

## **KEAMANAN AKUN WEB DENGAN TIME BASED ONE TIME PASSWORD**

**Ummul Khair<sup>1</sup>, Arief Budiman<sup>2</sup>, Calvin Chiuloto<sup>3</sup>**

<sup>1234</sup>Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan

e-mail: <sup>1</sup>ummulkhair@unhar.ac.id, <sup>2</sup>ariefbudiman@unhar.ac.id,  
<sup>3</sup>kalvinchiuloto@unhar.ac.id

### **ABSTRAK**

Pesatnya perkembangan teknologi dengan banyaknya umat manusia yang menggunakan *internet* untuk keperluan sehari-hari memberi kemudahan dalam berinteraksi dan mencari informasi menjadi lebih cepat dan tepat. Sehingga kenyamanan juga terasa bagi banyak pihak yang bertransaksi, namun perlu menjadi perhatian bahwa ketika semakin menginginkan kenyamanan maka keamanan juga sangat perlu diperhatikan. Karena kenyamanan berbanding terbalik dengan keamanan, semakin pengguna menginginkan kenyamanan maka pengguna juga harus memperhatikan keamanannya. Penggunaan *internet* dalam keseharian menjadi hal yang umum sekarang, sehingga penggunaan *password* untuk keamanan suatu akun menjadi suatu keharusan. Beberapa situs di *internet* yang banyak digunakan menggunakan keamanan berupa *password* untuk akun. *Time-Based One-Time Password (TOTP)* merupakan salah satu cara dalam menggunakan *password* untuk keamanan suatu *web*. Dengan menggunakan *TOTP* maka akan sulit dilakukan pencurian karena *password* akan dikirim *real time* setiap akan masuk ke halaman *web*.

**Kata kunci:** *Time-Based One-Time Password, Smartphone Android, Web*

### **ABSTRACT**

*The rapid development of technology with the large number of people using the internet for daily needs makes it easier to interact and search for information more quickly and precisely. So that comfort is also felt by many parties making transactions, but it needs to be taken into account that when you increasingly want comfort, security also really needs to be considered. Because comfort is inversely proportional to security, the more users want comfort, the more users must pay attention to security. Using the internet in everyday life has become commonplace now, so using a password to secure an account has become a necessity. Several sites on the internet that are widely used use security in the form of passwords for accounts. Time-Based One-Time Password (TOTP) is one way to use passwords for web security. By using TOTP, it will be difficult to steal because the password will be sent in real time every time you enter a web page.*

**Keywords:** *Time-Based One-Time Password, Smartphone Android, Web*

## 1. PENDAHULUAN

Pesatnya perkembangan teknologi dengan banyaknya pengguna yang menggunakan internet untuk keperluan sehari-hari memberi kemudahan dalam berinteraksi dan mencari informasi menjadi lebih cepat dan tepat. Sehingga kenyamanan juga terasa bagi banyak pihak yang bertransaksi, namun perlu menjadi perhatian bahwa ketika semakin menginginkan kenyamanan maka keamanan juga sangat perlu diperhatikan. Karena kenyamanan berbanding terbalik dengan keamanan, semakin pengguna menginginkan kenyamanan maka juga harus memperhatikan keamanannya.

Penggunaan internet dalam keseharian menjadi hal yang umum sekarang, sehingga penggunaan password untuk keamanan suatu akun menjadi suatu keharusan. Beberapa situs di internet yang banyak digunakan menggunakan keamanan berupa password untuk akun. Misalnya sosial media, toko online dan web penyedia unduh game, video maupun aplikasi. Namun pencurian password kerap dilakukan oleh oknum-oknum yang tidak bertanggung jawab untuk mendapatkan keuntungan. Pencurian password dapat dilakukan dengan banyak metode seperti keylogger, sniffing, phishing, akses wifi umum, snooping saat password diketikkan, atau menebak password menggunakan data umum seperti alamat rumah, tanggal kelahiran atau nama keluarga.

Time-Based One-Time Password (TOTP) merupakan salah satu cara dalam menggunakan password untuk keamanan suatu web. Dengan menggunakan TOTP maka akan sulit dilakukan pencurian karena password akan dikirim real time setiap akan masuk ke halaman web. Dalam proses yang akan digunakan dalam penelitian ini adalah sebuah web yang menggunakan teknologi Time-Based One-Time Password (TOTP) kemudian ada aplikasi android yang akan mengolah dan memberi password pada pengguna. Sehingga aplikasi android akan dijadikan sebagai token yang mengolah data password yang akan digunakan untuk login pada halaman web.

TOTP adalah varian time-based dari algoritma ini, dimana nilai T, berasal dari referensi waktu dan langkah waktu, menggantikan counter C dalam perhitungan HOTP. Implementasi TOTP mungkin menggunakan fungsi HMAC-SHA-256 atau HMAC-SHA-512, berdasarkan SHA-256 atau SHA-512 [SHA2] fungsi hash, sebagai ganti fungsi HMAC-SHA-1[1].

Otentikasi Time-Based OTP melalui tunnel terkunci (TOAST) adalah sebuah aplikasi smartphone yang memperoleh seed rahasia dari server melalui tunnel terkunci-TLS/SSL, menyimpan nilai seed pada smartphone menggunakan keystroke yang dilindungi password, dan kemudian menggunakan seed untuk menghasilkan kode unik sepanjang waktu satu kali[2].

Penggunaan Time-Based One-Time Password (TOTP) ini diharapkan akan dapat membuat web lebih aman dari kasus pencurian password. Penelitian ini berfokus pada pembuatan web dilengkapi dengan Time-Based One-Time Password (TOTP) dan sebuah aplikasi android yang akan digunakan sebagai token yang mengelola password-nya dan penelitian ini akan berjudul "Pengamanan Akun Web Menggunakan Time-Based One-Time Password".

## 2. METODE PENELITIAN

Analisis sistem berikut merupakan uraian dari keseluruhan informasi seperti mengidentifikasi masalah, mengevaluasi masalah dan sebagainya. Analisis sistem dilakukan untuk membantu proses dalam perancangan dan pembuatan aplikasi dengan menggunakan algoritma Time-Based One-Time Password untuk keamanan password ketika masuk kedalam web sehingga pengamanan web dapat lebih baik. Pengguna akun akan merasa nyaman untuk melakukan login melalui perangkat apapun tanpa mengkhawatirkan keamanan perangkat tersebut, walaupun seharusnya login diperangkat yang aman.

Sistem yang dirancang merupakan sistem yang memakai keamanan dalam hal masuk atau login dalam sistem. Dalam penggunaan Time-Based pada One-Time Password yang digunakan dalam website diharapkan akan dapat menambah keamanan karena penggunaan password secara real time dapat menyulitkan para hacker dalam pencurian password sehingga keamanan akun akan ditingkatkan. Penggunaan TOTP(Time-Based One-Time Password) banyak digunakan oleh website terkenal.

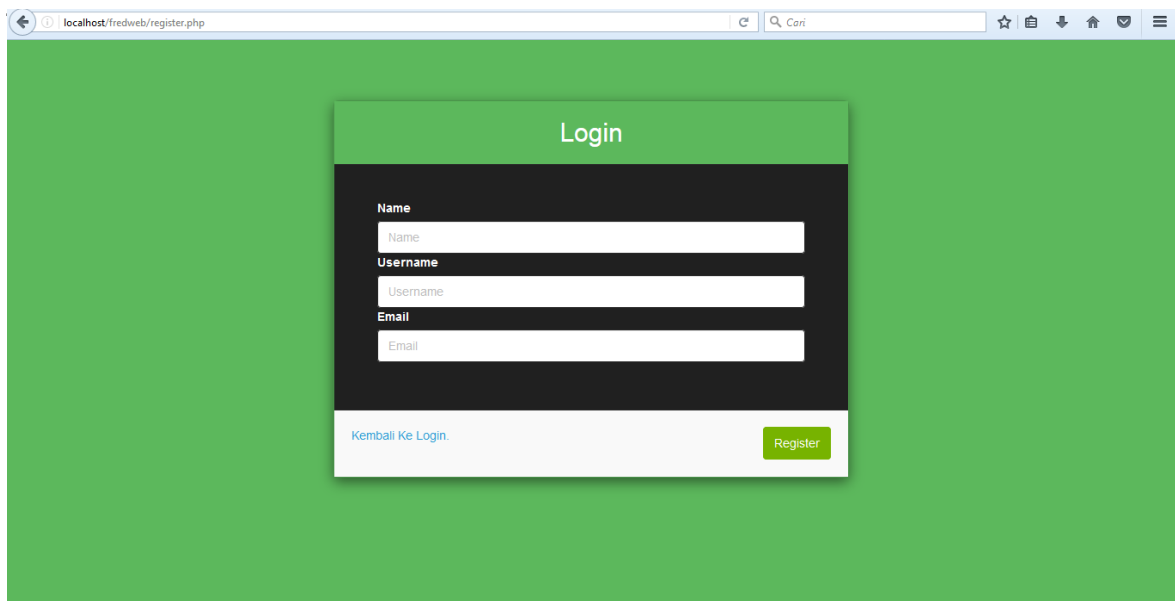
## 3. HASIL DAN PEMBAHASAN

Tahap implementasi merupakan tahapan dimana proses penggunaan aplikasi sesuai yang diinginkan setelah melewati proses perencanaan, analisis dan pembangunan aplikasi yang kemudian diuji kelayakannya untuk selanjutnya dioperasikan sebagaimana mestinya sesuai dengan fungsi dan kelayakannya. Berikut ini akan dijelaskan tentang implementasi dari analisis dan perancangan yang telah dilakukan terhadap aplikasi *Time-Based One-Time Password* adalah sebagai berikut:

### 3.1 Membuka Registrasi Website

Tahap ini merupakan tahap menjalankan *web* dan membuka *form* registrasi *user* agar *user* terdaftar didalam *web*.

.



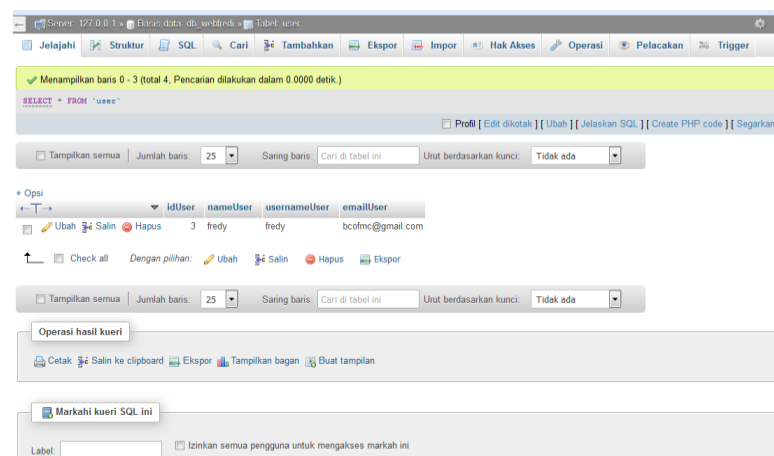
**Gambar 1. Tampilan Registrasi User**

Disini pengguna perlu mengisi *Name*, *Username* dan *Email*.

1. *Name* untuk nama lengkap sang pemilik akun.
2. *Username* sebagai *id* pengguna untuk *login*.
3. *Email* untuk *email* si pengguna, wajib diisi.

### 3.2 Tampilan Akun yang Sudah Terdaftar

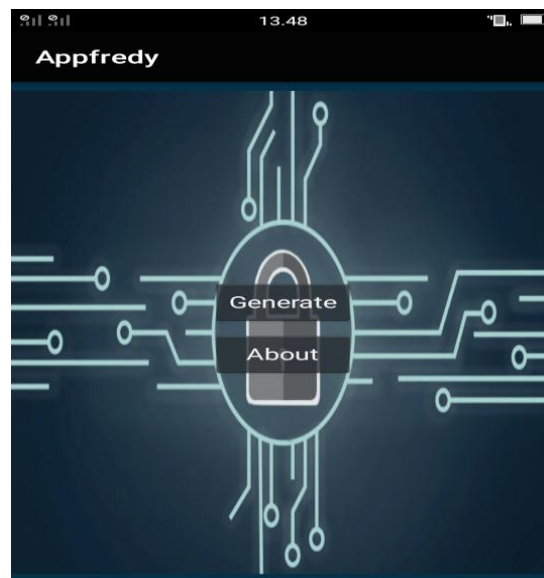
Setelah melakukan registrasi maka akun akan ditambahkan ke *database*, Akun-akun inilah yang akan diamankan menggunakan metode *Time-Based One-Time Password*.



**Gambar 2. Tampilan akun yang terdaftar di Database**

### 3.3 Membuka Aplikasi Android

Pada saat hendak *login* dibutuhkan kode *password* dan terdapat kode aktivasi. Maka selanjutnya membuka aplikasi *android* untuk mendapatkan kode *password* yang nantinya kode aktivator akan di-*generate* untuk menghasilkan kode *password*. Maka pilih opsi paling atas yaitu *Generate*.



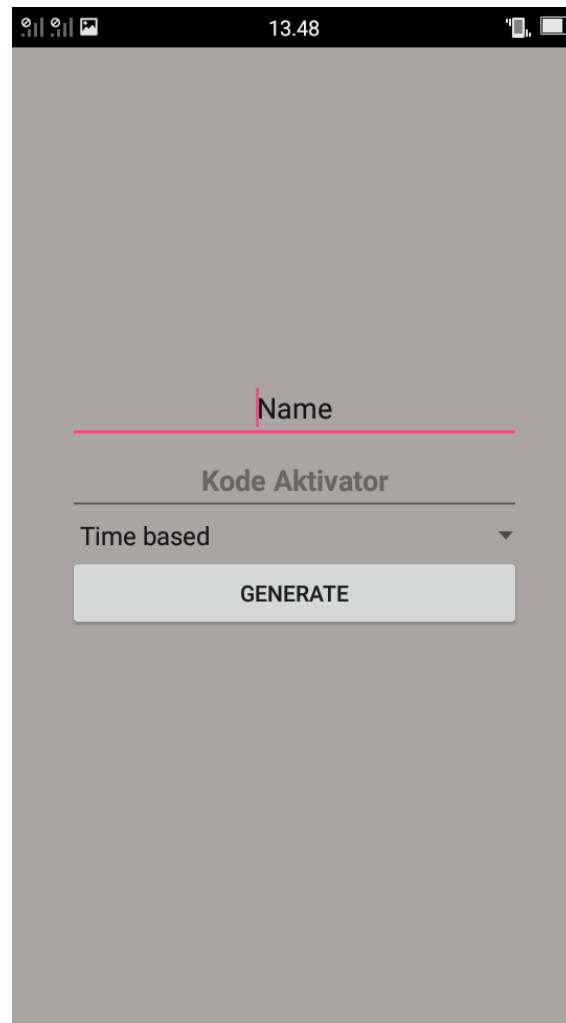
**Gambar 3. Tampilan Utama Aplikasi**

Penjelasan tampilan utama aplikasi adalah sebagai berikut:

1. *Generate* adalah opsi utama dalam aplikasi ini, yaitu opsi untuk melakukan *generate* kode aktivator untuk menghasilkan kode *password*.
2. *About* hanya merupakan tampilan *about* aplikasi.

### **3.4 Membuka Opsi *Generate***

Pada proses mendapatkan kode *password*, kode aktivator yang ada di *web* harus dimasukkan pada aplikasi *android*.

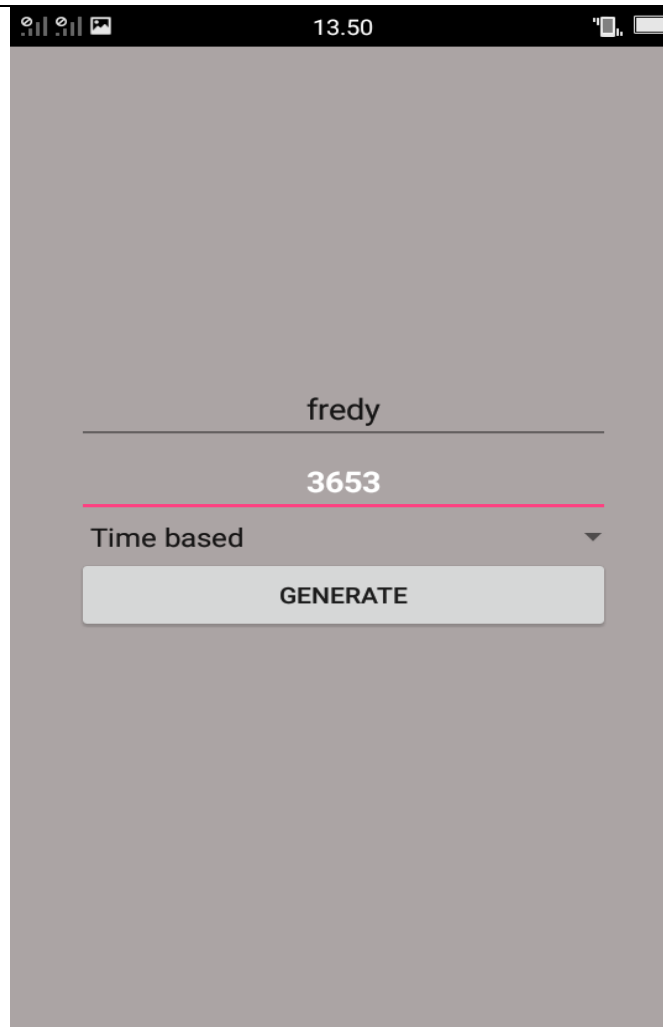


**Gambar 4. Generate Kode**

1. Pengguna memasukkan *username* pengguna pada kolom *Name*.
2. Pengguna memasukkan kode aktivator yang pada halaman *login web* ke kolom kode aktivator.
3. Pengguna menekan opsi *Generate* untuk mendapatkan kode *password*.

### **3.5 Melakukan Proses *Generate Kode Validasi***

Pengguna memasukkan *username* dan kode aktivator sebelum melakukan *generate*.



**Gambar 5. Memasukkan *username* dan kode aktivator**

Penjelasan proses memasukkan data pengguna adalah sebagai berikut:

1. Pengguna memasukkan *username* yang telah didaftarkan pada *web*.
2. Pengguna memasukkan kode aktivator yang terdapat pada halaman *login web*
3. Pengguna menekan opsi *generate* untuk mendapatkan kode *password*.

### **3.6 Hasil *Generate* Menggunakan *Time-Based One-Time Password***

Setelah memasukkan *username* dan kode aktivator, pengguna melakukan proses *generate*. Tampilan baru akan muncul, menampilkan kode *password*. Kode *password* ini yang dibutuhkan pengguna untuk *login*, kode ini akan berganti setelah 30 detik.



**Gambar 6. Hasil Generate**

Pengujian terhadap proses pengolahan *Time-Based One-Time Password* untuk menghasilkan *password* secara *real time* dan terbatas dengan waktu. Pada pengujian ini akan dilakukan dengan menggunakan rentang waktu yang berbeda. Apakah sebelum 30 detik *password* yang dihasilkan sama atau sudah berubah dan juga sebaliknya apabila setelah 30 detik *password* yang dihasil berubah atau tidak. Dan apabila lebih dari 30 detik maka *password* dapat digunakan atau tidak. Berikut ini merupakan tabel pengujian.

**Tabel 1. Pengujian *Time-Based One-Time Password***

<b>Pukul/Tanggal</b>	<b>Perangkat</b>	<b>Kode</b>	<b>Pengujian</b>	<b>Hasil</b>
13.50 / 04 Juni 2017	OPPO	3653	Masuk Aplikasi	Berhasil 069849
			Percobaan setelah 30 detik	Gagal, login tidak berhasil

#### **4. KESIMPULAN**

Setelah menyelesaikan serangkaian tahapan terhadap pembangunan aplikasi *Time-Based One-Time Password* untuk pengamanan akun *web* hingga pada tahapan pengujian, maka dapat diambil beberapa kesimpulan diantaranya adalah sebagai berikut:

1. Secara umum aplikasi yang dibangun telah bisa berjalan pada perangkat *Android* dan *browser* dengan baik.
2. Dari hasil pengujian aplikasi pada *generate* dapat menghasilkan *password* yang sesuai dengan batasan yaitu 6 digit *password*.



### **DAFTAR PUSTAKA**

- [1] M'Raihi, David, et al. 2011. *TOTP: Time-Based One-Time Password Algorithm*. Mei 2011. ISSN: 2070-1721. 685 E. Middlefield Road, Mountain View, CA 94043. Internet Engineering Task Force (IETF)
- [2] Kaur, Navpreet dan Devgan, Mandeep. 2015. *A Comparative Analysis of Various Multistep Login Authentication Mechanisms*. Oktober 2015. Volume 127 –No.9. Punjab. International Journal of Computer Applications (0975 –8887). Impact Factor (RJIF 5.72)
- [3] Sofana, Iwan. 2013. *Membangun Jaringan Komputer*. 2013. Bandung: INFORMATIKA
- [4] Riza, Muhammad. 2016. *Sistem Keamanan Jaringan Komputer*. <https://microcyber2.com/sist/em-keamanan-jaringan-komputer/>. Tanggal Akses 15/07/2017, 21:00 WIB
- [5] Rachmadi, Moch.Luthfi. 2013. *Tips Membuat Website tanpa Coding & Langsung Online*. Yogyakarta : ANDI
- [6] Yank Kevin. 2012. *PHP & MYSQL: Novice to Ninja*. 2012. USA: SitePoint Pty. Ltd
- [7] Ritonga Pahmi. 2015. *Pengertian Bahasa pemrograman PHP menurut para pakar*. <http://www.bangpahmi.com/2015/03/pengertian-bahasa-pemrograman-php.html>. Tanggal Akses 15/07/2017, 21:00 WIB
- [8] Winarno, Edi et al. 2013. *Belajar Pemrograman VB6 dalam Sekejap*. 2013. Jakarta: PT ELEX MEDIA KOMPUTINDO
- [9] Murya, Yosef dan Hesnananda, Rizki. 2014. *PROJECT PHP 15 JUTA*. : Jasakom
- [10] Adelheid, Andrea. 2013. *1 Hari Menjadi Hacker*. Jagakarsa: mediakita
- [11] Zak, Diane. 2014. *Clearly Visual Basic: Programming with Microsoft Visual Basic 2012*. 2014. USA: Course Technology
- [12] Setiawan, Hendri. 2016. *Pengertian Bahasa Pemrograman*. <http://www.hendrisetiawan.com/2016/04/pengertian-bahasa-pemrograman-munir.html>. Tanggal Akses 15/07/2017,21:00 WIB
- [13] Hariyanto, Bambang. 2014. *Esensi-esensi Bahasa Pemrograman Java*. Bandung: INFORMATIKA

- [14] Mon, Yi-Jen. 2013. *Android-based Java Programming for Mobile Phone LED Control*. Maret 2013. Taiwan. Department of Computer Science and Information Engineering, Taoyuan Innovation Institute of Technology
- [15] Bohang, Fatimah Kartini. 2016. *Evolusi OS Android, dari Versi 1.0 hingga 7.0 Nougat*. <http://tekno.kompas.com/read/2016/10/17/19480037/evolusi.os.android.dari.ver-si.1.0.hingga.7.0.nougat?page=all>. Tanggal Akses 15/07/2017, 21:00 WIB
- [16] Lee, Sunguk. 2012. *Unified Modeling Language (UML) for Database Systems and Computer Applications*. Maret 2012. Volume 5. No 1. Korea, Research Institute of Industrial Science and Technology 2016.