Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password

Alfat Yanuar Fitriyansyah[1],M.Hazri[2]

[1] Universitas Amikom Yogyakarta
alfat.09@students.amikom.ac.id
[2] Universitas Amikom Yogyakarta
hazri.15@students.amikom.ac.id

ABSTRAK

Pengamanan web login dengan menggunakan OTP (One Time Password) yang menghasilkan sebuah kode lewat SMS untuk otentikasi suatu aktivitas login. OTP yang dikirimkan kepada pengguna/user akan dicocokkan dengan data yang tersimpan pada sebuah database, maka yang dimana pada saat melakukan Login pengguna/user tidak hanya akan dimintai username dan password saja sebagai pengamanan tetapi juga akan dimintai sebuah Kode OTP yang nantinya dikirimkan melalui SMS pada ponsel pengguna/user. Dengan melakukan metode penelitian yang meliputi Pengumpulan Data, Analisa serta Kesimpulan maka penulis dapat menyimpulkan masalah dan solusi yang bisa diberikan.Waktu aktif untuk pengamanan login dengan OTP berbasis SMS selama satu sampai 3 menit, pembatasan tersebut yang berguna untuk mempersempit waktu hacker untuk menyadap dan menyusup.

Kata Kunci : OTP, Pengamanan Login, SMS, Web.

ABSTRACT

Web login security by using OTP (One Time Password) which generates a code via SMS to authenticate a login activity. OTP sent to the user / user will be matched with data stored in a database, so that when logging in the user / user will not only be asked for a username and password as security but will also be asked for an OTOP Code which will be sent via SMS to cell phone user / user. By conducting research methods that include Data Collection, Analysis and Conclusion, the author can conclude the problems and solutions that can be given. Active time for securing logins with SMS-based OTP for one to 3 minutes, these restrictions are useful for narrowing the hacker time to tap and infiltrate .

Keywords : OTP, Login Security, SMS, Web.

I. PENDAHULUAN

A. LATAR BELAKANG

Keamanan adalah perhatian utama dalam segala sektor sekarang ini meliputi, dunia perbankan, aplikasi pemerintahan, organisasi kemiliteran, institusi pendidikan dan lain sebagainya. Perkembangan yang sangat pesat pada layanan online memicu peningkatan jumlah identitas digital setiap pengguna butuhkan. Dan password menjadi pengamanan yang

paling banyak digunakan untuk saat ini [1].

Para pengguna biasa menggunakan kata-kata yang sudah pasti mereka mudah diingat seperti Nama, umur, tanggal lahir, kata sandi atau bahkan password seperti ini sangatlah mudah dipecahkan dengan menggunakan program pemecah sandi yang sederhana.

Berbagai informasi pengguna menjadi sangat rentan terhadap beberapa tindakan pencurian data yang melalui berbagai serangan contohnya yakni serangan ***Phising***. Serangan ***Phising*** sering sekali digunakan untuk memalsukan alamat E-mail yang akan terkirim dari sumber yang sekiranya terlihat terpercaya. Pelaku kejahatan internet membuat sebuah pesan yang seolah-olah dapat dipercaya oleh korban, sehingga dengan menggunakan format yang mirip dengan yang asli maka korban akan terkecoh dengan alamat E-mail tersebut. Dengan menggunakan teknik social engineering mereka mampu menarik korbannya untuk membalas pesan mereka.

Maka dari itu dalam dalam permasalahan ini penulis ingin mengambil salah satu contoh yaitu keamanan pada web login mahasiswa di sebuah kampus/universitas yang dimana saat mahasiswa/mahasiswi dalam melakukan login, mereka hanya memasukkan Nomor Induk Mahasiswa (Nim) dan Password.

Ketidakmampuan proses single factor authentication dalam mengamankan akun-akun penting para pengguna ini dapat memicu berbagai kebutuhan otentikasi lebih dari satu faktor. Proses Two factor authentication (2FA) adalah sistem otentikasi yang membutuhkan 2 faktor untuk melakukan otentikasi identitas pengguna.

B. ***RUMUSAN MASALAH***

Berdasarkan uraian latar belakang diatas, maka penulis dapat merumuskan masalah sebagai berikut :

1. Bagaimana menerapkan ***Pengamanan Web Login Mahasiswa*** dengan menggunakan ***Two-Factor Time-Based One Time?***
2. Bagaimana caranya agar saat Mahasiswa dalam melakukan Login ke sebuah web Universitasnya aman dari orang-orang yang tidak bertanggung jawab?

C. ***TUJUAN***

Adapun yang menjadi tujuan dari penelitian ini adalah :

1. Mengetahui sistem kerja dari pengamanan Web Login dengan menggunakan ***Two-Factor Time-Based One Time*** dengan baik.
2. Agar dalam melakukan aktivitas Login pada Web Mahasiswa/Mahasiswi terhindar dari serangan-serangan yang dapat membahayakan Informasi Pribadi Mahasiswa.

II. LANDASAN TEORI DAN METODE PENELITIAN

A. One Time Password (OTP)

One-time password (OTP) adalah merupakan salah satu kata sandi yang cukup valid dan bisa digunakan hanya untuk satu kali sesi login atau transaksi saja pada sebuah komputer atau perangkat digital lainnya. Berbeda dengan ***Password Statis***, OTP (One-Time Password) juga dapat bertahan dari berbagai serangan replay attack. Terdapat 3 cara untuk menggunakannya diantaranya yakni OTP: ***time-synchronization OTP*** adalah OTP yang digunakan berdasarkan waktu sekarang, ***previous-password-based OTP*** adalah OTP yang digunakan berdasarkan dengan password yang digunakan sebelumnya, dan yang terakhir adalah ***challenge-based OTP*** adalah OTP yang digunakan berdasarkan challenge dari server.

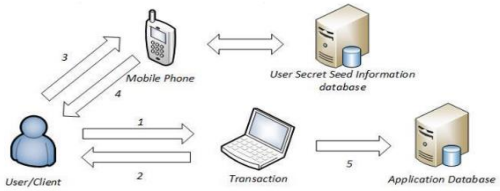
Pengembangan OTP bertujuan untuk mengurangi terjadinya replay attack serta mengurangi resiko password dikirimkan ke pihak lain melalui media lain. replay attack merupakan sebuah serangan yang memanfaatkan cookie yang sudah pernah disimpan dari sesi sebelumnya dan dapat digunakan untuk sesi yang lain. OTP sendiri hanya bisa digunakan satu kali dan memiliki waktu yang terbatas, oleh karena itu *one time password* sangat cocok untuk diimplementasikan pada web kampus atau perusahaan[2].

Analisa ini bertujuan untuk menganalisis sistem Two-factor authentication dengan menggunakan Nomor Induk Mahasiswa (Nim) dan Password sebagai faktor otentikasi pertama dan One Time Password yang dikaitkan dengan perangkat android dengan metode time-based one time password (TOTP) sebagai otentikasi kedua.

Dari hasil analisis masalah yang didapatkan oleh penulis, berdasarkan hasil dari berbagi analisis masalah yang ada, ditemukan permasalahan yakni pada sistem login yang masih memiliki kelemahan password yang mudah ditebak/diketahui maupun disadap oleh hacker. [3]

B. ***Arsitektur Sistem***

Berikut alur kerja sistem yang bisa dijelaskan melalui gambar berikut : [4]



Gambar 1.Arsitektur Sistem

Pada gambar diatas, terdapat alur yang telah diberi nomor masing-masing dengan keterangan sebagai berikut :

1. User atau pengguna dapat melakukan request transaksi pada sistem melalui perangkat komputer atau alat digital lainnya.
2. Sebelum memenuhi request dari pengguna, sistem terlebih dahulu melakukan verifikasi dengan meminta kode one time password (OTP).
3. Pengguna melihat informasi kode OTP pada aplikasi yang terdapat pada perangkat android pengguna yang sebelumnya telah menyimpan kode secret seed.
4. Pengguna mendapatkan informasi kode OTP yang diperlukan untuk melanjutkan transaksi.
5. Apabila kode OTP yang dimasukan oleh pengguna sesuai maka transaksi yang dilakukan oleh pengguna akan disimpan dan diproses pada database aplikasi.

C. ***Metode Otentikasi***

Metode otentikasi berikut bertujuan untuk membuktikan bahwa siapa saja pengguna yang sebenarnya dan apakah pengguna merupakan pengguna asli/sah untuk masuk ke sebuah sistem. Untuk membuktikan hal tersebut apakah ia pengguna yang sah atau tidak sah dapat dijelaskan dalam metode otentikasi berikut :

A. Something you know

Metode otentikasi ini adalah yang paling umum atau yang paling sering digunakan dalam hal

mengandalkan kerahasiaan suatu informasi. Contohnya adalah password atau PIN dengan asumsi bahwa tidak ada seorangpun yang dapat mengetahui kerahasiaan tersebut kecuali dirinya sendiri.

B. Something you have

Metode otentikasi ini merupakan faktor tambahan untuk membuat otentikasi menjadi lebih aman dengan mengandalkan suatu barang yang sifatnya unik seperti contohnya *smart card, kartu tanda mahasiswa, hardware token, usb token* dan sebagainya, dengan asumsi bahwa tidak seorangpun yang dapat memiliki *hardware* tersebut kecuali dirinya sendiri.

C. Something you are

Metode otentikasi ini sangat jarang sekali dipakai karena faktor teknologi dan manusia, yaitu dengan mengandalkan bagian-bagian tubuh dari orang tersebut yang sudah menjadi ciri fisik manusia seperti *sidik jari, retina* dan lain-lain.

D. Something known about

Metode otentikasi terakhir yakni bahwa tidak ada seorang pun di dunia ini yang mampu menirukannya atau dalam kata lain tidak dapat dimodifikasi oleh orang lain. Sebagai contohnya *tanda tangan* yang dianggap sebagai bukti otentik dari diri pengguna.

D. *Two Factor Authentication*

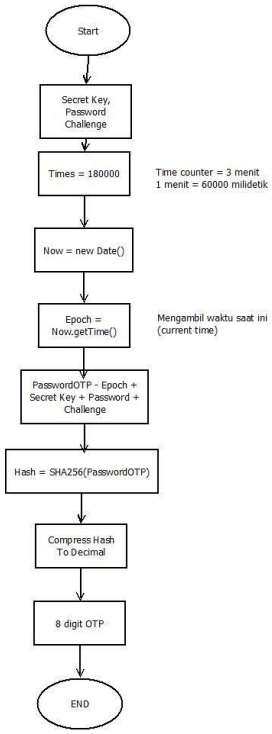
Pada aplikasi kritis dan sensitif seperti transaksi keuangan, satu metode otentikasi saja tidak cukup maka muncul istilah 2FA (Two Factor Authentication) yang merupakan sistem otentikasi yang menggabungkan 2 metode otentikasi berbeda (Seth Rosenblatt, 2015).[5]

Empat dari metode otentikasi ini dapat digabungkan guna meningkatkan keamanan contohnya *Something You Have* (Kartu Tanda Mahasiswa) yang dapat digabungkan dengan *Something You Know* (PIN). Contoh lain yang dapat kita ambil yakni ketika saat berbelanja di suatu *Supermarket* kita biasanya menggunakan yang Namanya *Kartu Kredit,* yang dimana ada beberapa metode otentikasi yaitu *Something You Have* (kartu kredit), *Something You Know* (PIN) yang biasa diinputkan kedalam mesin yang bernama EDC *(Electronic Data Capture)* dan *Something You Can* (tanda tangan) ke nota pembayaran.

Pada kasus lainnya yang dapat kita ambil contoh lain yakni pada *Internet Banking* yang dimana juga menggunakan 2FA dengan menggabungkan *Something You Know* (password statis) dengan *Something You Have* (token hardware).

E. *Time-BasedOne Time Password (TOTP)*

Time-Based One Time Password (TOTP) adalah sebuah algoritma yang dikembangkan oleh HMAC ***(Hashes Message Authentication Code)*** yang dimana dengan menggabungkan antara secret key dengan current timestamp (waktu saat ini) dan menggunakan fungsi kriptografi hash untuk menghasilkan password sekali pemakaian. Untuk memberikan gambaran cara kerja algoritma TOTP dapat dilihat pada flowchart pada Gambar 2.



Gambar 2.Flowchart Algoritma TOTP

Pada Gambar 2 dapat dijelaskan algoritma TOTP sebagai berikut :

1. Inisialisasi secret key diambil dari serial number token virtual yang sifatnya unik.
2. Inisialisasi challenge code berupa bilangan decimal 8 digit dengan kombinasi 2 digit dihasilkan secara random menggunakan library RandomUtils dan 6 digit diambil dari 6 digit terakhir dari nomor rekening.
3. Times adalah counter atau umur token password sebesar 3 menit. Pada bahasa Scala satuan terkecil untuk waktu yang dapat dijadikan untuk kalkulasi adalah milidetik sehingga harus di konversi dari menit ke milidetik dengan perhitungan 3 menit = 3x60 detik = 180 detik. 180 detik = 180x1000 milidetik = 180000 milidetik.
4. Epoch adalah jangka waktu yang dihitung saat challenge code di generate.

5. Password OTP dihasilkan dari penggabungan epoch, secret key, dan challenge code.
6. Proses hashing terhadap password OTP menggunakan enkripsi SHA256.
7. Hasil hashing dikonversi menjadi bilangan desimal untuk diambil token password sebesar 8 digit.

F. Analisis Swot

Analisis SWOT adalah sebuah cara yang sering digunakan untuk mencari dan melakukan dalam melakukan evaluasi dari sebuah rancangan yang ingin diciptakan dengan memperhatikan macam-macam unsur yakni kekuatan (strengths), kelemahan (weakness), peluang (opportunuties), dan ancaman (threats), maka dari keempat unsur itulah yang dapat melandasi terbentuknya sebuah analisis SWOT yang sering kali digunakan sampai saat ini.

Analisis SWOT juga memiliki berbagai fungsi utama selain membahas keempat unsur yang ada di Analisis SWOT, yakni analisis dari Kekuatan (strength) yang diciptakan dalam bentuk suatu proyek kerja, kemudian bagaimana bisa dalam mengatasi suatu ancaman (treats) yang ada dalam suatu proyek yang sedang dibangun/dikerjakan, kemudian juga mengatasi berbagai kelemahan (weakness) yang dapat memicu adanya ancaman saat proyek ini selesai dirancang dan telah menjadi konsumsi Publik.

1) Kekuatan (Strength)

Pada analisis ini penulis dapat melihat kekuatan dari sebuah sistem pengamanan pada Web Login Mahasiswa dengan menggunakan Algoritma *Two-Factor Time-Based One Time Password* yang dimana Mahasiswa/Mahasiswi dalam melakukan aktivitas Login akan melalui 2 step verifikasi. Yang pertama dengan menggunakan *Username* dan *password* atau dengan *Nomor Kartu Mahasiswa* dan *password* yang berguna untuk lebih mengamankan data-data pribadi mereka yang ada di halaman web Mahasiswa/Mahasiswi tersebut.

2) Kelemahan (Weakness)

Pada analisis ini penulis dapat mengetahui seberapa banyaknya kelemahan dari penerapan Algoritma *Two-Factor Time-Based One Time Password* pada Web Login Mahasiswa/Mahasiswi, salah satu kelemahan yang menjadi fokus penulis yakni pada proses registrasi dan aktivasi Token TOTP sehingga diperlukan mekanisme tambahan yang berfungsi untuk membuktikan apakah pengguna tersebut valid. Salah satu cara yang mungkin bisa digunakan yakni dengan menggunakan SMS ataupun konfirmasi melalui E-mail. Selain itu

resiko serangan lainnya adalah media penyimpanan kunci bersama haruslah aman dan terenkripsi. Dengan TOTP, kita juga dapat mengurangi resiko serangan phising dan eavesdropping.

3) **Peluang (Opportunities)**

Dalam analisis Peluang dapat digunakan untuk melihat seberapa luas cakupan peluang keamanan dari Algoritma *Two-Factor Time-Based One Time Password.* Dalam hal ini Mahasiswa/Mahasiswi dalam hal penggunaan cukup mudah untuk melakukannya. Hal yang pertama yakni Mahasiswa/Mahasiswi perlu yang Namanya *Username* dan *password* yang berguna untuk login di web Mahasiswa. Hal yang kedua yakni tidak hanya dengan menggunakan *Username* dan *password* Mahasiswa/Mahasiswi juga dapat menggunakan kode *One Time Password* (OTP) yang dimana kode tersebut akan dikirimkan melalui ponsel masing-masing dengan menggunakan SMS/Telpon.

4) **Ancaman (Threats)**

Dalaman analisis Ancaman, yang bertujuan untuk mengetahui berbagai ancaman yang mungkin akan dialami dalam melakukan aktivitas Login pada Web Mahasiswa/Mahasiswi hanya jika nomor telepon Mahasiswa/Mahasiswi telah di salah gunakan oleh orang yang tidak bertanggung jawab maka orang tersebut dapat dengan mudah masuk ke halaman Web Mahasiswa/Mahasiswi dan mengganti nomor telepon yang ada di data pribadi pada Web Mahasiswa.

G. Keamanan Komputer

Pada keamanan komputer terdapat beberapa aspek yang diperhatikan diantaranya : [5]

a. ***Authentication***, agar si penerima mendapatkan informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai si penerima yang mengirim informasi tersebut. Dengan kata lain, informasi tersebut benar-benar dari orang yang dikehendaki/dikenal.

b. ***Integrity***, keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan pula bahwa informasi tersebut yang dikirim tidak diubah/dimodifikasi oleh orang yang tidak dikenal dalam proses pengiriman informasi tersebut.

c. ***Non-repudiation***, merupakan hal yang bersangkutan dengan si pengirim. Si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi/pesan tersebut.

d. ***Authority***, informasi yang berada pada suatu sistem jaringan, tidak dapat diubah atau dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.

e. ***Confidentiality***, yakni suatu usaha untuk menjaga informasi tersebut dari orang yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan informasi yang diberikan kepada orang lain.

f. ***Availability***, aspek-aspek dalam *Availability* biasanya berhubungan dengan ketersediaan informasi yang dibutuhkan. Sistem informasi yang biasa diserang atau dibobol dapat menghambat atau meniadakan akses ke informasi tersebut.

g. ***Privacy***, merupakan lebih ke arah data-data yang bersifat pribadi.

h. ***Access Control***, aspek ini biasa berhubungan dengan cara mengatur akses ke informasi. Hal itu juga biasanya berhubungan dengan masalah *authentication* dan *privacy*. *Access Control* biasa dilakukan dengan menggunakan kombinasi user id dan password.

H. Metode Penelitian

Dalam proses pembuatan sebuah sistem informasi dengan menggunakan metode waterfall dengan tujuan akan mempermudah penulis dalam proses penelitian :

a. ***Pertama***, dengan melakukan pengumpulan sebuah data. Berawal dari sebuah proses yang dimana dengan membangun perangkat lunak adalah untuk melakukan riset yang berguna untuk mendapatkan data-data yang sekiranya diperlukan.

b. ***Kedua***, setelah mendapatkan data yang diperlukan, maka tahapan selanjutnya yakni menganalisa dari kebutuhan dari aplikasi yang akan penulis buat. Di dalam proses kedua ini, akan dapat menyimpulkan bahwa hal apa saja yang fungsi dan informasi yang akan dibutuhkan untuk menunjang sebuah sistem informasi yang akan dirancang.[6]

c. ***Ketiga***, setelah selesai menganalisa data dan sudah mendapatkan sebuah kesimpulan, maka langkah selanjutnya yakni berupa mendesain perangkat lunak yang mungkin akan dibuat. Beberapa hal yang mungkin juga dirancang yakni dengan merancang Database.

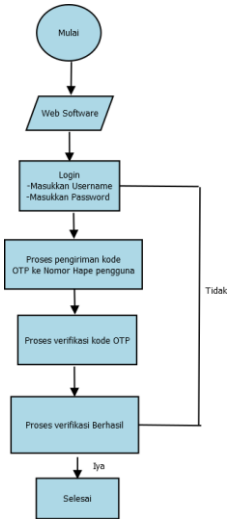
d. ***Keempat***, setelah selesai dalam proses perancangan perangkat lunak dan database, langkah selanjutnya yakni perancangan proses pengkodean. Di dalam proses ini, dengan menggunakan pemrograman PHP yang bisa dijadikan untuk membangun perangkat lunak tersebut serta menggunakan algoritma hash SHA-512 untuk menerapkan kode OTP serta menggunakan MySQLi sebagai perancangan database.

e. ***Kelima***, setelah selesai dalam proses pengkodean langkah selanjutnya yakni percobaan untuk pengimplementasian serta uji coba perangkat lunak tersebut.

III. HASIL DAN PEMBAHASAN

A. *Blok Diagram Sistem*

Berikut gambaran secara umum dari sistem yang dapat dilihat pada Gambar 3.



Gambar 3. Blok Diagram Sistem

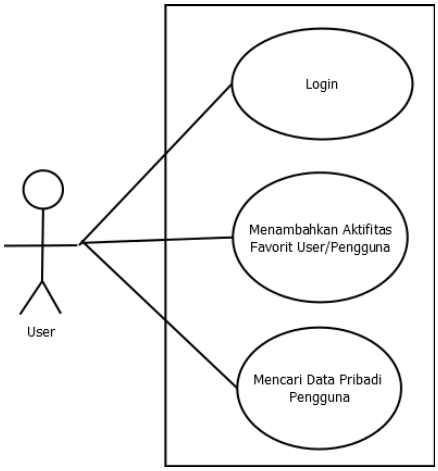
Pada tahapan analisis terhadap kebutuhan perancangan keamanan berbasis *Time-Based One Time Password* berikut tahapan yang dapat diproses berdasarkan Gambar 3 :

1. User pengguna biasa akan membuka terlebih dahulu web software atau biasa disebut Browser. Pada step/tahap ini user/pengguna akan membuka web Universitas/Kampus masing-masing dengan domain ac.id.
2. Selanjutnya pengguna akan diarahkan untuk mengisi halaman web login yang berguna untuk dapat mengakses halaman Web Mahasiswa mereka secara Online. Beberapa syarat yang sering sekali yang dapat digunakan untuk login ke halaman web mahasiswa mereka yakni dengan menggunakan Nomor Induk Mahasiswa (NIM) dan Password yang biasanya sudah tersedia/sudah ditentukan dari Kampus/Universitas.
3. Tahap selanjutnya yakni user/pengguna akan mendapatkan berupa Kode OTP yang akan secara langsung dikirimkan melalui SMS yang dimana nomor yang dikirimkan kode OTP tersebut sudah terdaftarkan pada Tab Data Pribadi di Halaman Web User/Mahasiswa.
4. Selanjutnya setelah mereka mendapatkan kode OTP tersebut melalui SMS, sistem akan

melakukan verifikasi apakah kode OTP tersebut benar atau tidak. Jika Benar, maka Pengguna/User akan langsung ditujukan menuju halaman Web Mahasiswa mereka. Jika Salah, maka secara otomatis tampilan web menunjukkan penolakan dan akan secara otomatis Pengguna/User harus mengulang step dari awal yakni mulai dari mengisi Nomor Induk Mahasiswa dan Password guna mengamankan akun pengguna.[7]

B. Use Case Diagram

Use Case Diagram biasa digunakan untuk memodelkan proses kebiasaan berdasarkan perspektif pengguna sistem. *Use Case Diagram* sendiri terdiri atas diagram untuk *Use Case* yang meliputi *use case login,* yakni menambahkan aktivitas favorit pengguna,mencari informasi tentang tanggal lahir pengguna,mencari makanan kesukaan pengguna dan hobi dari si pengguna itu sendiri. *Use Case Diagram* dapat dilihat pada Gambar 4.



Gambar 4.Use Case Diagram

Pada *use case* yang terdapat pada Gambar 4, hanya terdapat satu actor yakni *user,* serta beberapa fungsionalitas dari *user* dan sistem. Berikut adalah beberapa deskripsi dari masing-masing fungsionalitas yang terdapat pada Gambar 4.

1. Fungsionalitas *Login,* pada fungsionalitas ini user pertama kali memasukkan username dan password dan mengklik tombol Login yang berfungsi sebagai trigger untuk masuk ke dalam sistem.
2. Fungsionalitas Menambah Aktivitas Favorit, pada fungsionalitas ini user dapat menambah aktivitas favorit yang bertujuan untuk menentukan kegiatan yang sering dilakukan ketika mengakses web login mahasiswa.
3. Fungsionalitas Mencari Data Pribadi, pada fungsionalitas ini user mencari/menambahkan

data pribadi mereka kedalam halaman web mahasiswa.

C. Rumus Perhitungan

Proses yang dapat menghasilkan *password* sekali pemakaian dapat menggunakan Algoritma *Time-Based One Time Password* (TOTP) yang dimana dapat menggunakan suatu perhitungan yang ditumjukkan pada persamaan.

$$TOTP = HMAC(K, T)$$

Yang dimana :

TOTP ***:*** *Time-Based One Time Password.*

HMAC ***:*** *Keyed-hash Message Authentication Code merupakan suatu/sebuah fungsi kriptografi yang dikombinasikan dengan secret key.*

K(Secret Key): *Sebuah kode rahasia yang diambil dari serial number token virtual dan disimpan pada sisi server juga client.*

T = *adalah jumlah time-steps antara inisial counter T0 dengan waktu saat ini (current time)*

Untuk menghitung T dapat menggunakan persamaan.

$$T = currentTime(now) – T0/X$$

Yang dimana :

Unix time(now) *: waktu saat ini (current time)*

T0 : *waktu awal untuk menghitung timesteps secara default di inisialisasi dengan nilai = 0.*

X : *time step dengan inisialisasi = 30 detik.*

Pada proses perhitungan Algoritma *Keyed-Hash Message Authentication Code* (HMAC) dapat menggunakan persamaan.

$$HMAC = SHA256 (K + 0x5c5c)... | SHA256 (K + 0x5c5c)... |$$

Yang dimana :

K : Secret Key

0x5c5c : nilai hexadecimal dari waktu.

IV. KESIMPULAN

Pada hasil analisis yang telah penulis temukan yakni pengamanan web login mahasiswa menggunakan algoritma Two-Factor Time-Based One Time Password dapat mengurangi terjadinya pencurian data yang bersifat pribadi pada web login mahasiswa/mahasiswi.Dengan mengandalkan kode OTP yang akan dikirim melalui SMS, setiap aktivitas login yang dilakukan akan secara otomatis dimintai kode OTP tersebut yang dimana, kode OTP tersebut akan dikirim melalui SMS lewat ponsel Mahasiswa/Mahasiswi tersebut.Hal ini dilakukan yang bertujuan agar informasi dan data pribadi Mahasiswa/Mahasiswi tidak bocor/diketahui oleh orang yang tidak dikenal/tidak berhak mengakses informasi tesebut.

V. REFERENSI

[1] T. Wijaya and D. Purwanti, "Sistem Two-Factor Authentication Dengan Algoritma Time-Based One-Time Password Pada Aplikasi Web Menggunakan," *Mahasiswa.Dinus.Ac.Id*, no. x, pp. 1–7, 2012.

[2] P. Smp and N. Tangerang, "IMPLEMENTASI KEAMANAN LOGIN DENGAN METODE ONE TIME PASSWORD (OTP) MENGGUNAKAN FUNGSI HASH ALGORITMA SHA-512," vol. 1, no. 1, pp. 335–339, 2018.

[3] U. Ungkawa, I. A. Dewi, and K. R. Putra, "Implementasi Algoritma Time-Based One Time Password Dalam Otentikasi Token Internet Banking," *Tek. Inform. Fak. Teknol. Ind. Inst. Teknol. Nas. Bandung*, pp. 2–11, 2013.

[4] M. Penelitian, "SISTEM PENILAIAN ONLINE MENGGUNAKAN KEAMANAN ONE TIME PASSWORD DENGAN ALGORITMA SHA 512 BERBASIS WEB," vol. 1, no. 3, pp. 938–943, 2018.

[5] A. Prayogo *et al.*, "Implementasi One Time Password pada Sistem Login dengan Algoritma SHA-256 dan DES pada Aplikasi EO Blucampus Berbasis Client," vol. 1, no. 2, 2018.

[6] H. Lase, F. T. Informasi, U. B. Luhur, P. Utara, K. Lama, and S. H. Algorithm, "IMPLEMENTASI ONE TIME PASSWORD (OTP) MOBILE TOKEN DENGAN

MENGGUNAKAN METODE ALGORITMA MD5 DAN SHA,” vol. 1, no. 1, pp. 153–158, 2018.