# Securing the Website Login System with the SHA256 Generating Method and Time-based One-time Password (TOTP)

**[1]Iman Permana, [2]Mardi Hardjianto, [3]Kiki Ahmad Baihaqi**
[1,2]Program Studi Magister Ilmu Komputer, Universitas Budi Luhur
[3]Program Studi Teknik Informatika, Universitas Buana Perjuangan Karawang
Email: iman.permana@budiluhur.ac.id

***Abstract***

*Security to enter a system has a very important role because as the main entrance to access data sources. but often lack the attention of the owners and managers of information systems. To reduce these weaknesses, one method that is widely used today is to use One-Time password, which is where the password we have becomes dynamic, meaning that at a certain time the password is always changing, the positive side is that it makes it difficult for others to steal our passwords because besides representative passwords that are difficult to understand and passwords are always changing. This study discusses One-Time Password installed on a mobile device where the password is randomized using a combination of two algorithms namely SHA256 and Time-based One Time Password. The development of this login method can reduce the level of theft of passwords owned by users who are entitled to access information sources.*

***Keywords:*** *One-Time Password, SHA256, Time-base One Time Password*

**Abstrak**

Keamanan untuk masuk kedalam sebuah sistem mempunyai peranan sangat penting karena sebagai pintu masuk utama untuk mengakses ke sumber data. tapi sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Untuk mengurangi kelemahan tersebut salah satu metode yang banyak dipakai saat ini adalah menggunakan One-Time password yaitu dimana password yang kita miliki menjadi dinamis artinya pada saat tertentu password selalu berubah-ubah, sisi positifnya yaitu mempersulit bagi orang lain untuk mencuri password kita karena selain reprenstatif password yang sulit dimengerti dan password selalu berubah-ubah. Penelitian ini membahas One-Time Password yang dipasang di perangkat mobile dimana password diacak menggunakan gabungan dua algoritma yaitu SHA256 dan Time-based One Time Password. Dengan pengembangan metode login ini dapat mengurangi tingkat pencurian terhadap password yang dimiliki pengguna yang berhak mengakses sumber informasi.
Kata Kunci: *One-Time Password, SHA256, Time-base One Time Password*

## 1. PENDAHULUAN

Banyak situs saat ini menjadikan halaman login sebagai titik masuk untuk mengakses informasi, dimana pengguna harus mengotentikasi dirinya ke situs tersebut. Ketika proses otentikasi dilakukan maka akan ada pemilahan berdasarkan hak pengguna terhadap sebuah sistem. Hal demikian dilakukan karena seharusnya hanya pengguna yang berhak saja yang boleh mengakses informasi.[1] Beberapa metode telah dikembangkan diantaranya untuk mengurangi tingkat terjadinya pencurian password oleh hacker. Pengamanan Sistem dengan metode One-Time Password (OTP) dapat menjadi salah satu solusi permasalahan tersebut, password OTP diambil dari beberapa karakter awal atau awal hasil algoritma fungsi Hash.[2]

Selain itu juga dikembangkan keamanan berlapis atau two factor authentication dengan bantuan smartphone sebagai keamanan berlapis tersebut. Upaya yang dilakukan adalah untuk memanfaatkan telepon pengguna sebagai faktor kedua kriptografi dan ada juga menggunakan security key USB sebagai keamanan faktor kedua.[3]

Penelitian yang telah dilakukan seperti SMS diperkenalkan untuk melawan phishing dan serangan lain terhadap layanan Internet dan pencurian password. Teknik ini terbukti mengurang tingkat kemungkinan password dapat dicuri oleh Hacker. Suatu pendekatan diusulkan di mana pengguna akan mengambil satu kali kata sandi melalui SMS. OTP dan PIN rahasia yang diterima diumpankan ke aplikasi seluler untuk menghasilkan transaksi kata sandi[4].

Algoritma Hash [5] dinilai cukup efektif dipergunakan untuk keperluan proses pengamanan login pengguna sistem. Dalam hal ini Algoritma hash SHA256 dinilai cukup sesuai dan aman. Karena pada algoritma hash ini tidak terdapat kemungkinan untuk terjadi collision sehingga dapat dipastikan setiap proses hashing dari data yang berbeda akan menghasilkan kode hash yang unik. Dengan demikian akan memperkuat proses pengacakan password sehingga password tidak mudah ditebak oleh Hacker. Time-based One-time Password (TOTP) akan digabungkan dengan SHA256. Dengan menggabungkan kedua otentikasi tersebut diduga dapat meningkatkan keamanan pada saat pengguna masuk ke dalam sebuah sistem.

## 2. METHODS

Dalam penelitian ini akan dibangun menggunakan metode metode pembangkit SHA256 dan Time-based One-time Password (TOTP). Pembakitan One-time Password bersifat self generated. Dimana pengguna tidak perlu memasukan challenge untuk mendapatkan password nya karena web server di buat untuk tidak mengeluarkan challenge. Pengguna hanya perlu melihat mobile aplikasinya disana akan tersedia sederetan angka yang bisa kita gunakan untuk masuk kedalam sistem website. Mobile token akan keluar secara random dalam periodik waktu tertentu. One-time Password dibangkitkan secara self generate dimana waktu saat itu sebagai parameter pembuatan One-time Password digabungkan dengan pengguna. Pemilihan metode pembangkit SHA256 berdasarkan peneletian yang dilakukan oleh Thomas and Jose [6] di dalam penelitian yang berjudul “A Comparative Study on Different Hashing Algorithms” bahwa algoritma SHA memainkan peran yang sangat penting dibandingkan dengan MD5 karena tingkat kinerja algoritma SHA relatif lebih baik.

Dalam proses implementasi sistem yang telah dibuat, dibutuhkan proses pendataan terlebih dahulu. Pendataan ini maksudnya yaitu semua pengguna sistem harus didaftarkan terlebih dahulu kedalam database yang ada disistem. Sebelum dilakukan pendataan tersebut sistem yang berbasis web harus diunggah terlebih dahulu ke sebuah web server. Serta sistem berbasis mobile dipasang pada setiap perangkat mobile/smartphone para pengguna sistem. Proses pendaftaran hanya dapat dilakukan oleh seorang yang mempunyai hak tersendiri untuk masuk kehalaman pendaftaran pengguna artinya

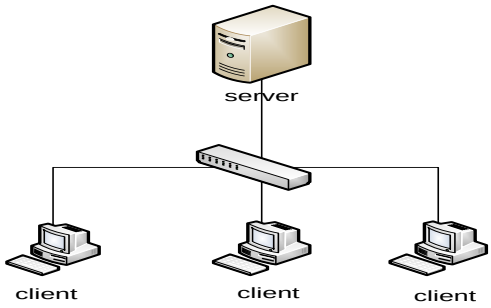
pengguna tidak dapat melakukan pendaftaran sendiri kedalam sistem. Regulasi ini diatur untuk mencegah orang-orang yang tidak berhak, masuk ke dalam sistem.

Setelah dilakukan proses pedaftaraan pada sistem maka pengguna akan mendapatkan username dan password yang telah dibuat oleh sesorang yang mempunyai hak melakukan pedaftaran pengguna sistem atau bisa disebut juga administrator dari sistem. Tetapi sistem Time-based One-time Password (TOTP)[7] tidak langsung aktif ketika administrator mendaftarkan pengguna tersebut. Dalam artian Time-based One-time Password (TOTP) tersebut dapat diakifkan dari sistem pengguna. Terdapat menu didalam tampilan pengguna ketika masuk kedalam sistem untuk mengaktifkan fasilitas TOTP. Untuk mengaktifkan Time-based One-time Password (TOTP) pengguna masuk terlebih dahulu kedalam sistem berbasis web. Menggunakan username dan password yang diberikan administrator sistem. Sistem web akan melakukan pengecekan terhadap username dan password yang dimasukan pada kolom isian username dan password. Apabila username dan password yang dimasukan cocok dengan data username dan password yang terdapat dalam database maka sistem akan mengijinkan pengguna masuk ketampilan menu utama pengguna atau sering disebut juga tampilan home.

Apabila pengguna telah masuk kedalam home maka terdapat fasilitas untuk mengaktifkan TOTP. Pengguna hanya tinggal mengklik tombol active Time-based One-time Password (TOTP) maka akan muncul sebuah QR-Code [8], QR-Code ini lah yang harus dipindai oleh pengguna menggunakan sistem berbasis mobile yang telah dipasang pengguna sebelumnya pada perangkat mobile/smartphone mereka masing-masing. Setelah berhasil memindai QR-Code maka secara otomatis sistem Time-based One-time Password (TOTP)) aktif. Yang perlu diperhatikan didalam sistem ini yaitu ketika status Time-based One-time Password (TOTP) aktif, tampilan pada halaman login sistem sama sekali tidak berubah. Maksudnya tampilan akan tetap meminta username dan password pengguna tetapi pengguna. Dalam hal ini pada saat memasukan password dengan kode OTP yang di generate oleh sistem berbasis mobile, bukan lagi menggunakan password yang diberi oleh administrator sistem sebelumnya.

Kode Time-based One-time Password (TOTP) pada sistem yang dibuat salah satunya menggunkan sebuah metode berbasis waktu. Jadi pengguna harus benar-benar memperhatikan pengaturan waktu pada perangkat mobile/smartphone yang telah dipasang sistem mobile nya. Apabila pengaturannya waktunya tidak sama dengan waktu pada web server. Maka dapat dipastikan setiap kali melakukan generate kode TOTP tidak akan dapat dipakai untuk masuk kedalam sistem berbasis web. Disebabkan oleh hasil generate antara aplikasi mobile dengan sistem web berbeda. Oleh sebab itu pengaturan waktu menjadi hal penting pada pembangunan sistem ini, karna apabila satu detik saja berbeda pada perhitungan kode OTP pun akan menghasilkan kode TOTP yang berbeda pula.

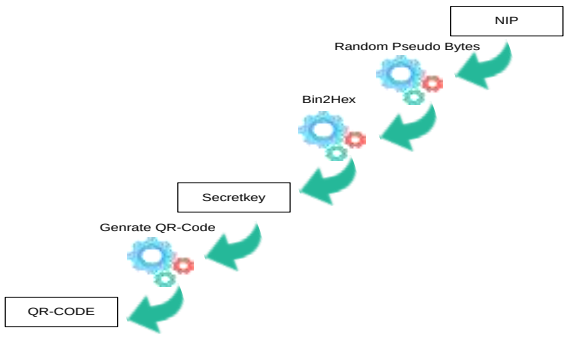
Adapun gambaran infrastruktur sistem dapat dilihat pada Gambar 1 di bawah ini, sistem berbasis web yang berjalan menggunakan metode client-server. Sistem website akan ditempatkan pada sebuah server yang akan melayani permintaan dari para client melalui sebuah jaringan.




Gambar 1. Gambaran Infrastruktur Sistem

Setiap client terhubung ke server dengan jaringan client-server maka setiap client yang terhubung dengan server akan dapat dengan mudah untuk mengakses sistem yang diletakan di server. Pengamanan yang dibuat pada sistem adalah dengan membuat otentikasi password. adapun password yang dimasukan oleh pengguna untuk masuk ke dalam sistem adalah hasil generate dari aplikasi mobile milik pengguna tersebut yang dimana akan didapatkan dengan men scan QR-code yang ditampilakan oleh sistem berbasis web.

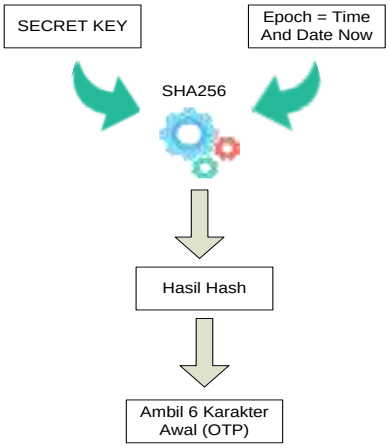
QR-code yang akan dibentuk oleh sistem website yaitu berisi secret key yang diacak menggunakan hash SHA-256, adalah gambaran tentang pembentukan QR-code.




Gambar 2. Proses Pembentukan QR-Code

Penjelasan:

1. Ambil NIP yang sedang masuk di dalam sistem
2. Buat secret key dari NIP pengguna yang telah diambil sebelumnya, kemudian lakukan random presudo byte dan Bin2Hex dan simpan hasilnya di database.
3. Tampilkan QR-Code dengan berisi secret key yang tersimpan di database.




Gambar 3. Proses Pengambilan 6 Karakter Awal OTP

Penjelasan:

1. Ambil secret key yang disimpan di mobile atau database website
2. Ambil waktu dan tanggal saat ini sesuai yang tedapat di perangkat mobile Atau Server
3. Buat kode OTP dari gabungan secret key dan waktu tanggal saat ini dan hash dengan SHA256
4. Ambil 6 digit pertama dan gunakan sebagai kode OTP untuk masuk ke sistem website.

## 3. RESULTS AND DISCUSSION

Setelah dilakukan pembuatan aplikasi website dan aplikasi mobile berdasarkan metode yang telah diusulkan, maka langkah selanjutnya yaitu adalah menguji sistem. Prose pengujian bertujuan untuk mengidetifikasi apakah aplikasi website dan aplikasi mobile yang telah dibangun telah sesuai dengan analisa kebutuhan sebelumnya. Pengujian dilakukan menggunakan skenario Sniffing. skenario Sniffing yaitu proses pemantauan dan penangkapan semua paket yang melewati jaringan tertentu menggunakan tool sniffing. Wireshark tool yang dipilih untuk melakukan skenario Sniffing ini. selain dilakukan skenario sniffing dilakukan pula pengujian brute force attack dengan bantuan software Brutus serta dilakukan survei kebutuhan waktu oleh koresponden. Pengujian-pengujian dengan dua software ini bertujuanan untuk memastikan sistem yang telah dilakukan melakukan pengamanan terhadap proses otentikasi pada aplikasi website dan pengujian waktu sebagai bahan evaluasi pemberian waktu pada sistem.

### *4.1 Sniffing password dengan wireshark*

1. Pertama membuat koneksi antara web server, client dan peretas menjadi satu network
2. Peretas Mulai Menjalankan Aplikasi Wireshark untuk melakukan proses sniffing password. dipilh interface Ethernet karna koneksi dilakukan dengan media Ethernet.
3. Client mengakses aplikasi webdosen melalui browser, client mulai memasukan NIP dan kode OTP yang di generate oleh perangkat mobile.

4. Pada langkah selanjutnya Peretas mulai menseleksi paket-paket yang ditangkap oleh Wireshark. Karena yang ingin di sniffing adalah paket http maka dilakukan filtering untuk protocol http saja.
5. Setelah mendapatkan paket yang diinginkan, untuk dapat mengetahui detail isi paket tersebut, dapat dilakukan dengan mengklik kanan pada paket kemudian pilih Follow kemudian TCP steam.
6. diketahui NIP dan Password yang dikirim oleh client adalah NIP=101010 dan Password =22d81b.
7. Setelah mengetahui data-data apa saja yang dimasukan oleh client, maka kita coba untuk login kedalam sistem menggunakan data-data yang kita dapat.
8. Setelah menekan tombol “Login”, maka akan muncul penolakan dari sistem bahwa data yang dimasukan salah.

### *4.2 Brute Force Attack Dengan Brutus*

1. Peretas Mulai Menjalankan Aplikasi Brutus.
2. Client mengakses aplikasi webdosen melalui browser, client mulai memasukan NIP dan kode OTP yang di generate oleh perangkat mobile.
3. Aplikasi Brutus mulai melakukan proses attack dengan membuka wordlist dan user file yang ada didalam aplikasi mulai mencocokan semua isi wordlist yang ada di file aplikasi.

### *4.3 Pengujian Kebutuhan Waktu Akses*

Setelah dilakukan tahapan pengujian yang dilakukan sebelumnya berupa sniffing password dengan brute force attack, dilakuan pengujian terakhir yaitu dengan melakukan survei terhadap beberapa dosen untuk melihat berapa banyak waktu yang dibutuhkan untuk mengoprasikan model sistem login yang telah dikembangkan. Hasil uji coba terhadap beberapa dosen yang mengoperasikan aplikasi dapat dilihat di Tabel dibawah ini:

| No | Nama | Fakultas | Waktu |
|---|---|---|---|
| 1 | Relawan 1 | FTI | 24.24 |
| 2 | Relawan 2 | FTI | 22.98 |
| 3 | Relawan 3 | FTI | 21.11 |
| 4 | Relawan 4 | FEB | 48.18 |
| 5 | Relawan 5 | FEB | 26.72 |
| 6 | Relawan 6 | FT | 20 |
| 7 | Relawan 7 | ASTRI | 28.67 |
| 8 | Relawan 8 | FT | 17.54 |
| 9 | Relawan 9 | FTI | 62 |
| 10 | Relawan 10 | FEB | 23.61 |
| 11 | Relawan 11 | FTI | 36.43 |
| 12 | Relawan 12 | FTI | 33.78 |
| 13 | Relawan 13 | FTI | 28.73 |
| 14 | Relawan 14 | FEB | 34.18 |
| 15 | Relawan 15 | FEB | 24.97 |
| 16 | Relawan 16 | FTI | 14.73 |

| | | | |
|---|---|---|---|
| 17 | Relawan 17 | FT | 53.33 |
| 18 | Relawan 18 | FEB | 22.58 |
| 19 | Relawan 19 | FT | 35.16 |
| 20 | Relawan 20 | FTI | 15.02 |
| Rata-rata waktu | | | **29.70** |

Dari tabel 1 dapat disimpulkan bahwa waktu rata-rata relawan dalam mengoperasikan model sister login terhadap 20 dosen dari beberapa fakultas menghasilkan rata-rata 29.70 detik.

## 4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan telah menghasilkan sebuah sistem keamanan login web mengimplementasikan One Time Password dengan mengunakan metode pembangkit SHA256 dan Time-based One Time Password (TOTP), dapat ditarik kesimpulan bahwa pengembangan ini mengurangi resiko terjadinya pencuri dikarnakan password yang selalu berubah-ubah setiap 60 detik sekali. Setelah dilakukan pengujian kemanan dari aplikasi yang telah dibuat dilakukan skenario sniffing didapatkan hasil bahwa password dapat di curi akan tetapi password tidak dapat digunakan kembali untuk melakukan akses masuk kedalam aplikasi webdosen serta pemberian waktu 60 detik dalam setiap perubahan kode dirasa cukup karena setelah dilakukan survei terhadap 20 dosen dari beberapa fakultas menghasilkan rata-rata 29.70 detik.

## REFERENCES

[1] Van,Acker et al.(2017) ‘Measuring login webpage security' Proceedings of the Symposium on Applied Computing. ISBN: 9781450344869. doi: 10.1145/3019612.3019798
[2] Virgian, D. et al. (2016) ‘Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator ( PRNG ) Linear Congruential Generator ( LCG ) di Perangkat B ... BIT VOL 13 No . 1 April 2016 ISSN : 1693-9166 Pengamanan Sistem Me’, BIT, 13(April 2017), pp. 64–73.
[3] Lang, J. et al. (2017) ‘Security keys: Practical cryptographic second factors for the modern web’, in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 422–440. doi: 10.1007/978-3-662-54970-4_25.
[4] Hamdare, S., Nagpurkar, V. and Mittal, J. (2014) ‘Securing SMS Based One Time Password Technique from Man in the Middle Attack’, 11(3), pp. 154–158.
[5] Juardi, D. (2017). KAJIAN VULNERABILITY KEAMANAN DATA DARI EKSPLOITASI HASH LENGTH EXTENSION ATTACK. incomtech, 6(1).
[6] Thomas, C. G. and Jose, R. T. (2015) ‘A Comparative Study on Different Hashing Algorithms’, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3(Special Issue 7), pp. 170–175.
[7] El-Booz, S. A., Attiya, G. and El-Fishawy, N. (2016) ‘A secure cloud storage system combining Time-based One Time Password and Automatic Blocker Protocol’, 2015 11th International Computer Engineering Conference: Today Information Society What’s Next?, ICENCO 2015. EURASIP Journal on Information Security, pp. 188–194. doi: 10.1109/ICENCO.2015.7416346.
[8] Juardi, D. (2019). Presensi dan Reminder menggunakan QR Code (Studi Kasus: SMA XXX). Systematics, 1(1), 33-43.