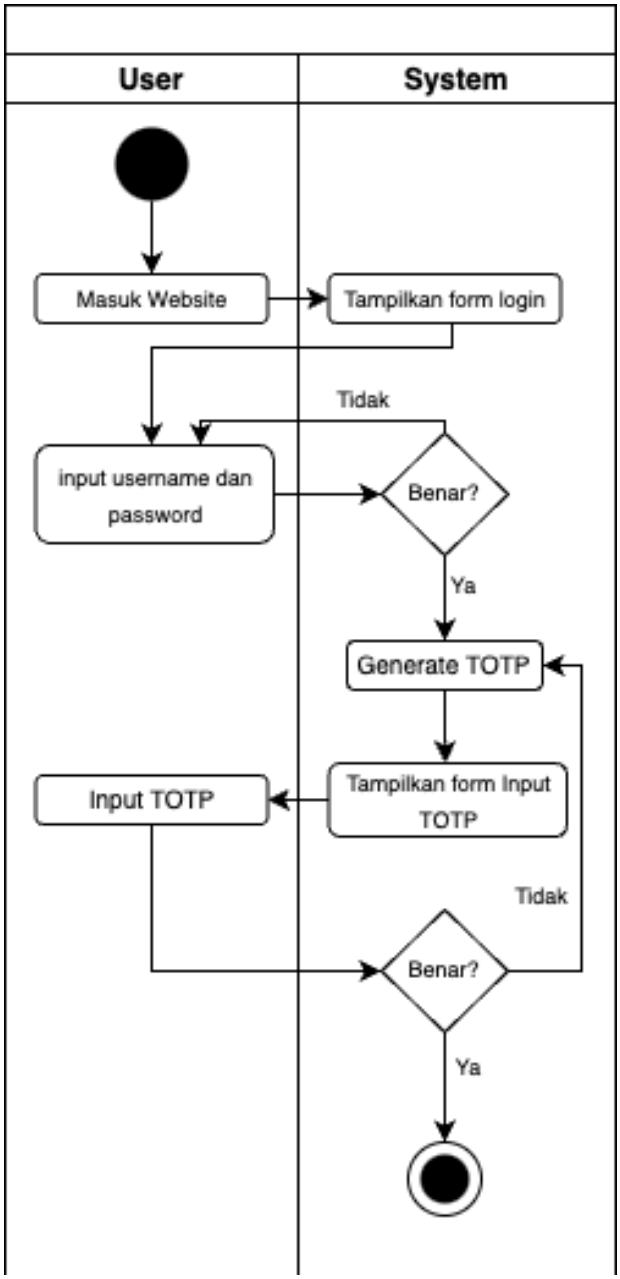
e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653

Activity Diagram merupakan rancangan aliran aktivitas atau aliran kerja dalam sebuah sistem yang akan dijalankan. *Activity Diagram* juga digunakan untuk mendefinisikan atau mengelompokan aluran tampilan dari sistem tersebut. *Activity Diagram* memiliki komponen dengan bentuk tertentu yang dihubungkan dengan tanda panah.



Gambar 3. Activity Diagram proses login

Proses *activity diagram*, *user* masuk ke *website*, kemudian *system* akan menampilkan *form login*, lalu *user* menginput *username* dan *password*, *system* akan cek kebenaran *username* dan *password* tersebut, jika salah maka kembali menginput *username* dan *password*, jika benar maka proses selesai.



Gambar 4. Activity diagram proses login dengan TOTP

Proses *activity diagram,* user masuk ke website kemudian system akan menampilkan form login, lalu user menginput username dan password, system akan memvalidasi jika salaha maka username dan password diinput kembali, jika benar maka proses generate TOTP dijalankan oleh system lalu menampilkan form input TOTP, kemudian user menginput TOTP yang telah didapatkan melalui email/WhatsApp, setelah itu system kembali memvalidasi TOTP, jika salah maka TOTP degenerate kembali, apabila benar maka proses selesai.

2.2. Teknik Pengujian Sistem

Pengujian sistem adalah pengujian berdasar spesifikasi / kebutuhan perangkat lunak. Pengujian ini biasanya dilakukan berdasarkan spesifikasi yang dianalisa secara informal dan manual.

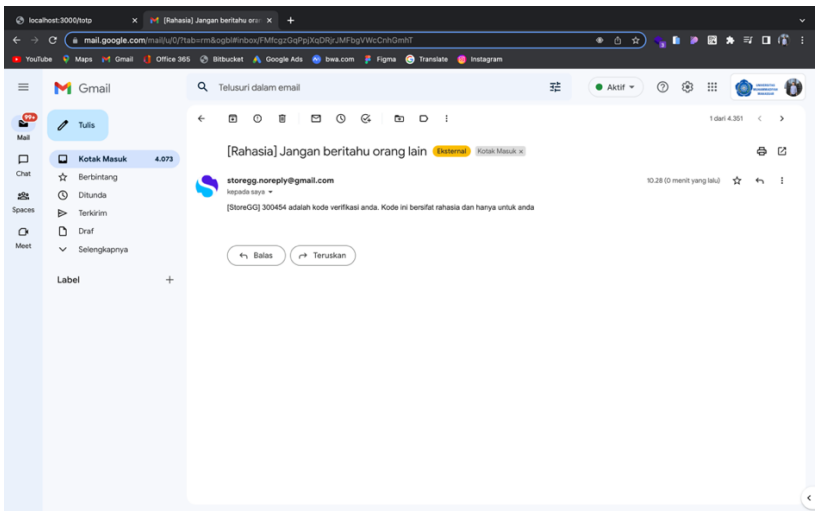
Black Box Testing (Pengujian kotak hitam) bertujuan untuk menunjukkan bagaimana fungsi perangkat lunak bekerja, apakah data *input* dan *output* telah berjalan sebagaimana dimaksud dan apakah informasi yang disimpan secara *external* selalu dijaga kemutahirannya.

AINET Jurnal Informatika
e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653

Pengujian sistem yang akan dilakukan pada penelitian ini terdapat beberapa poin antara lain: Pengujian enkripsi data user**,** Yaitu menguji keberhasilan generate TOTP setelah dilakukan enkripsi data user dengan algoritma SHA-256. Pengujian TOTP**,** Dilakukan dengan menginput beberapa kode TOTP dengan waktu berbeda, serta menginput kode TOTP yang salah, bertujuan untuk menguji keberhasilan *login* menggunakan kode TOTP. Pengujian *User***,** Membuktikan kebenaran user yang login setelah melalui tahap verifikasi TOTP.

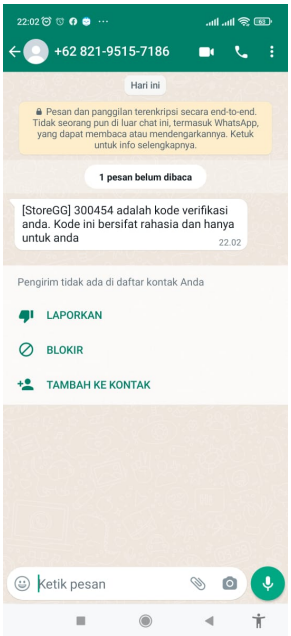
3. Hasil dan diskusi

Ini adalah tampilan pesan pada email pengguna yang menerima pesan kode verifikasi, mereka memiliki waktu terbatas untuk memasukkan kode pada halaman verifikasi TOTP.



Gambar 5. Tampilan pesan kode TOTP

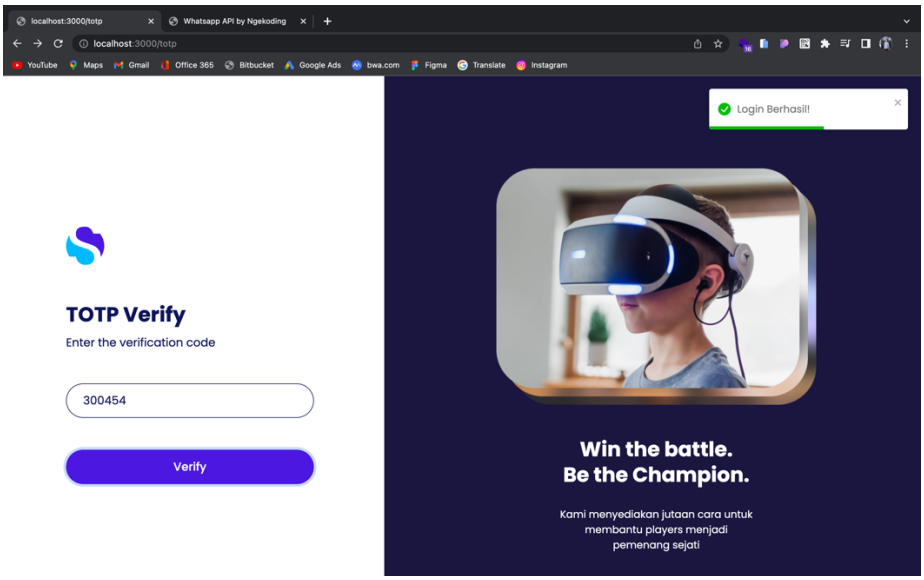
Selain dikirim melalui email, pesan yang berisi kode TOTP juga dikirimkan ke nomor whatsapp pengguna.



Gambar 6. Kode verifikasi TOTP yang dikirim ke WhatsApp

Setelah *user* berhasil menginput kode verifikasi dengan benar, maka aplikasi ini selanjutnya akan menampilkan halaman *Home*.

AINET Jurnal Informatika
e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653



Gambar 7. Kode verifikasi TOTP benar dan berhasil login

Tabel berikut adalah hasil uji coba yang telah dilakukan beberapa kali untuk login ke dalam aplikasi.

Table 1. Uji Coba TOTP

No.	Waktu Login	Kode yang diterima	Waktu input kode	Kode yang diinput	Hasil
1.	10:22	989909	10:24	989909	Gagal
2.	10:26	592817	10:26	59281	Gagal
3.	10:28	300454	10:28	300454	Berhasil
4.	13:25	801228	13:26	801228	Berhasil
5.	13:35	324820	13:35	324820	Berhasil
6.	13:39	971561	13:37	971662	Gagal
7.	13:51	440250	13:51	440150	Gagal
8.	14:01	345776	14:01	345776	Berhasil
9.	14:03	739807	14:06	739807	Gagal
10.	14:11	060754	14:11	479894	Gagal
11.	14:35	178106	14:35	178106	Berhasil
12.	18:25	078742	18:25	078742	Berhasil
13.	19:42	569050	19.44	669050	Gagal
14.	20.35	532231	20.35	532231	Berhasil
15.	20.40	479894	20:41	479894	Berhasil

Berdasarkan TOTP yang diinputkan menghasilkan kesimpulan sebagai berikut.. Keterlambatan memasukkan kode verifikasi, *User* harus memasukkan kode verifikasi baru karena sudah lebih dari satu menit, Kode verifikasi yang dimasukkan salah karena tidak sesuai dengan kode yang diterima, Berhasil karena memasukan kode verifikasi sebelum 1 menit dan menginput kode dengan benar.

Dalam pembuatan website StoreGG dengan keamanan data *Time Based One Time Password* menggunakan Algoritma SHA-256 memiliki beberapa kelebihan dan kekurangan pada aplikasi, Kelebihan Aplikasi adalah Bersifat online dan dapat diakses dimana saja dan bisa melalui handphone, Berbasis web sehingga mudah untuk diakses, Pengguna lain tidak dapat masuk apabila tidak memiliki kode verifikasi yang dikirim ke *email*/*whatsapp*. Kekurangan Aplikasi adalah Batasan waktu verifikasi hanya satu menit, jadi jika server atau jaringan ponsel sedang down dan ada pesan masuk yang lebih lama dari itu, maka verifikasi akan gagal. Setelah itu, *User* harus memasukkan kode verifikasi baru

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan mengenai proses TOTP dalam masalah keamanan login pada website StoreGG tersebut, antara lain : Kode *One Time Password* bisa dikirim dari server ke nomor *whatsapp* dan email pengguna, Jika *password user* diketahui orang lain, penggunaan kode TOTP dapat melindungi akun, Jika Anda memasukkan kode verifikasi lebih dari 1 menit setelah diterima, kode tersebut tidak berlaku lagi, dan Anda harus memasukkan kode baru.

Referensi

[1] R. D. A. Ciputra, "IMPLEMENTASI ONE TIME PASSWORD MOBILE TOKEN DENGAN ALGORITMA SECURE HASH ALGORITHM 1 (SHA1) PADA LOGIN WEBSITE PUSDASKRIMTI KEJAKSAAN AGUNG REPUBLIK INDONESIA," pp. 1-54, 2017.

[2] M. Prawiro, "Cyber Crime: Pengertian, Jenis, dan Metode Kejahatan Cybercrime," 5 September 2018. [Online]. Available: https://www.maxmanroe.com/vid/teknologi/pengertian-cyber-crime.html#:~:text=Sniffing%20adalah%20bentuk%20cyber%20crime,merusak%2F%20menghapus%20data%20milik%20korban.

[3] G. Y. Utama, "IMPLEMENTASI ALGORITMA TOTP SHA-3 UNTUK PENGELOLAAN PASSWORD WIFI PADA MEDIA TEMPAT SAMPAH," pp. 1-15, 2020.

[4] U. Ungkawa, I. A. Dewi and K. R. Putra, "IMPLEMENTASI ALGORITMA TIME-BASED ONE TIME PASSWORD DALAM OTENTIKASI TOKEN INTERNET BANKING," pp. 2-11, 2017.

[5] S. Ayu Lestari, "PERANCANGAN SISTEM INFORMASI REGISTRASI TEMPAT USAHA UNTUK MENDUKUNG PEMETAAN WILAYAH PADA KANTOR KECAMATAN KOSAMBI KABUPATEN TANGERANG," *Widuri,* pp. 1-50, 2018.

[6] N. S. Hapsari, Y. Fatman and I. , "Implementasi Metode One Time Password pada Sistem Pemesanan Online," *JURNAL MEDIA INFORMATIKA BUDIDARMA,* vol. 4, pp. 930-939, 4 October 2020.

[7] A. T. Wicaksono and T. Fatimah, "SISTEM PENILAIAN ONLINE MENGGUNAKAN KEAMANAN ONE TIME PASSWORD DENGAN ALGORITMA SHA 512 BERBASIS WEB," vol. 1, pp. 938-942, 3 Juli 2018.