p-ISSN: 2460-173X
e-ISSN: 2598-5841

Sistem Pengamanan Dokumen dengan Algoritma *Time-Based One Time Password (TOTP)* pada *Two-Factor Authentation (2FA)*

Laila Qadriah*[1], Sayed Achmady[2], Husaini[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Jabal Ghafur
E-mail: *[1]laila_qadriah@unigha.ac.id, [2]sayedachmady@unigha.ac.id,
[3]husainizaki@unigha.ac.id

Abstrak

Keamanan dokumen menjadi perhatian utama pada era digital, karena hampir keseluruhan dokumen saat ini menggunakan sistem komputer yang dapat disimpan secara online. Keamananan data suatu dokumen merupakan komponen penting yang harus diperhatikan oleh semua pengguna untuk meminimalisir terjadinya penyalahgunaan akun. Implementasi keamanan dibutuhkan untuk menghindari ancaman seperti pembacaan data serta modifikasi data oleh pihak yang tidak berwewenang. Oleh karena itu dibutuhkan sistem pengamanan ekstra untuk menjaga keamanan dokumen. Penelitian ini bertujuan untuk merancang sistem pengamanan dokumen dari segi proses otentikasi yang mengalami perubahan pada proses login dengan menggunakan metode Two-factor authentication (2FA). Ada banyak cara untuk mengimplementasikan 2FA, salah satunya adalah dengan menggunakan algoritma Time Based One Time Password (TOTP) untuk menghasilkan kata sandi sekali pakai. Kata sandi ini memiliki masa berlaku yang terbatas dan selalu berubah setiap waktu. Penelitian ini diawali dengan implementasi algoritma TOTP untuk mendapatkan one-time password (OTP) yang dikirim ke email pengguna. Selanjutnya, proses pengamanan pada lapis kedua dilakukan dengan menggunakan metode 2FA melalui proses *scanning QR Code melalui aplikasi Google Authenticator dan diakhiri dengan proses upload dokumen. Penelitian ini menunjukkan bahwa sistem pengamanan dokumen dengan algoritma TOTP pada 2FA dapat meningkatkan keamanan data suatu dokumen.*

Kata Kunci *— Sistem, Keamanan Dokumen, Otentikasi, TOTP, 2FA*

Abstract

Document security is a major concern in the digital era because almost all documents today use computer systems that can be stored online. The security of document is the highest component that must be considered by all users to minimize account abuse. Security implementation is used to avoid of threats such as data reading and data modification by unauthorized parties. Therefore, an extra security system is needed to maintain document security. This research aims to design a document security system in terms of the authentication process that changes in the login process by using Two-factor authentication (2FA) method. There are many ways to implement 2FA, one of which is to use a Time Based One Time Password (TOTP) algorithm for creating one-time password. The generated password has a limited validity period and always changes within a certain period. This study begins the implementation of the TOTP algorithm to generate a one-time password (OTP) that will sent to the email. Furthermore, the second-layer security process is apply the 2FA method through the QR Code scanning process with the Google Authenticator application and upload of the document. This research shows that a document security system with the TOTP algorithm on 2FA enhance the data security of a document.

Keywords: *System, Document Security, Authentication, TOTP, 2FA*

Received: 7 November 2022
Accepted: 23 Juni 2023

1. PENDAHULUAN

Pengaman dokumen sangat dibutuhkan bagi semua kalangan instansi, seperti proses penyimpanan yang kredibel supaya dapat digunakan ketika diperlukan. Dalam instansi, saat ini pengaman dokumen berbentuk fisik, seperti kertas menjadi hal yang lumrah dan biasa, dimana hanya menggunakan pengamanan seadanya. Pada suatu waktu mungkin saja hilang karena bencana maupun hal-hal lainnya yang dapat merugikan pengguna [1]. Antisipasi ini perlu pembenahan untuk menjaga dokumen dengan baik, agar dapat diakses dan diperoleh suatu saat ketika diperlukan.

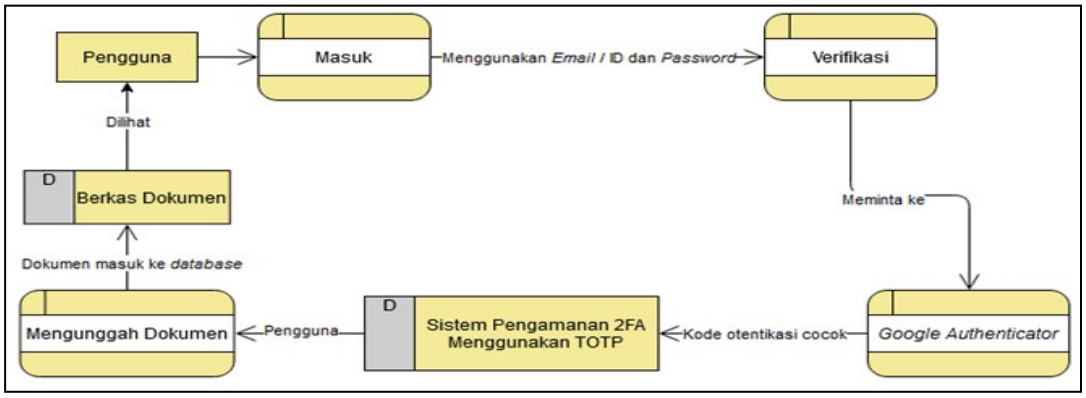
Sistem pengaman dokumen juga menjadi sebuah layanan menjanjikan, dengan banyaknya bantuan penjagaan dokumen berkredibilitas tinggi yang sangat lengkap saat ini, mulai dari pihak ketiga seperti brankas maupun internet [2]. Dahulu penggunaan pengaman dokumen bersifat tidak online yang berbentuk fisik, dimana mempunyai resiko besar akan kehilangan dokumen. Apalagi jika dokumen yang bersifat rahasia yang digunakan pada instansi pemerintahan maupun swasta. Hampir keseluruhan dokumen saat ini menggunakan sistem komputer, baik yang disimpan secara online maupun tidak online [3].

Banyak layanan pengaman dokumen yang dapat diperoleh di internet. Penggunaan sistem ini memerlukan satu sistem pengaman dokumen bersifat rahasia atau *classified*, yang mana hanya dapat digunakan oleh pihak yang mempunyai otoritas [4]. Proses otentikasi semacam identitas dan password dapat digunakan sebagai pengaman dokumen online. Salah satu metode keamanan yang diterapkan pada pengamanan dokumen online yaitu *Two-factor authentication (2FA)* adalah sebuah metode otentikasi elektronik yang menggunakan dua faktor yang bersifat independent dan hanya dapat digunakan setelah mendapatkan persetujuan pengguna komputer untuk memperoleh akses ke halaman situs web atau aplikasi secara sukses dengan menggunakan kata sandi yang hanya digunakan sekali pada saat melakukan akses sesi maupun transaksi [5]. Sistem *two factor authentication* merupakan kombinasi *username* dan *password* untuk meningkatkan keamanan dengan menghasilkan *password* dinamis *One Time Password*. Salah satu teknik untuk mendapatkan *One Time Password* adalah dengan menggunakan metode *Time-Based One-time password (TOTP).* Sebuah TOTP biasanya diperoleh dalam bentuk kode 6-digit sandi. Teknik yang digunakan TOTP dalam pengiriman kode sandi sangat unik dan rahasia yang diperoleh secara acak dan dianggap lebih aman karena perubahan kata sandi secara terus menerus atau bergantian setiap 30 detik melalui koneksi aplikasi otentikator dan teknik lainnya yang dapat mempermudah kinerja dan memperkuat keamanan. Pengiriman TOTP melalui otentikator adalah teknik baru dari pengembangan *One-time Password (OTP)* untuk meningkatkan keamanan, efisiensi dan efektivitas dalam memperoleh sandi [6].

2. METODE PENELITIAN

Metode yang digunakan dalam perancangan sistem pengamanan dokumen adalah *Two-factor authentication (2FA)* adalah metode otentikasi elektronik yang membutuhkan 2 faktor untuk melakukan otentikasi pengguna [7]. Sistem *Two-factor authentication* ini dapat dirancang dengan menggunakan kombinasi username dan password serta divalidasikan kepemilikannya dengan password dinamis *One-time password (OTP*). *One-time password* adalah kata sandi yang valid dan hanya bisa digunakan satu kali login pada komputer atau alat digital lainnya [8]. Salah satu metode untuk membangkitkan *One-time password* adalah algoritma *Time-Based One-time password (TOTP)*, algoritma ini memiliki kemampuan untuk menghasilkan password sekali pemakaian. Proses kerja sistem pengamanan dokumen menggunakan Algoritma *Time-Based One-time password (TOTP)* pada *Two-factor authentication (2FA)* Berbasis Web dapat dilihat pada gambar 1 dibawah ini :

p-ISSN: 2460-173X
e-ISSN: 2598-5841



Gambar 1. Proses Kerja Sistem Pengamanan Dokumen

Gambar 1 menjelaskan bahwa pengguna masuk ke dalam situs web dan melakukan otentikasi menggunakan ID dan password, jika ID dan password benar akan diarahkan ke dalam halaman verifikasi, namun jika salah di ID dan password, pengguna akan gagal dan sistem menganggapnya sebagai kesalahan. Pengguna yang benar dalam proses otentikasi masuk akan diarahkan ke halaman verifikasi yang meminta kode 6-digit dari Google Authenticator. Jika kode 6-digit benar, maka pengguna akan diizinkan masuk ke situs web untuk pengelolaan dokumen [9].

Tahapan pengujian sistem dilakukan dengan perolehan otentikasi masuk seperti pada umumnya. Namun yang membedakan dengan proses masuk lainnya adalah terdapat pada lapisan kedua, yaitu halaman tahap verifikasi akun. Ketika proses penginputan *id* dan kata sandi, akun wajib terdaftar ke dalam *database server* agar dapat diterima ke tahapan selanjutnya. Jika tidak, pengguna harus mendaftarkan diri agar memperoleh akun. Setiap akun memiliki perbedaan, mulai dari *id* akun dan kode google pada akun. Perbedaan ini, diverifikasi agar tidak ada bentrokan dan duplikat dengan akun lain. Kode google ini, dibedakan setiap akun untuk dapat memperoleh proses otentikasi melalui *Google Authenticator* [10]. Halaman verifikasi dari pendaftaran akun dapat diperoleh melalui proses *scanning QR Code*, dengan otomatis memperoleh kode google yang dihasilkan oleh *QR Code* itu.

Proses sudah tergolong unik bagi setiap pengguna, dengan memasukkan kode google ke dalam tahapan otentikasi, maka pengguna akan diarahkan ke halaman utama, guna dapat melakukan proses manajemen dokumen [11].

Kelemahan pada penerapan metode single factor authentication dapat diatasi dengan metode two factor authentication. Metode Two factor authentication merupakan pengamanan lapis kedua yang harus dilewati setelah memasukan username dan password. Salah satu contoh two factor authentication adalah timed based one-time password (TOTP) dengan kode pembangkitan OTP (one time password) berdasarkan waktu dan secret key.

Kelebihan penerapan TOTP adalah tidak mengandalkan koneksi ke server pada saat pembangkitan kode OTP nya, sehingga tidak membutuhan waktu yang lama dalam pembangkitan kode OTP dan tidak dibutuhkan adanya proses penyimpanan kode OTP ke dalam sebuah database.

3. HASIL DAN PEMBAHASAN

Halaman masuk ini digunakan sebagai media dari proses otentikasi masuk ke dalam *website*. Di mana, menggunakan nama pengguna atau *e-mail* dan kata sandi. Dipastikan akun sudah didaftarkan ke dalam *server* sebelumnya. Sebaliknya, pengguna harus mendaftarkan akun terlebih dahulu.

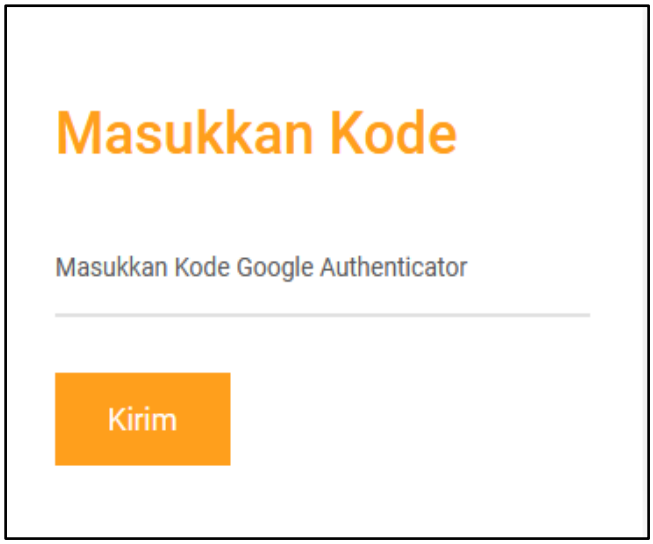
Bagi pengguna yang telah mendaftarkan akun, akan diarahkan langsung ke halaman verifikasi, yaitu halaman tempat di mana kode google akan diminta oleh sistem, dengan

p-ISSN: 2460-173X
e-ISSN: 2598-5841

pencocokan pada aplikasi *Google Authenticator*, yang selanjutnya dapat mengakses dokumen dalam manajemen. Pengguna akan dapat dihadapkan langsung dengan *Interface*/antar muka program dalam proses otentikasi masuk ke sebuah website serta arahan dan informasi *login* dengan kriteria yang diberikan. Berikut ini Gambar 2 dari halaman proses otentikasi masuk ke dalam sistem.

Gambar 2. Halaman Masuk

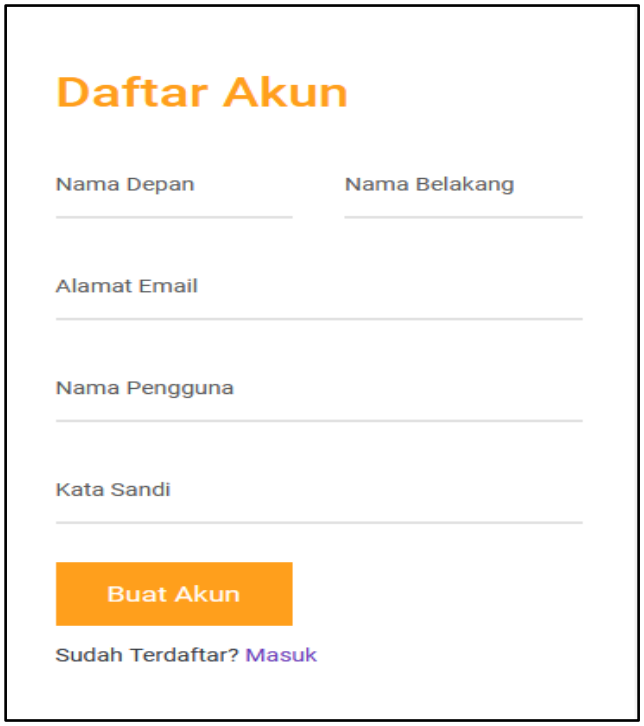
Berikut gambar 3 dari halaman verifikasi yang diarahkan ke pengguna saat telah masuk menggunakan informasi krisensial *login*:



Gambar 3. Halaman Verifikasi Akun

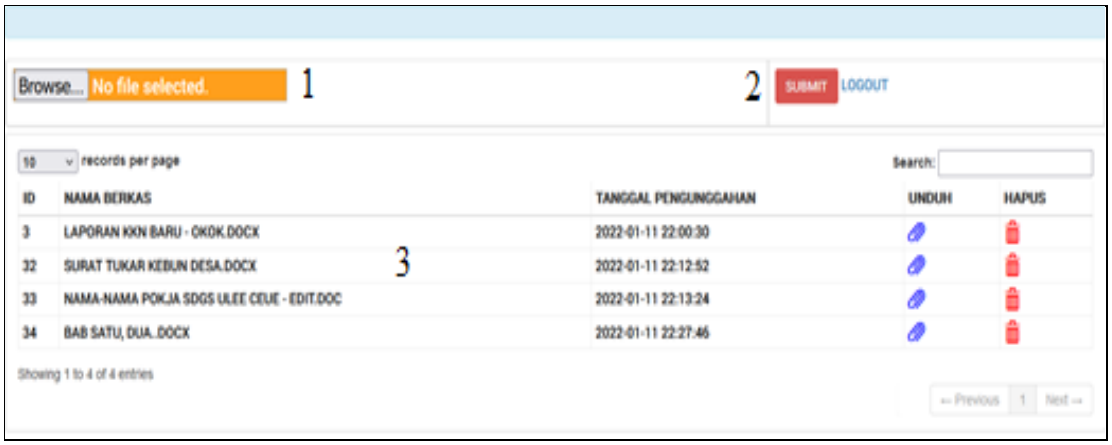
Sebaliknya, jika pengguna belum memperoleh akun. Maka dengan mudah dapat mendaftarkan akun menggunakan halaman yang telah disediakan dengan memasukkan beberapa informasi yang dapat digunakan untuk proses *login* ke dalam aplikasi.

p-ISSN: 2460-173X
e-ISSN: 2598-5841



Gambar 4. Halaman Pendaftaran

Halaman pendaftaran pada Gambar 4 mencakup pendataan dari pengguna-pengguna baru (*register*), dimana pengguna ini akan menggunakan aplikasi ini dan mengelola beserta dengan objek yang mereka unggah selanjutnya. pada halaman manajemen dokumen yang dapat di lihat pada Gambar 5.



Gambar 5. Manajemen Dokumen

Pada halaman manajemen dokumen terdapat beberapa opsi yang dapat digunakan oleh pengguna dalam proses eksekusi pengunggahan dokumen. Diantaranya:

1. *Browse*, digunakan untuk memilih berkas dokumen yang dikehendaki pengguna untuk diunggah.
2. *Submit*¸ setelah pengguna memilih dokumen yang dikehendaki, pengguna dapat menekan tombol ini untuk mengunggah.
3. Daftar dari dokumen yang telah diunggah oleh pengguna, diperlihatkan di sini.

Dalam tahapan percobaan sistem, terdapat hambatan untuk merancang sistem agar dapat berfungsi dengan target yang dibutuhkan. Berikut di antaranya proses-proses percobaan yang telah dilakukan dijelaskan pada Tabel 1.

Tabel 1. Uji Coba Sistem

No	Percobaan	Keterangan	
		Google Authenticator	*Website*
1	Percobaan 1	Kode tidak muncul	Tidak menanggapi dan tidak masuk
2	Percobaan 2	Kode muncul	Tidak menanggapi dan tidak masuk
3	Percobaan 3	Kode muncul	Menanggapi dan tidak masuk
4	Percobaan 4	Kode muncul	Menanggapi dan masuk

Dalam tahapan pengujian sistem, terdapat beberapa langkah yang terkesan *familiar* dengan perolehan otentikasi masuk seperti pada umumnya. Namun, yang membedakan dengan proses masuk lainnya, adalah terdapat pada lapisan kedua, yaitu halaman tahap verifikasi akun. Ketika proses memasukkan *id* dan kata sandi, akun wajib terdaftar ke dalam *database server* yang umumnya dapat diterima ke tahapan selanjutnya. Jika tidak, pengguna baru dapat mendaftarkan diri agar memperoleh akun. Setiap akun memiliki perbedaan, mulai dari *id* akun dan kode google pada setiap akun.

Id akun dan kode google dari setiap akun dapat memperoleh proses otentikasi melalui *Google Authenticator* secara berbeda. Permintaan PIN yang terdapat pada halaman verifikasi setelah menyelesaikan formulir pendaftaran akun, diperoleh melalui proses *scanning QR Code* melalui aplikasi *Google Authentication*. Setelahnya, *Google Authentication* akan memberikan kode google ke dalam *smartphone* pengguna.

4. KESIMPULAN

Penggunaan metode TOTP sebagai algoritma 2FA dapat meningkatkan keamanan suatu sistem atau layanan dengan memberikan lapisan keamanan tambahan yang dapat mencegah serangan phishing di mana penyerang mencoba mencuri informasi login pengguna dengan membuat halaman palsu yang mirip dengan tampilan halaman autentikasi asli. Karena kode waktu terbatas yang dihasilkan oleh aplikasi autentikasi hanya berlaku sesaat dan tidak dapat digunakan kembali, serangan phishing menjadi lebih sulit dilakukan. Kode yang bersifat dinamis dan berubah setiap beberapa detik, sehingga pengguna harus memasukkan kode dengan cepat dan akurat agar autentikasi berhasil. Kesalahan pengguna dalam memasukkan kode dapat menyebabkan penolakan akses. Penerapan algoritma 2FA dengan metode TOTP merupakan pilihan yang baik untuk meningkatkan keamanan sistem atau layanan. Meskipun ada potensi kesalahan manusia, manfaat keamanan yang diperoleh dari penggunaan metode ini jauh lebih besar dari pada kerugian potensial.

DAFTAR PUSTAKA

[1] Eldas PR, Dhanar IS. *Sistem Informasi Manajemen Di Era Revolusi Industri 4.0*. Vol. 1. Zahira Media Publisher. 2021.
[2] Angga AP, Desi N. Rancangan Aplikasi Pengamanan Data dengan Algoritma Advance Encyption Standar (AES). *Jurnal Teknik Informatika*. 2018; 11(2): 177.
[3] Ibnu DI, N. Sukamto, Evfi M. Implementasi TOTP (Time-Based One-Time Password) Untuk Meningkatkan Keamanan Transaksi E-Commerce. *Jurnal Prosiding Konferensi Nasional Sistem dan Informasi*. 2016.

[4] Tina K. Efektivitas Komunikasi Organisasi Melalui Penerapan Sistem Administrasi Persuratan Terintegrasi di Universitas Lampung. *INTER KOMUNIKA: Jurnal Komunikasi*. 2020; 5 (1): 31-42.
[5] Herri S, Dewi S, Boy GR. Implementasi Time-Based One Time Password (TOTP) Pada Sistem Two Factor Authentication (2FA). *Jurnal Teknologi [internet]*. 2020; 13(1):63-16 Januari 2021. Availabel from : https://doi.org/10.3415/jurtek.v13i1.2967
[6] Nani SH, Yenni F, Isbandi. Implementasi Metode One Time Password Pada Sistem Pemesanan Online. *Jurnal Media Informatika Budidarma*. 2020; 4 (4): 930 - 939. Available From http://dx.doi.org/10.30865/mib.v4i4.2195
[7] Muhammad S, Febriawan, D. *Modul Pembelajaran E-Commerce*: Media Sains Indonesia. 2021.
[8] Alfat YF, Muhammad H. Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password. Sainstech: *Jurnal Penelitian dan Pengkajian Sains dan Teknologi*. 2020; 3 (1).
[9] Jeperson H. *Konsep sistem informasi*. Deepublish .2015.
[10] Sunderi Pranata, Tri NH, Yamaki H. Analisis dan Implementasi Protokol Otentikasi FIDO U2F. Ultima Computing: *Jurnal Sistem Komputer* 9.1 2017: 30-35.
[11] Adi P, Muhammad A, Janner H, Ridha SS. *Konsep Dasar E-Commerce*. Yayasan Kita Menulis. 2021.

Biodata Penulis

Laila Qadriah, Lahir di Mesjid Runtoh, 15 Juli 1985, Menyelesaikan S1 Matematika Fakultas MIPA, Universitas Syiah Kuala pada tahun 2008 dan menyelesaikan S2 Master Of Applied Mathematics, Dong Hwa University, Taiwan pada tahun 2013. Penulis adalah salah satu Dosen Tetap di Fakultas Teknik Prodi Teknik Informatika, Universitas Jabal Ghafur, Sigli Aceh.

Sayed Achmady, Lahir di Pidie, 6 Oktober 1985, Menyelesaikan S1 Teknik Informatika Fakultas Teknik Universitas Jabal Ghafur pada tahun 2008 dan Menyelesaikan S2 Teknik Informatika Universitas Sumatera Utara pada tahun 2015. Penulis juga salah satu Dosen Tetap di Fakultas Teknik Prodi Teknik Informatika, Universitas Jabal Ghafur, Sigli Aceh.

Husaini, Lahir di Cebrek, 31 Desember 1971, Menyelesaikan S1 Teknik Informatika Fakultas Teknik Universitas Jabal Ghafur pada tahun 2001 dan Menyelesaikan S2 Ilmu Komputer Universitas Gadjah Mada pada tahun 2008. Penulis merupakan salah satu Dosen Tetap di Fakultas Teknik Prodi Teknik Informatika, Universitas Jabal Ghafur, Sigli Aceh.