IMPLEMENTASI *TIME-BASED ONE TIME PASSWORD (TOTP)* PADA SISTEM *TWO FACTOR AUTHENTICATION (2FA)*

Herri Setiawan[1], Dewi Sartika[2], Boy Gilang Ramadhan[3]
[123]Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Indo Global Mandiri
herri@uigm.ac.id, dewi.sartika@uigm.ac.id, boy@uigm.ac.id

ABSTRACT

The ease of access to services via the internet creates new problems, these problems are related to the security of access to information. Internet security is a mandatory thing that must be considered for all users, both from physical security, data, and applications. Security implementation is used to avoid various forms of threats such as data reading, data modification, interruptions by unauthorized parties. Authentication is one way to avoid this problem. There are two types of authentication, namely one factor and two-factor authentication. This research will implement the Time-Based One Time Password (TOTP) algorithm in the Two Factor Authentication (2FA) system. This system implementation combines a mobile phone as an authentication token in an Android application based on the process of reading a Quick Response Code (QR Code) or in the form of a secret key in a Web application that is known only to the user. The implementation of TOTP on the 2FA system as a dual security method at the time of authentication can be implemented in Web and Android applications to carry out its functions. The results of testing the application using the User Acceptance Test (UAT) by giving questionnaires to 40 respondents showed 85.8% who answered Strongly Agree.

Keywords: *Internet, Security, 2FA, TOTP, QR-Code, UAT*

INTISARI

Internet, Keamanan, *2FA*, *TOTP, QR-Code, UAT*.Kemudahan akses layanan melalui internet menimbulkan permasalahan baru, permasalahan tersebut adalah terkait keamanan terhadap akses informasi. Keamanan internet merupakan hal wajib yang harus diperhatikan untuk semua pengguna baik dari keamanan fisik, data dan juga aplikasi. Implementasi keamanan digunakan untuk menghindari berbagai macam bentuk ancaman seperti pembacaan data, modifikasi data, interupsi oleh pihak yang tidak berwenang. Otentikasi adalah salah satu cara menghindari permasalahan tersebut. Terdapat dua jenis otentikasi yaitu otentikasi *one factor* dan *two factor*. Dalam penelitian ini akan dilakukan implementasi algoritma *Time-Based One Time Password (TOTP)* pada sistem *Two Factor Authentication (2FA)*. Implmentasi sistem ini mengkombinasikan telepon genggam sebagai token otentikasi pada aplikasi *Android* yang berdasarkan pada proses pembacaan *Quick Response Code (QR Code)* atau dalam bentuk *secret key* pada aplikasi *Web* yang hanya diketahui oleh pengguna. Penerapan *TOTP* pasa sistem *2FA* sebagai metode keamanan ganda pada saat otentikasi dapat diimplementasikan pada aplikasi *Web* dan *Android* untuk menjalankan fungsinya. Hasil pengujian aplikasi menggunakan *User Acceptance Test (UAT)* dengan memberikan kuisioner terhadap 20 responden didapatkan hasil 85,8% yang menjawab Sangat Setuju.

Kata Kunci: Internet, Keamanan, *2FA*, *TOTP, QR-Code, UAT*.

PENDAHULUAN

Pada saat ini kemudahan akses layanan melalui *internet* menimbulkan permasalahan baru, permasalahan tersebut adalah terkait keamanan terhadap akses informasi. Oleh karenanya, keamanan merupakan hal penting dan wajib diperhatikan bagi semua pengguna baik dari sis keamanan fisik, data dan juga aplikasi.

Penerapan keamanan digunakan untuk menghindari berbagai macam bentuk ancaman seperti pembacaan data, modifikasi data, dan interupsi oleh pihak yang tidak berwenang. Cara menghindari permasalahan tersebut dapat dilakukan salah satunya dengan cara otentikasi. Otentikasi adalah proses membuktikan suatu identitas (Kessler, 2019). Otentikasi bertujuan membuktikan keabsahan seseorang dalam menggunakan suatu layanan.Terdapat dua jenis otentikasi berdasarkan jumlah metode yang digunakan yaitu otentikasi *one factor* dan *two factor*. Metode otentikasi dilihat dalam 3 (tiga) kategori metode, yaitu : *Something you kno, Something you have* dan *Something you are*. Otentikasi *one factor* merupakan otentikasi yang menerapkan satu metode sedangkan otentikasi *two factor* merupakan otentikasi

yang mengkombinasikan dua atau lebih metode otentikasi untuk meningkatkan keamanan. Otentikasi *two factor* dapat dimanfaatkan untuk meminimalisir serangan pengalihan akun, khususnya untuk data yang sensitif seperti transaksi perbankan.

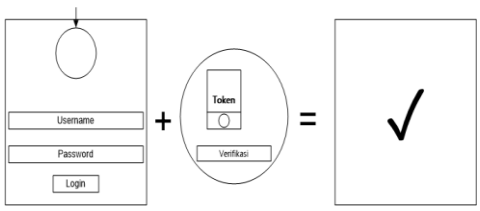
Oleh karena itu pada penelitian ini akan dilakukan implementasi dari otentikasi menggunakan algoritma *Time-Based One Time Password (TOTP)* berbasis *Two Factor Authentication (2FA)*. Menurut M'Raihi, Machani, Pei, & Rydell (2011), *Time-Based One Time Password (TOTP)* adalah ekstensi dari *HMAC-based One-time Password (HOTP)* yang menghasilkan kata sandi satu kali dengan cara mengambil keunikan dari waktu sekarang. Sistem ini akan mengkombinasikan telepon genggam yang digunakan sebagai token otentikasi pada aplikasi *Android* yang akan dibangun serta dihasilkan berdasarkan proses pembacaan *QR Code* atau dalam bentuk *secret key* pada aplikasi *web* yang hanya diketahui oleh pengguna. Melalui proses otentikasi dengan token dapat dilakukan dengan lebih aman sebab proses otentikasi tidak hanya dengan mengingat *password* tapi juga harus memasukan token yang ada pada telepon genggam pengguna, dimana token tersebut selalu berubah dalam jangka waktu tertentu.

Penerapan *TOTP* berbasis *2FA* sebagai metode keamanan ganda pada saat otentikasi diharapkan dapat diterapkan sebagai alternatif untuk keamanan dan meminimalisir berbagai macam ancaman serangan retas seperti pengalihan akun pengguna oleh pihak yang tidak berwenang

METODE PENELITIAN

1. Metode Pengembangan Sistem

Sistem yang akan dibangun akan diimplementasikan dalam bentuk proses otentikasi pengguna di sebuah aplikasi *online* berbasis *web* dan juga dibangun sebuah aplikasi *Android* yang dalam hal ini disebut otentikator sebagai pembangkit token.



Gambar 1. Gambaran Umum Sistem

Gambar 1. adalah gambaran umum sistem yang akan dibangun yaitu aplikasi *web* dan *android*. Pengguna mengakses halaman *login* lalu dihadapkan tampilan masukan token dilanjutkan mengambil token pada aplikasi *android* untuk dimasukan ke *form web* dan proses otentikasi selesai.

Metode yang digunakan adalah *prototype* dikarenakan metode ini memiliki keuntungan lebih dalam hal komunikasi yang intens antara pengembang dan pengguna, agar pengembang dapat dengan mudah untuk menentukan kebutuhan pengguna dan meminimalkan risiko kesalahan persepsi. Adapun tahapan pengembangan dengan metode *prototype* adalah sebagai berikut (Pressman, 2010):

a. *Communication*

Communication merupakan tahap awal penelitian. Pada tahapan ini, dikumpulkan informasi dan kebutuhan yang dibutuhkan dalam pembangunan *prototype*. Kebutuhan yang dimaksud adalah kebutuhan perangkat keras dan perangkat lunak yang dibutuhkan untuk membangun aplikasi serta pengetahuan tentang proses otentikasi dua langkah pada saat *login* di aplikasi *web* dan otentikator pada aplikasi *Android*.

b. *Quick Plan*

Pada tahapan ini, dilakukan perancangan cepat atau perancangan sementara berdasarkan pengumpulan data yang diperoleh. Perancangan cepat ini juga melibatkan perancangan aplikasi yang akan dibangun dimana peneliti menggunakan pemindaian *Quick Response Code (QR Code)* pada aplikasi *Web* dari aplikasi *Android* sebagai otentikator untuk mendapatkan token yang telah dibangkitkan.

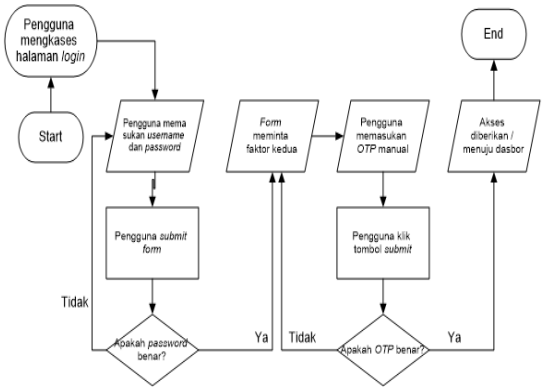
c. *Modelling Quick Design*

Pada tahap ini dilakukan perancangan perangkat lunak yang akan dibangun. Gambar 2 adalah *Flowchart* Sistem dengan alur urutan proses (instruksi) sebagai berikut:

1. Start
2. Mengakses halaman *login.*
3. Memasukan *username* dan *password*.
4. Klik *submit form* setelah memasukan *username* dan *password*.
5. Pada kondisi ini, sistem akan mencocokan *username* dan sekaligus memproses *password* menjadi

terenkripsi dengan *SHA-256 Hash* sebelum dikirim ke *web* untuk diverifikasi kredensial sesuai dengan yang tersimpan di basis data.

6. Jika kondisi kredensial benar, maka akan diteruskan ke halaman otentikasi 2 langkah/faktor kedua. Jika tidak, maka akan kembali lagi ke halaman *login*.
7. Pada halaman otentikasi 2 langkah/faktor kedua, pengguna diwajibkan untuk memasukan *OTP*/Token yang dihasilkan melalui aplikasi Otentikator yang sudah dipasang pada *Android* lalu klik *submit*.
8. Jika kondisi otentikasi dengan masukan *OTP*/Token benar, maka akan diberikan akses dan menuju halaman dasbor. Jika tidak, maka pengguna akan dialihkan kembali ke *form* untuk memasukan kembali *OTP*/Token sampai benar.
9. Pengguna berhasil sampai ke halaman dasbor dan dapat melakukan apapun pada sistem terhadap fasilitas yang telah diberikan pada *website* tersebut.
10. End



Gambar 2. *Flowchart* Sistem

d. *Construction Of Prototype*
Pada tahap ini, peneliti akan membahas implementasi perangkat lunak yang akan dijelaskan pada Hasil dan Pembahasan

e. *Deployment Delivery & Feedback*
Tahapan terakhir ini merupakan tahapan implementasi software ke customer, perbaikan perangkat lunak, evaluasi perangkat lunak, dan pengembangan perangkat lunak berdasarkan umpan balik yang diberikan agar sistem dapat tetap berjalan dan berkembang sesuai dengan fungsinya.

2. Metode Pengujian *User Acceptance Test (UAT)*

User Acceptance Testing (UAT) adalah proses verifikasi bahwa solusi yang dibuat dalam sistem sudah sesuai untuk pengguna. Proses ini berbeda dengan pengujian sistem (memastikan software tidak crash dan sesuai dengan dokumen permintaan pengguna), melainkan memastikan bahwa solusi dalam sistem tersebut akan bekerja untuk pengguna (Wikipedia contributors, 2020).
Pengujian akan dilakukan terhadap pengguna dengan mencoba menjalankan aplikasi dan mengisi kuesioner. Persentase masing-masing jawaban dicari berdasarkan dari data hasil kuisioner dengan menggunakan rumus kuisioner:

$$Y = P/Q * 100\% \quad (1)$$

Keterangan:
Y : Nilai persentase
P : Total Skor
Q : Skor tertinggi

Hasil *UAT* dinilai dalam 5 kategori, yaitu SS (Sangat Setuju), S (Setuju), CS (Cukup Setuju), KS (Kurang Setuju) dan TS (Tidak Setuju). Pertanyaan-pertanyaan yang diteliti untuk kuesioner dapat dilihat pada Tabel 1.

Untuk mengukur sikap dari pengunjung aplikasi yang telah dibangun digunakan *Skala Likert*. *Skala Likert* merupakan skala yang digunakan untuk mengukur persepsi, sikap atau pendapat seseorang atau kelompok mengenai sebuah peristiwa atau fenomena sosial, berdasarkan definisi operasional yang telah ditetapkan oleh peneliti.

Tabel 1. Pertanyaan Kuesioner

No	Pertanyaan	Penilaian				
		SS	S	CS	KS	TS
1	Apakah aplikasi berpengaruh dalam segi keamanan?					
2	Apakah pengguna nyaman menggunakan aplikasi?					

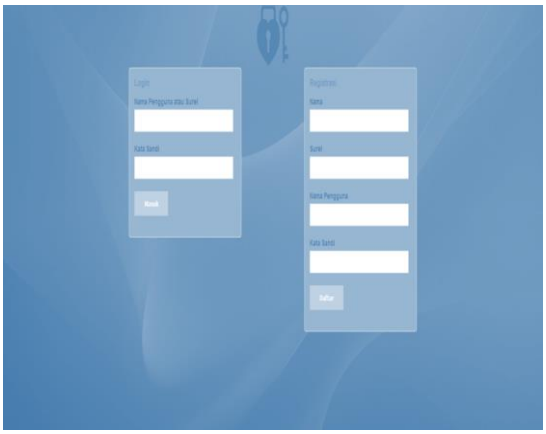
3	Apakah aplikasi efisien untuk diterapkan?
4	Apakah aplikasi dapat diterapkan dengan biaya terjangkau?
5	Apakah privasi pengguna dijamin terhadap penggunaan aplikasi?

HASIL DAN PEMBAHASAN

Hasil penelitian dibuat dalam dua tampilan antar muka yaitu Web dan Android, kedua aplikasi yang dibangun saling berhubungan satu sama lain.

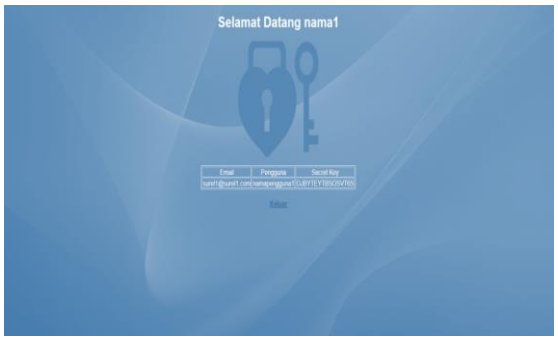
1. Antarmuka *Web*

Antarmuka *Web* seperti yang terlihat pada Gambar 3, merupakan tampilan halaman aplikasi yang telah ditanamkan metode *login Two Factor Authentication* (*2FA)*, pada saat *login* berhasil pengguna belum bisa langsung masuk halaman yang dituju, tetapi akan dihadapkan sebuah *form* (Gambar 4) yang berisikan *QR Code* untuk memasukan token yang dihasilkan pada perangkat *handphone* yang telah terpasang aplikasi Otentikator untuk dimasukan kembali ke *Web* untuk memvalidasi akses tersebut Sehingga, jika semua kredensial telah dimasukan dengan benar seperti identitas pengguna dan kata sandi lalu berlanjut ke validasi token yang benar maka pengguna baru diarahkan ke halaman yang dimaksud, dalam hal ini adalah halaman Dasbor (Gambar 5).



Gambar 3. Tampilan Utama *Web*

Gambar 4. Tampilan Validasi



Gambar 5. Tampilan Dasbor

2. Antarmuka *Android*

Antarmuka *Android* merupakan tampilan halaman aplikasi Otentikator yang telah ditanamkan metode *2FA* yang akan membangkitkan sebuah token yang dibutuhkan oleh aplikasi *Web* pada saat aksi pemindaian *QR Code* yang telah dilakukan sebelumnya, pada penelitian ini aplikasi *Android* yang dibangun menggunakan bahasa pemrograman *Java*. Pada aplikasi ini terdapat beberapa fitur diantaranya menambah, mengubah dan menghapus data token yang telah tersimpan pada perangkat *handphone*. Sehingga, sampai disini sudah terlihat hubungan teknis antara aplikasi *Web* dan *Android*.

Pada tampilan dasbor ini akan menampilkan data token yang telah berhasil dibuat dari proses pemindaian *QR Code*

terhadap aplikasi *web* jika sebelumnya sudah ditambahkan, dapat dilihat pada Gambar 6.

Gambar 6 Tampilan Utama *Android*

Gambar 7 merupakan langkah untuk menambah token baru yang dilakukan dengan cara memindaikan *QR Code* yang ditampilkan oleh aplikasi *Web* dengan menyentuh gambar *QR Code* pada pojok kanan atas, dapat dilihat pada Gambar 6.

Gambar 7. Tampilan Pemindaian

3. Hasil Pengujian *UAT*

Berdasarkan hasil kuesioner terhadap 40 (empat puluh) pengguna, didapatkan persentase masing-masing jawaban dengan menggunakan persamaan (1).

Skor untuk jawaban kuesioner yang telah diberikan yaitu:

1. Jawaban SS diberi nilai 5
2. Jawaban S diberi nilai 4
3. Jawaban CS diberi nilai 3
4. Jawaban KS diberi nilai 2
5. Jawaban TS diberi nilai 1

Untuk mengetahui interpretasi skor hasil perhitungan dapat dilihat pada Tabel 2.

Tabel 2. Interpretasi Skor Perhitungan

Nilai	Keterangan
81% - 100%	Sangat Setuju
61% - 80%	Setuju
41% - 60%	Cukup Setuju
21% - 40%	Kurang Setuju
0% - 20%	Tidak Setuju

Hasil perhitungan jawaban dari 5 (lima) pertanyaan, didapatkan persentase 89%, 80.5%, 84.5%, 93.5, 81.5. Berdasarkan persentase rata-rata dari 5 pertanyaan yang diberikan seperti terdapat pada Tabel 1, didapatkan sebesar 85,8% responden memilih *Sangat Setuju* terhadapt Implementasi *Time-Based One Time Password (TOTP)*

KESIMPULAN

Berdasarkan implementasi dan hasil pengujian dari aplikasi ini, dapat diambil kesimpulan sebagai berikut:

1. Penelitian ini berhasil membangun sebuah aplikasi *Two Factor Authentication (2FA)* berbasis *Web* dan *Android* sebagai metode otentikasi 2 langkah.
2. Fitur yang ada pada *2FA* yang dibangun dapat diimplementasikan pada aplikasi *Web* dan *Android* untuk menjalankan fungsinya sesuai dengan hasil yang diharapkan dan hasil pengujian UAT disimpulkan bahwa pengguna sangat setuju bahwa privasi atau data pengguna akan terjaga.

DAFTAR PUSTAKA

Kessler, G. C. (2019). *An Overview of Cryptography (Updated Version 24 January 2019)*. Daytona Beach. Retrieved from https://commons.erau.edu/cgi/viewcontent.cgi?article=1466&context=publication

M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). *TOTP: Time-Based One-Time Password Algorithm*. *Internet Engineering Task Force (IETF)*. California. Retrieved from http://mirror.cogentco.com/pub/rfc/pdf/rfc6238.txt.pdf

Pressman, R. S. (2010). *Software Engineering : A Practitioner's Approach*. (F. M. Schilling, Ed.) (7th ed.). New York, NY, 10020: McGraw-Hill.

Wikipedia contributors. (2020). Acceptance testing. In Wikipedia, The Free Encyclopedia. Retrieved May 11, 2020, from https://en.wikipedia.org/w/index.php?title=Acceptance_testing&oldid=970088426