Perancangan Sistem Pengamanan Dokumen Menggunakan Algoritma Time-Based One Time Password (TOTP) Pada Two-Factor Authentation (2FA) Berbasis Web

Design of a Document Security System Using the Time-Based One-Time Password (TOTP) Algorithm in Web-Based Two-Factor Authentication (2FA)

Faridzoel Mossal[1*], Sayed Achmady[1], Zikrul Khalid[1]

[1]Universitas Jabal Ghafur, Glee Gapui, 24163, Indonesia
*corresponding author: faridzoelmossal58@gmail.com

Tanggal Submisi: 15 Agustus 2022, Tanggal Penerimaan: 29 Agustus 2022

Abstrak

Pengaman dokumen sangat dibutuhkan bagi semua kalangan instansi untuk memperoleh penyimpanan kredibel. Pengamanan komputerisasi menjadi terobosan andalan. Menggunakan tahapan pengamanan lapisan ganda pada website dengan kombinasi TOTP dan 2FA dalam proses masuk ke dalam sistem, menjadikan pengamanan dokumen lebih terjaga. Pemahaman dalam merancang sistem masuk berlapis ganda, memerlukan tahapan dalam mempelajari materi tentang sistem TOTP dan 2FA. Termasuk dari tahapan implementasi sistem. Kemudian masuk ke tahapan evaluasi atau pengujian kinerja sistem baru dan kegiatan pemeliharaan. Dengan begitu, menghasilkan luaran yang mengedepankan keamanan pengguna dalam mengamankan dokumen dengan proses otentikasi ke dalam website menggunakan metode dua lapisan TOTP dan 2FA. Manfaat yang diperoleh dari perancangan sistem ini adalah ditujukan kepada instansi, dengan penyimpanan dokumen elektronik skala besar, dengan simpanan dokumen bersifat rahasia. Manfaat juga ditujukan kepada kalangan publik, agar dapat mengamankan dokumen penting dengan baik dan terjaga.

Kata Kunci: TOTP, 2FA, sistem, dokumen, pengamanan

Abstract

Document security is required for all agency circles to achieve trustworthy storage. Security through computerization was a significant breakthrough. Using double-layer security on the website with the TOTP combination 2FA in the process of entering the system, documents are safer. Understanding how to design a double-plated system necessitates a stage of learning TOTP and 2FA material. This includes the steps of system implementation. Then comes the evaluation stage, which includes evaluating new performance systems and maintenance tasks. As a result, creating an outpost that advances user security in securing documents with authentication procedure into the website utilizing two-layer of TOTP and 2FA. The advantage of this system's design is targeted to the agency, with a large-scale electronic document, with a stockpile of confidential papers. The advantages are also directed to the general public, in order to keep vital papers safe and secure.

Keywords: TOTP, 2FA, systems, documents, security

PENDAHULUAN

Prioritas dalam menjaga privasi di dalam internet perlu dijaga baik, terutama kepada pengaman dokumen sangat dibutuhkan bagi semua kalangan instansi, seperti proses penyimpanan kredibel untuk digunakan ketika diperlukan. Dalam instansi, saat ini pengaman dokumen berbentuk fisik, seperti kertas menjadi hal yang lumrah dan biasa, yang mana hanya menggunakan pengamanan seadanya. Di mana pada suatu waktu mungkin saja pada dapat berimbas kehilangan karena bencana maupun hal-hal lainnya yang dapat merugikan pengguna. Antisipasi ini perlu pembenahan untuk menjaga dokumen dengan baik, agar dapat diakses dan diperoleh suatu saat diperlukan.

Menggunakan layanan sistem pengamanan dokumen berkomputerisasi menjadikan media penyimpanan yang dapat diandalkan. Sistem pengaman dokumen juga menjadi sebuah layanan menjanjikan, dengan banyaknya bantuan penjagaan dokumen berkredibilitas tinggi yang lengkap.

Banyak layanan pengaman dokumen yang dapat diperoleh di internet. Sistem layanan ini dapat digunakan untuk bidang jarak jauh maupun bidang dalam lingkup satu ruang. Menggunakan sistem ini, memerlukan satu sistem pengaman dokumen bersifat rahasia atau classified, yang mana hanya dapat digunakan oleh pihak yang mempunyai otoritas. Menggunakan proses otentikasi semacam identitas dan kata sandi, sudah dapat digunakan sebagai pengaman dokumen daring.

Time-Based One-time password (TOTP), adalah sebuah sandi valid yang hanya digunakan sekali pada saat melakukan akses sesi maupun transaksi. Teknik ini digunakan pada sistem komputer atau sistem alat digital lainnya. Sebuah TOTP biasanya diperoleh dalam bentuk sandi 6-digit ke komunikasi elektronik. Teknik yang digunakan pengiriman TOTP sangat khas, bisa dengan bergiliran berganti 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) dengan tatanan keamanan, efisiensi dan efektivitas dalam memperoleh sandi. TOTP dengan melalui teknik ini sangat menguntungkan bagi pihak dalam berbagai aspek, seperti keamanan, keandalan, dan teknik.

Multi-factor authentication (2FA), adalah sebuah metode otentikasi elektronik yang mana menggunakan proses persetujuan pengguna komputer untuk memperoleh akses ke halaman situs web atau aplikasi secara sukses dengan penyerahan bukti. Metode yang digunakan pada 2FA tergolong rapi dan efektif untuk proses masuk pengguna, perolehan

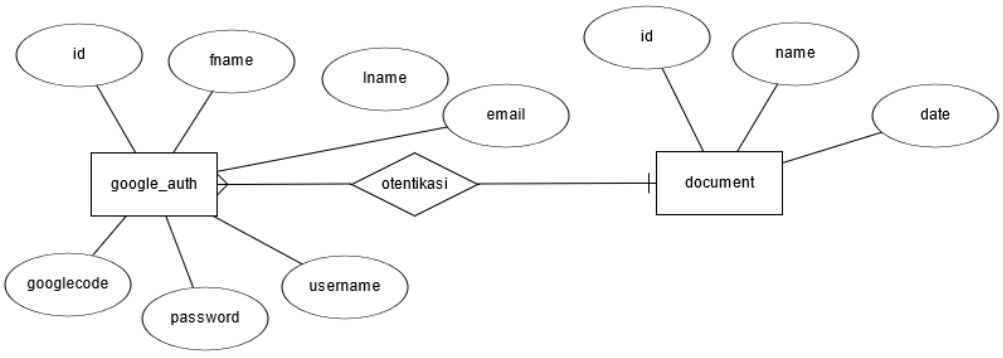
bukti atau faktor dapat diinput dengan sandi tertentu untuk dicocokkan dengan halaman situs web atau aplikasi yang dituju. 2FA umumnya sangat digantungkan kepada keawetan penjagaan kemanan dokumen penting, seperti informasi identitas pribadi, detail, maupun aset finansial.

METODE PENELITIAN

Penelitian ini dilakukan melalui beberapa tahapan yang sistematis. Tahap pertama adalah studi literatur, yaitu dengan membaca dan memahami berbagai referensi dari buku, artikel, jurnal, makalah, dan situs yang berkaitan dengan sistem pengamanan dokumen. Selanjutnya, dilakukan pengumpulan data dengan merelevansikan berbagai informasi terkait, seperti jenis dokumen elektronik (e-document), guna memperoleh hasil yang sesuai dengan tujuan penelitian. Setelah itu, tahap analisis sistem dilakukan untuk menentukan standar kinerja sistem serta menyusun rencana desain yang tepat. Tahap berikutnya adalah perancangan desain sistem, yang mencakup pembuatan antarmuka situs web dan struktur keamanan dokumen menggunakan algoritma TOTP pada 2FA, dengan fokus utama pada pengamanan proses log masuk pengguna.

Entity Relationship Diagram (ERD)

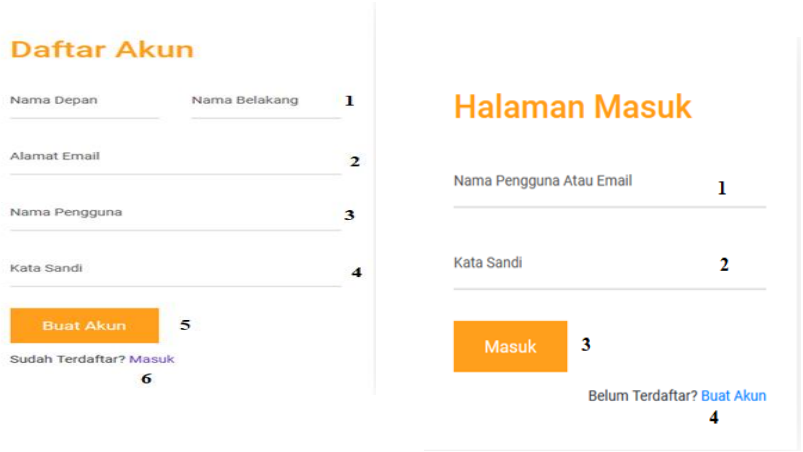
Diagram ERD menggambarkan hubungan antar entitas. Struktur wajib dipertimbangkan sebelum sistem keamanan dokumen menggunakan algoritma TOTP pada 2FA diimplementasikan. Seperti satu pengguna yang didaftarkan, bisa mengakses semua dokumen yang diunggah pengguna lainnya dan pengguna yang memperoleh akses masuk, dapat memperoleh akses penuh ke dalam sistem manajer berkas. Berdasarkan pertimbangan yang diambil dari poin-poin di atas, maka ERD untuk sistem keamanan dokumen menggunakan algoritma TOTP pada 2FA disajikan pada Gambar 1.



Gambar 1. ERD pada sistem

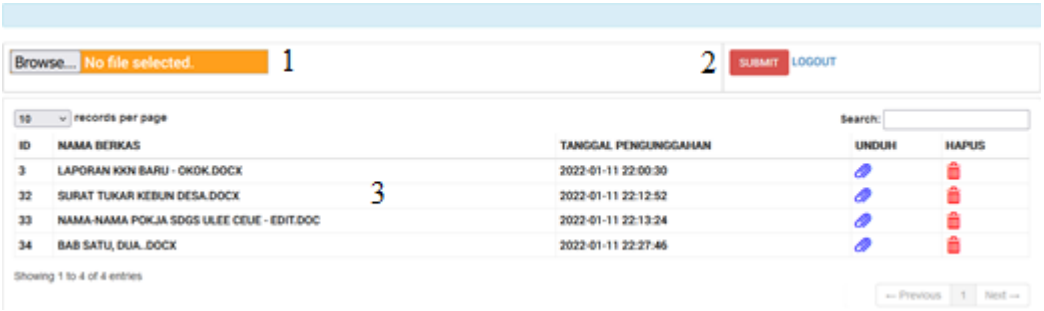
HASIL DAN PEMBAHASAN

Halaman 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. Jika pengguna belum memperoleh akun. Maka dapat mendaftarkan akun menggunakan halaman yang telah disediakan dengan memasukkan beberapa informasi, Adapun tampilan halaman ini dapat dilihat pada Gambar 2 yang dapat digunakan untuk proses *login* ke dalam aplikasi.



Gambar 2. Halaman pendaftaran akun dan halaman masuk

Bagi pengguna yang telah mendaftarkan akun atau telah memulai sesi masuk melalui halaman masuk, maka akan diarahkan langsung ke halaman verifikasi, yaitu halaman tempat di mana kode google akan diminta oleh sistem, dengan pencocokan pada aplikasi *Google Authenticator*, yang selanjutnya dapat mengakses dokumen dalam manajemen. Perolehan proses masuk dirancang bersamaan dengan objek yang diteliti. Dalam tahapan ini, objek tersebut sebagai dokumen, membutuhkan media sebagai penyimpanan dokumen-dokumen. Dapat dilihat pada Gambar 3.



Gambar 3. Manajer Berkas Dokumen

KESIMPULAN

Keamanan dokumen tidak hanya penting dalam bentuk digital tetapi juga dalam bentuk fisik sebagai cadangan jika terjadi kehilangan atau kerusakan data. Penelitian ini mengembangkan sistem keamanan dokumen dengan mengombinasikan algoritma 2FA dan metode TOTP untuk meningkatkan perlindungan. Sistem dirancang dengan integrasi API publik yang memungkinkan proses otentikasi melalui Google Authenticator, di mana kode verifikasi digunakan untuk memastikan kecocokan dengan PIN terdaftar saat masuk ke dalam sistem. Desain ini bertujuan untuk memberikan kemudahan bagi pengguna dalam mengakses dan mengamankan dokumen tanpa hambatan, dengan antarmuka yang intuitif serta pemanfaatan RESTful API sebagai penghubung dengan manajer berkas.

SARAN

Penulis yakin jurnal ini jauh dari kata sempurna dan harapan ke depannya, dengan jurnal ini pengembangan sistem baru dengan fitur-fitur mutakhir dapat dilakukan oleh anak-anak bangsa.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada kedua orangtua, saudara-saudara, pembimbing jurnal, serta civitas kampus Fakultas Teknis Informatika Universitas Jabal Ghafur yang menjadikan jurnal ini dibentuk sampai saat ini.

DAFTAR PUSTAKA

Doly, R. 2017. Implementasi One Time Password Mobile Token Dengan Algoritma Secure Hash Algorithm 1 (Sha1) Pada Login Website Pusdaskrimti Kejaksaan Agung Republik Indonesia. Jakarta: Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Budi Luhur.

Dzulqaidah, A. 2012. Pembangkitan Kombinasi Kode pada Google Authenticator. Bandung: Institut Teknologi Bandung.

Hapsari, N.S. Dan Fatman, Y. Dan Isbandi, I. 2020. Implementasi Metode One Time Password pada Sistem Pemesanan Online. Bandung: Program Studi Teknik Informatika Universitas Islam Nusantara.

Id, Ibnu. 2016. Implementasi TOTP (Time-Based One-Time Password) Untuk Meningkatkan Keamanan Transaksi E-Commerce. Batam: Konferensi Nasional Sistem Informasi Universitas Riau.

Musliyana, Zuhar. Dan Arif, Teuku Dan Munadi, Rizal. 2016. Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. Banda Aceh: Jurusan Teknik Elektro, Fakultas Teknik, Universitas Syiah Kuala.

Yusuf, R.B. Dan Anggriawan, E.S. Dan Negara, S.T. 2015. Penerapan Metode Smart Authentication Dalam Layanan E-Banking Menggunakan Two Channel Authentication Dan Qr-Code Pada Perangkat Mobile Android. Bogor: Seminar Nasional Sistem Informasi Indonesia Sekolah Tinggi Sandi Negara.

Garg, G. 2015. How QR Codes work: Everything you need to know. https://scanova.io/blog/blog/2015/02/19/how-qr-codes-work, diakses tanggal 20 Oktober 2021.

Josefsson, S. 2003. The Base16, Base32, and Base64 Data Encodings. https://tools.ietf.org/html/rfc3548, diakses tanggal 14 Oktober 2021.

Lodha, T. 2018. Google Authenticator and how it works?. https://medium.com/@tilaklodha/google-authenticator-and-how-it-works-2933a4ece8c2, diakses tanggal 16 Oktober 2021.

M'Raihi, D. dkk. 2011. OTP: Time-Based One-Time Password Algorithm. https://datatracker.ietf.org/doc/html/rfc6238, diakses tanggal 12 Oktober 2021.