**JURNAL MEDIA INFORMATIKA BUDIDARMA**
**Volume 4, Nomor 4, Oktober 2020, Page 930-939**
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

# Implementasi Metode *One Time Password* pada Sistem Pemesanan *Online*

**Nani Sarah Hapsari, Yenni Fatman*, Isbandi**

Fakultas Teknik, Program Studi Teknik Informatika, Universitas Islam Nusantara, Bandung, Indonesia
Email: [1]nanisarahhapsari30@gmail.com, [2,*]yennifatman@gmail.com, [3]4isbandi@gmail.com
Email Penulis Korespondensi: [2,*]yennifatman@gmail.com

**Abstrak**−Sistem keamanan yang paling sering digunakan pada metode otentikasi adalah kata sandi (password). Adanya kemudahan dalam hal implementasi menjadi faktor utama dari pemanfaatan sistem berbasis password dan banyaknya penggunaan jaringan yang belum aman masih menjadi ancaman untuk beberapa aplikasi, contohnya pada aplikasi berbasis website pemesanan online ini. Di mana penjual harus melakukan pendaftaran terlebih dahulu untuk dapat melakukan pemesanan. Oleh karena itu, perlu adanya suatu mekanisme untuk mencegah terjadinya dampak negatif dari berbagai serangan keamanan salah satunya dengan penerapan sistem two factor authentication, dapat dibangun dengan menggunakan kombinasi username dan password serta divalidasikan kepemilikannya dengan password dinamis one time password. Salah satu metode untuk membangkitkan One Time Password (OTP) adalah Time-based One Time Password (TOTP), metode ini membangkitkan sebuah password dinamis yang berubah mengikuti suatu jeda waktu tertentu. Di mana password tersebut dihasilkan melalui proses enkripsi Secure Hash Algorithm 256 (SHA-256) dengan bantuan pseudo random number generator yang menghasilkan 6 digit nilai heksadesimal. Hasil dari pengujian sistem pada awal hingga akhir pengujian sistem yaitu penerapan skenario yang memperoleh hasil pengujian berupa output yang dihasilkan dan penilaian dengan rentang nilai sekitar 95% - 100%. Rata-rata hasil yang dicapai sukses dan sesuai berdasarkan perancangan yang dilakukan.

**Kata Kunci:** Keamanan, Pemesanan Online, Password, Username, Two Factor Authentocation, One Time Password

**Abstract**−The most commonly used security system in the authentication method is the password. The ease of implementation is a major factor in the use of password-based systems and the use of insecure networks is still a threat for some applications, for example on this online ordering website based application. Where the seller must register in advance to be able to place an order. Therefore, it is necessary to have a mechanism to prevent the negative impact of various security attacks, one of which is by implementing a two factor authentication system, it can be built using a combination of username and password and validated ownership with dynamic passwords one time password. One method for generating One Time Password (OTP) is Time-based One Time Password (TOTP), this method generates a dynamic password that changes following a specified time lag. Where the password is generated through the Secure Hash Algorithm 256 (SHA-256) encryption process with the help of a pseudo random number generator that produces a 6-digit hexadecimal value. The results of the system testing at the beginning to the end of the system testing are the application of scenarios that obtain test results in the form of outputs and assessments with a range of values around 95% - 100%. The average results achieved are successful and appropriate based on the design carried out.

**Keywords**: Security, Online Reservation, Password, Username, Two Factor Authentication, One Time Password

## 1. PENDAHULUAN

Sistem keamanan yang paling sering digunakan pada metode otentikasi adalah kata sandi (*password*). Adanya kemudahan dalam hal implementasi menjadi faktor utama dari pemanfaatan sistem berbasis *password* dan pengguna juga sudah terbiasa dengan sistem semacam ini sehingga waktu penyesuaian dapat diminimalkan. Di sisi lain, banyaknya penggunaan jaringan yang belum aman (misalnya protokol HTTP) masih menjadi ancaman bagi pengguna mengingat seringkali *password* satu-satunya mekanisme yang digunakan [1] karena keamanan menjadi perhatian utama pada era digital.

Terkadang pengguna kurang waspada terhadap *password* yang dimiliki sehingga terjadi pen-curian *password*, misalnya pemilihan *password* yang sudah umum digunakan seperti tanggal lahir, hal ini menyebabkan orang lain akan dapat dengan mudah menebak *password* yang dibuat. Pada kasus lain pengguna menuliskan *password* pada media tertulis yang kemudian secara sengaja atau tidak sengaja dapat dibaca pihak lain [2].

Selain itu, banyak metode yang sering digunakan oleh peretas untuk dapat mengetahui *username* dan *password* dari sebuah akun (*account*). Salah satu cara yang digunakan peretas untuk mengetahui informasi akun seseorang adalah *sniffing*. *Sniffing* atau dalam konteks pencurian *password* sering disebut *password sniffing* adalah suatu teknik pencurian *password* dengan bantuan perangkat lunak dengan mengambil informasi *remote login* seperti *username* dan *password* [3]. Biasanya serangan yang rentan terjadi dialami pengguna yaitu berbentuk *Cross Site Request Forgery* (CSRF) pada hak akses sistem.

Masalah lain yang juga muncul dan sering terlupakan adalah banyaknya *user* yang menggunakan perangkat yang tidak aman dalam melakukan proses *login* [4]. Beberapa contohnya yaitu melakukan suatu transaksi dan perdagangan barang secara elektronik, pelayanan (pemesanan, reservasi, *helping*, serta lainnya), dan segala bentuk informasi yang dilakukan secara elektronik. Misalnya penggunaan komputer di tempat publik seperti bandara, perpustakaan umum, dan warnet. Meskipun telah memanfaatkan jaringan yang aman sekalipun, namun *password* akan dapat terbaca oleh komputer yang telah terpasang perangkat lunak *keylogger* [4].

Semua masalah tersebut tentunya dapat diatasi dengan berbagai cara, salah satunya dengan menggunakan *Two Factor Autentication* (TFA) atau secara umum dikenal sebagai faktor otentifikasi merupakan sistem


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
**Volume 4, Nomor 4, Oktober 2020, Page 930-939**
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

keamanan yang terdapat di beberapa aplikasi yang umum diketahui dan dapat digunakan berdasarkan dengan kebutuhan penggunanya.

*Two Factor Authentication* ( TFA) merupakan sebuah metode otentikasi pengguna di mana dua faktor (dari empat metode otentikasi) yang bersifat independen akan digunakan dalam membuktikan adanya pernyataan bahwa sebuah entitas atau identitas itu asli. Dengan menggunakan TFA, maka *password* bukanlah menjadi *single point of attack* dalam hal akses kepada identitas pengguna [5]. Banyak perusahaan besar yang telah mulai menggunakan TFA sebagai tambahan pengamanan terhadap serangan *brute-force* terhadap *password*, seperti Instagram, Facebook, Google, Twitter, dan beberapa Brand E-Commerce.

Di era digital ini, khalayak ramai sudah tidak ingin direpotkan dengan antrian yang panjang ketika melakukan pembelian di suatu toko atau tempat-tempat pembelian yang bersifat umum seperti halnya untuk membeli 2 sampai 5 porsi makanan di suatu kedai, bahkan bisa langsung diantarkan ke rumah pembelinya. Maka, wujud dari penerapan Metode *One Time Password* (OTP) yaitu pada suatu sistem berbasis website adalah aplikasi e-commerce dalam bidang kuliner mie ayam, di mana hal tersebut diterapkan pada fitur pemesanan makanan secara *online* (*online reservation*) untuk menghindari antrian yang panjang di tempat pembelian dan mempermudah pengguna dalam melakukan pemesanan dengan ketentuan bahwa pengguna diharuskan melakukan registrasi atau *login* terlebih dahulu untuk dapat menggunakan fitur pemesanan dan pembayaran hanya dapat dilakukan secara langsung ketika sampai di tempat. Dengan tujuan untuk memastikan apakah pengguna adalah pemilik akun tersebut, dengan orang yang sama, dan sungguh-sungguh melakukan pembelian ataukah hanya menunjukkan kepemilikan akun saja.

Pada sistem ini, yang difokuskan pada fungsi pemesanan makanan, data (*username*, *email*, *password*) menjadi sesuatu yang sangat privasi bagi pemilik akun karena tinggi-nya jumlah pengguna yang terbiasa dengan situs *online* terutama dalam bidang perbelanjaan sehingga bagaimanapun bentuk data yang digunakan, banyak sedikitnya data yang dikelola oleh aplikasi, tentunya haruslah terjaga keamanannya. Hal ini menerapkan suatu konsep sistem keamanan informasi [6].

*Two Factor Authentication* dengan menggabungkan 2 metode otentikasi yaitu *Something You Know* (*password* statis atau *password* milik pengguna pribadi) dengan *Something You Have* (token *hardware* atau sebuah alat dengan bentuk fisik yang dimiliki seperti ponsel yang mampu meng-hasilkan deret kode yang berubah-ubah), hal tersebut sudah diterapkan pada algoritma TOTP.

Di mana sistem *two factor authentication* dapat dibangun dengan menggunakan kombinasi *username* dan *password* serta divalidasikan kepemilikannya dengan *password* dinamis *one time password*. Salah satu metode untuk membangkitkan *one-time password* adalah *Time-based One Time Password* (TOTP), metode ini membangkitkan sebuah *password* dinamis yang berubah mengikuti suatu jeda waktu tertentu [5].

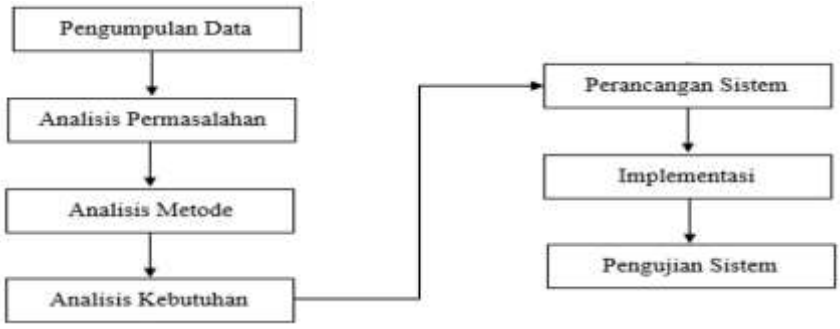
Penelitian mengenai Metode OTP yang dilakukan, terdiri dari beberapa kasus antara lain dalam implementasi terhadap keamanan e-commerce dan token *hardware* [5], [4], penarikan uang di ibank [7], [8], [9], verifikasi dokumen [10], [11]. Selain itu adapun peneliti yang menggunakan algoritma *secure hash* sebagai keamanan kode di beberapa kasus di antaranya pada penerapan untuk nilai suatu citra [12], [13], [14], dan sistem *login* di aplikasi suatu lembaga [3], [2], [15], [16], [17], dan [18].

## 2. METODOLOGI PENELITIAN

### 2.1 Tahapan Penelitian

Metode yang digunakan untuk menyelesaikan penelitian ini adalah menggunakan penelitian kualitatif. Menurut Bogdan dan Bikle, S. (1992: 21-22) menjelaskan bahwa penelitian kualitatif adalah salah satu prosedur penelitian yang menghasilkan data deskriptif berupa ucapan atau tulisan dan perilaku orang-orang yang diamati [19].

Pada penelitian ini menggunakan metode deskriptif karena menggambarkan, mendeskripsikan, menjelaskan secara sistematis *One Time Password* dan bagian-bagian digunakan dalam proses membangun suatu sistem. Berikut ini adalah langkah-langkah atau tahapan penelitian kualitatif yang dilakukan berdasarkan diagram ilmiah, dapat dilihat seperti pada gambar berikut ini:




**Gambar 1.** Tahapan Penelitian


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 930-939
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

Pada kegiatan pengumpulan data terdiri dari 2 yaitu studi literatur, di mana peneliti mempelajari data dari buku-buku, karya ilmiah, jurnal ilmiah, artikel, dan sumber internet selanjutnya studi lapangan di antaranya observasi, *focus group discussion*, dan dokumentasi. Dalam pembangunan sistem atau perangkat lunak, diperlukannya suatu analisis kebutuhan di mana perancangan sistem pemesanan *online* menggunakan Metode *Waterfall*. Tahap selanjutnya yaitu perancangan dilakukan untuk memberikan gambaran umum dari permasalahan yang ada. Proses perancangan pada sistem ini menggunakan UML (*Unified Modelling Language*) sebagai *modeling tools* untuk membantu menggambarkan rancangan sistem yang akan dibuat. Implentasi metode terletak pada proses ketika *user* akan *login* pada aplikasi pemesanan ini. Tahap terakhir yaitu Pengujian Sistem yang mengguna-kan Pengujian *Black Box*, berfokus pada persyaratan secara fungsional perangkat lunak.

### 2.2 *One Time Password*

*One Time Password* terdiri dari 2 kategori besar, yaitu HOTP (HMAC-*based* OTP) dan TOTP (Time-*based* OTP). *One Time Password* (OTP) yang disebut dengan istilah sandi sekali pakai, biasanya digunakan untuk transaksi *online* atau pendaftaran sebuah akun. Kode OTP terdiri dari kombinasi nomor unik dan rahasia yang diperoleh secara acak di mana kode OTP dimaksudkan untuk keamanan dan OTP dianggap lebih aman karena perubahan *password* secara terus-menerus.

Metode *One Time Password* adalah kata sandi yang valid (absah) dan dapat digunakan hanya untuk satu kali sesi *login* atau transaksi saja pada komputer atau alat digital lainnya. OTP biasanya digunakan sebagai mekanisme otentikasi tambahan untuk itu OTP sering disebut sebagai dua faktor otentikasi (*two-factor authentication* atau *second factor authentication*) [9]. Adanya mekanisme otentikasi ini dapat dibangun dengan menggunakan kombinasi *username* dan *password* serta divalidasikan kepemilikannya dengan *password* dinamis yaitu *one-time password*.

Mekanisme otentikasi bertujuan membuktikan kebenaran dan keaslian data pengguna dalam menggunakan sistem. Berikut, beberapa mekanisme otentikasi untuk membuktikan hal tersebut yaitu *something you know, something you have, something you are,* dan *something you can* [8].

### 2.3 *Two Factor Authentication*

*Two-Factor Authentication* merupakan sebuah metode otentikasi pengguna di mana dua faktor (dari empat) yang bersifat independen akan digunakan dalam membuktikan adanya klaim bahwa sebuah entitas atau identitas itu asli. Penggunaan *Two-Factor Authentication* akan dapat meng-urangi resiko seorang *adversary* dapat masuk ke sebuah sistem dengan menggunakan identitas pribadi individu karena selain harus mengetahui *password* yang kita gunakan, *adversary* juga harus mendapatkan informasi kedua yang bisa dihasilkan dari sumber yang berbeda [7].

Pada kebanyakan sistem yang ada saat ini digunakan kombinasi antara *username* atau *password* dan juga kode OTP (*One-Time Password*) yang dikirimkan melalui SMS ke perangkat digital (*smartphone*/tablet) atau dihasilkan melalui aplikasi pihak ketiga, misalnya Google *Authenticator* atau *Authy*. Salah satu kelemahan utama dari penggunaan OTP adalah rentan terhadap serangan *Phising* dan *Man-in-the-middle-Attack* [7].

### 2.4 *Secure Hash Algorithm* 256

Algoritma SHA-256 merupakan algoritma *hash* dari jenis SHA-2 yang menghasilkan *message digest* sepanjang 256 bit. Algoritma SHA-256 dapat digunakan untuk melakukan pengecekan integritas data, pembuatan *digital signature* [20].

Prinsip Dasar SHA-256 yaitu pembuatan *message digest* didasarkan pada pesan dengan panjang maksimum 256 bit, menggunakan *message schedule* yang terdiri dari 64 elemen kata 32 bit, 8 buah variabel 32 bit, dan variabel penyimpan nilai hash 8 buah kata 32 bit, serta hasil akhir didapat *message digest* sepanjang 256 bit [20]. Lebih jelasnya dapat dilihat pada perhitungan Algoritma Matematika di bawah ini [12]:

*a.* Penambahan Bit *Padding*

Sebelum menerapkan Algoritma SHA-256 dilakukan terlebih dahulu penyesuaian input berupa bilangan biner yaitu pengubahan pesan ke bentuk biner. Diketahui pesan atau *string* yang dimasukan pada sistem pemesanan ini biasa berbentuk penggabungan antara *username* dan *password* pada saat melakukan *login* sebagai *user*. Data yang digunakan pada perhitungan ini menggunakan data secara acak dan dapat dilihat pada Tabel 1 merupakan nilai pesan atau *string* yang berbentuk biner dan sudah diurutkan berdasarkan posisi biner.

**Tabel 1.** Nilai Pesan

| PESAN | BINER |
|---|---|
| N | 00010111 |
| A | 00001010 |
| N | 00010111 |
| I | 00010010 |
| 3 | 00000011 |
| 7 | 00000111 |


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 930-939
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

Dari tabel 4 di atas diketahui bahwa panjang M=48 bit. Proses berikutnya adalah dengan menambahkan *padding* bit 1 dan sisanya 0 sejumlah k, dengan persamaan sebagai berikut :
k=l+1=448 mod 512
k=48+1=448 mod 512
k=49=448 mod 512
k=448-49=399, maka banyaknya *padding* bit '0' yang ditambahkan yaitu 399.

b. Panjang *Append*
Penambahan panjang *append* dilakukan dengan penambahan panjang pesan sebanyak 64 bit di akhir. Panjang pesan adalah 48 bit

c. Panjang *Append*
Pada kasus ini panjang pesan tidak lebih dari 512 sehingga hanya menghasilkan 1 blok 512 bit yaitu M(0). Tahap selanjutnya adalah melakukan parsing pesan dengan membagi setiap blok 512 bit menjadi 16 blok berukuran 32 bit.

d. Inisialisasi Nilai *Hash*
Setelah proses parsing pesan maka langkah selanjutnya adalah inisialisasi nilai *hash* di mana nilai ini merupakan sebuah ketentuan yaitu:

**Tabel 2.** Initial *Hash Value*

| Variabel | *Hash Value* | *Initial* |
|---|---|---|
| $H_0^{(0)}$ | 6A09E667 | a |
| $H1^{(0)}$ | BB67EA85 | b |
| $H2^{(0)}$ | 3C6EF372 | c |
| $H3^{(0)}$ | A54FF53A | d |
| $H4^{(0)}$ | 510E527F | e |
| $H5^{(0)}$ | 9B05688C | f |
| $H6^{(0)}$ | 1F83D9AB | g |
| $H7^{(0)}$ | 5BE0CD19 | h |

Setelah diketahui *initial hash value*, kemudian diperoleh juga nilai K yang berasal dari konstanta SHA-256 dan nilai K terdiri dari K0 – K63.

e. Penjadwalan Pesan
Kemudian dilakukan proses penjadwalan pesan, pada langkah ini diawali dengan mengubah setiap blok pesan menjadi bilangan heksadesimal dengan ketentuan sebagai berikut :

$$Wt \begin{cases} Mt^{(i)} & 0 \le t \le 15 \\ \sigma_1^{(256)}(W_{t-2}) + (W_{t-7}) + \sigma_0^{(256)}(W_{t-15}) + (W_{t-16}) & 16 \le t \le 63 \end{cases} \quad (1)$$

Di mana :
$\sigma 1(256)(Wi{-}2) = ((Wi{-}2\ )ROTR\ 17) \oplus ((Wi{-}2\ )ROTR\ 19) \oplus ((Wi{-}2\ )SHR10)$
$\sigma 1(256)(Wi{-}15) = ((Wi{-}15)ROTR\ 7) \oplus ((Wi{-}15)ROTR\ 18) \oplus ((Wi{-}15)SHR3)$
Keterangan :
- Wt = Blok Pesan yang Baru
- Mt = Blok Pesan yang Lama
- Wi-2 = Blok Pesan dari W ke i-2
- Wi-15 = Blok Pesan dari W ke i-15
- ROT R = *Rotate Right*
- SH R = *Shift Right*
- $\oplus$ = Operator XOR

Pada Tabel 3 merupakan penjadwalan pesan yang dilakukan pada saaat ketika W0 sampai W23.

**Tabel 3.** Penjadwalan Pesan

| | | | |
|---|---|---|---|
| 17011749 | 03078000 | 00000000 | 00000000 |
| 00000000 | 00000000 | 00000000 | 00000000 |
| 00000000 | 00000000 | 00000000 | 00000000 |
| 00000000 | 00000000 | 00000000 | 00000030 |
| 00000000 | 00000000 | 00000000 | 00000000 |
| 00000000 | 00000000 | 00000000 | 00000000 |

f. Penjadwalan Pesan
Selanjutnya melakukan inisialisasi variabel kerja a, b, c, d, e, f, g dan h di mana setiap variabel diambil dari initial *hash value* a=H0 (0), b=H1 (0), c=H2 (0), d=H3 (0), e=H4 (0), f=H5 (0), g=H6 (0), h=H7 (0). Selanjutnya dilakukan proses komputasi fungsi *hash* SHA-256 dari t=0 - t=63. Namun dalam perhitungan ini hanya sampai t=0 hingga t=2.

Pada Tabel 4 diketahui t=0 sampai t=3 masing-masing mempunyai nilai, untuk mengetahui nilai a maka dilakukan perhitungan komputasi fungsi *hash* dan dapat dilihat pada Tabel 4.


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 930-939
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

**Tabel 4.** Proses Komputasi Fungsi *Hash* SHA-256

| | a | b | c | d | E | f | g | h |
|---|---|---|---|---|---|---|---|---|
| **Init** | 6a09 | bb67 | 3c6e | a54f | 510e | 9b05 | 1f83 | 5be0 |
| | e667 | ae85 | f372 | f53a | 527f | 688c | d9ab | cd19 |
| **t=0** | 0200 | 6a09 | bb67 | 3c6e | 0000 | 510e | 9b05 | 1f83 |
| | 0000 | e667 | ae85 | f372 | 0000 | 527f | 688c | d9ab |
| **t=1** | 0000 | 0200 | 6a09 | bb67 | 0000 | 0000 | 510e | 9b05 |
| | 0000 | 0000 | e667 | ae85 | 0000 | 0000 | 527f | 688c |
| **t=2** | 0000 | 0000 | 0200 | 6a09 | 0000 | 0000 | 0200 | 510e |
| | 0000 | 0000 | 0000 | e667 | 0000 | 0000 | 0000 | 527f |
| **t=3** | 0000 | 0000 | 0000 | 0200 | 0000 | 0000 | 0000 | 0200 |
| | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 |

g. Penjumlahan Hasil Akhir
Ketika proses komputasi sudah mencapai titik t=63 maka jumlahkan dengan initial hash value di titik tersebut. Namun dalam penjumlahan berikut variabel kerja menggunakan ketika fungsi hash berada di titik t=1, yang memungkinkan hasilnya tidak keseluruhan 0.

**Tabel 5.** Penjumlahan *Initial Hash Value*

| Variabel | *Hash Value* | | Variabel Kerja | Hasil |
|---|---|---|---|---|
| $\mathbf{H_0^{(0)}}$ | 6A09E667 | + | 00000000 | 00000000 |
| **H1(0)** | BB67EA85 | + | 02000000 | 02000000 |
| **H2(0)** | 3C6EF372 | + | 6A09E667 | 2808E262 |
| **H3(0)** | A54FF53A | + | BB67EA85 | A147A400 |
| **H4(0)** | 510E527F | + | 00000000 | 00000000 |
| **H5(0)** | 9B05688C | + | 00000000 | 00000000 |
| **H6(0)** | 1F83D9AB | + | 510e527f | 1102502B |
| **H7(0)** | 5BE0CD19 | + | 9b05688c | 1B004808 |

h. Keluaran atau *Output* yang Didapatkan
*Output* dari SHA-256 merupakan penggabungan dari H0(0) sampai H7(0) sebagai berikut :
00000000 || 02000000 || 2808E262 || A147A400 || 00000000 || 00000000 || 1102502B || 1B004808

Sehingga didapat nilai *hash* dari pesan M adalah, sebagai berikut :
00000000020000002808E262A147 A400000000000000000001102502B1B004808.

### 2.5 *Pseudo Random Number Generator*

Pembangkit Bilangan Acak adalah suatu metode yang dirancang untuk menghasilkan suatu urutan nilai yang tidak dapat ditebak polanya dengan mudah, sehingga urutan nilai tersebut dapat dianggap sebagai suatu keadaan acak (*random*). *Pseudo Random Number Generator* (PRNG) atau Pembangkit Bilangan Acak Semu merupakan suatu algoritma yang menghasilkan suatu urutan nilai yang setiap hasil nilainya bergantung pada nilai yang dihasilkan sebelumnya [1]. Salah satu cara yang dijadikan sebagai upaya peningkatan data yang bersifat privasi [21].

## 3. HASIL DAN PEMBAHASAN

Berikut ini merupakan hasil dan pembahasan berdasarkan penelitian yang dilakukan, antara lain:

### 3.1 Pengujian Sistem

Pengujian sistem pemesanan ini menggunakan Metode Pengujian Black Box. Pengujian black box ini berfokus pada persyaratan secara fungsional perangkat lunak. *Blackbox Testing* juga memungkinkan pengembang *software* untuk membuat himpunan kondisi input yang akan seluruh syarat-syarat fungsionalitas sistem.

1. Pengujian Fungsionalitas *Login* Pemesanan *Online*
Pengujian ini dilakukan untuk mengetahui keabsahan akun yang digunakan oleh pembeli untuk melakukan pemesanan makanan.

**Tabel 6.** Pengujian Fungsionalitas *Login*

| No. | Skenario Pengujian | Hasil yang Diharapkan | Hasil Pengujian | Kesimpulan |
|---|---|---|---|---|
| 1. | Registrasi Pembeli (nama, alamat email, | Data yang digunakan pada *form* registrasi berhasil dimasukkan dan dapat | Sukses Registrasi | Registrasi dapat dilakukan sesuai dengan yang diharapkan. |


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
**Volume 4, Nomor 4, Oktober 2020, Page 930-939**
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

| No. | Skenario Pengujian | Hasil yang Diharapkan | Hasil Pengujian | Kesimpulan |
|---|---|---|---|---|
| | *password*, *confirm password*) | digunakan kembali ketika *login* untuk kedua kalinya. | | |
| 2. | *Login* Pembeli (nama, alamat email, *password*) | Data yang dimasukan berhasil dan apabila terjadi kesamaan email dan lupa *password* diberikan notifikasi. | Sukses *Login* Pembeli | *Login* dapat dilakukan berdasarkan data pada saat registrasi. |
| 3. | *Two Factor Authentication* | Kode yang diperoleh melalui email dalam rentang waktu yang diberikan. | Sukses Memperoleh Kode | Email yang digunakan valid dan benar milik pengguna. |
| 4. | *Login Administrator* (alamat email dan *password*) | Data yang dimasukan sesuai dan tidak harus melakukan registrasi terlebih dahulu. | Sukses *Login Administrator* | Sudah bisa mengakses sistem tanpa harus melakukan pendaftaran. |
| 5. | *Generate* OTP | Bentuk kode yang diperoleh huruf dan angka, seperti 43cd07. | Sukses Tampil Kode | Kode yang ditampilkan sebanyak 6 digit. |
| 6. | *Input* Kode OTP | Kode valid akan langsung menuju halaman pemesanan. | Sukses *Input* Kode | Kode yang diperoleh untuk akses halaman pemesanan. *Input* dilakukan pada alamat ini localhost: 8000/2fa |
| 7. | *Input* Kode OTP | Kode error ketika tidak dapat akses halaman pemesanan. | Gagal *Input* Kode | Email yang digunakan tidak valid atau kode yang dimasukkan salah. |

Hasil pengujian login ini, yang dilakukan terhadap sistem melalui aplikasi pemesanan digunakan untuk memasukan data pengguna, baik itu data user sebagai pembeli dan *user* sebagai *administrator* serta data tersebut dapat digunakan kembali ketika akan melakukan pemesanan.

2. Pengujian Fungsionalitas Pemesanan *Online*

Pengujian dilakukan untuk mengetahui sejauh mana sistem dapat berjalan sesuai dengan yang diharapkan berdasar kondisi yang terjadi.

**Tabel 7.** Pengujian Fungsionalitas Pemesanan

| No. | Skenario Pengujian | Hasil yang Diharapkan | Hasil Pengujian | Kesimpulan |
|---|---|---|---|---|
| 1. | Halaman Pemesanan (kode transaksi dan nama pembeli) | Data kode transaksi dan nama pembeli tidak harus dimasukan karena sudah otomatis tampil berdasar kepemilikan akun. | Berhasil Tampil | Dapat mengisi beberapa data. |
| 2. | Halaman Pemesanan (nama makanan, jumlah pembelian, dan deskripsi) | Data pada *form* pemesanan hanya mengisi data yang kosong. | Berhasil *Input* Data | *Login* dapat dilakukan. |
| 3. | *Input* Pemesanan Makanan | Setelah data terpenuhi dan dikirim maka akan diarahkan ke halaman selanjutnya. | Berhasil *Input.* | Pemesanan dapat dilakukan. |
| 4. | Bukti Pemesanan | Data pada bukti pemesanan berdasarkan data yang masuk ketika melakukan pemesanan. | Berhasil Cetak Bukti | Bukti yang diperoleh sesuai. |
| 5. | Laporan Penjualan | Data laporan berdasarkan data yang masuk setiap harinya ketika melakukan pemesanan dengan aplikasi. | Berhasil Dibuat | Laporan sesuai dengan pemesanan per hari. |
| 6. | Rekap Laporan Penjualan | Data pada laporan berdasarkan data yang sudah terkumpul setiap harinya ketika melakukan pemesanan dengan aplikasi. | Berhasil Rekap | Laporan sesuai dengan hasil pengumpulan setiap harinya. |


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 930-939
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

Hasil pengujian pemesanan, yang dilakukan terhadap sistem digunakan untuk memperoleh data dan menilai tindakan sesuai dengan aktivitas yang dikerjakan oleh pembeli serta akan terlihat bagian yang memiliki kelebihan dan kelemahan.

### 3.2 Hasil Pengujian *Secure Hash Algorithm* 256 (SHA-256)

*Output* yang memungkinkan berdasarkan perhitungan dari SHA-256 yang merupakan penggabungan dari H0(0) sampai H7(0) sebagai berikut :
00000000 || 02000000 || 2808E262 || A147A400 || 00000000 || 00000000 || 1102502B || 1B004808. Sehingga didapat nilai *hash* dari pesan M adalah ketika berada di titik T=1, sebagai berikut : 0000000002000000 2808E262A147A400000000000000000001102502B1B004 808.

Dari analisa yang telah diperoleh terhadap fungsi *login* pada halaman mekanisme *Two Factor Authentication* berdasarkan *message* atau *password* yang dimasukan adalah menghasilkan nilai *hash* yang terdiri dari 6 digit bilangan heksadesimal (*based* on SHA-256) antara lain:

**Tabel 8.** Hasil Nilai *Hash*

| Gmail | *Message* | *Nilai Hash* |
|---|---|---|
| nanisarahhapsari30@gmail.com | nani37 | 271e76<br>43cc46<br>ac3f58<br>8ec8f0 |
| sarahsukamuljo@gmail.com | Gaharu<br>123456 | 323653<br>68ad9b<br>ed868c<br>289a89 |
| sarahsukamuljo9795@gmail.com | kevin 12345 | 0fa9d2<br>f19498<br>dc4477 |

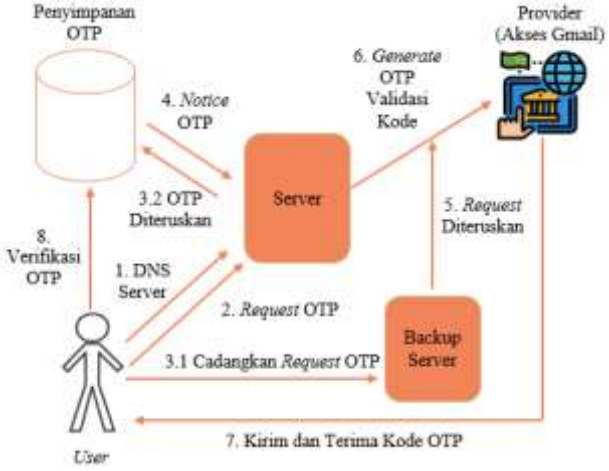
Tabel 7 merupakan tabel nilai hasil hash yang sudah diuji dengan algoritma SHA-256 kemudian nilai tersebut diacak kembali dengan sistem *pseudo random number*. *Source code* yang digunakan untuk memungkinkan memperoleh hasil SHA-256 adalah:

**$user->two_factor_token = bin2hex(random_bytes(3));**

Hasil nilainya bergantung pada pesan atau *password* yang dimasukkan sebelumnya dan mampu menghasilkan bilangan heksadesimal berdasarkan dasar fungsi algoritma matematikanya. Maksud *souce code* tersebut adalah bahwa hasil yang didasarkan ketika *user* melakukan *login* adalah saat terjadinya proses SHA-256 sebagai wujud validasi kode, dilanjutkan kembali dengan pengacakan nilai *string* untuk memperoleh kode yang lebih bervariasi.

### 3.3 Skema Alur Proses Mekanisme *One Time Password*

Pada proses OTP, *user* melakukan *login* atau pendaftaran pada sistem pemesanan kemudian akan di arahkan pada halaman mekanisme *Two Factor Authentication* (2FA), di mana halaman tersebut berisi tempat untuk memasukan kode OTP. Di mana berkaitan langsung dengan fungsi SMTP secara mendasar [22].




**Gambar 2.** Alur Mekanisme Proses OTP

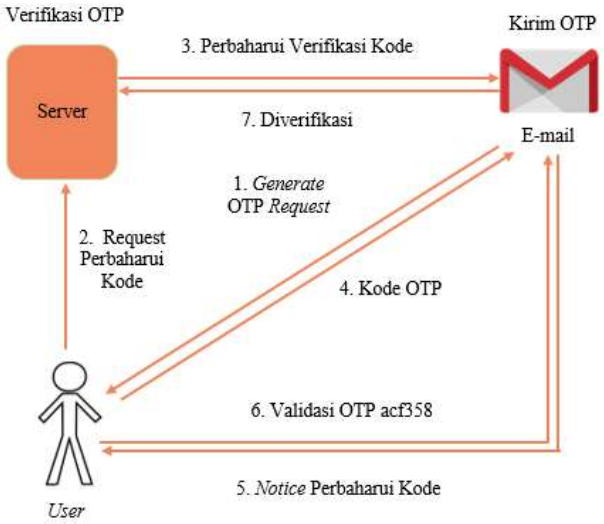
Bermula *user* melakukan permintaan pembangkitan kode OTP yang akan diterima melalui email (gmail) pemilik, sekaligus *user* meminta pula perbaharui kode kepada server lalu *server* dengan membawa pesan yang sama melanjutkan pembaharuan kode yang akan diverifikasi menuju email. Di mana email menjadi perantara


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 930-939
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

untuk menampung kode dan pembawa pesan untuk *user*. Dengan email menerima kode baru maka dipastikan datanya kode di email pengguna sebagai pesan bahwa kode telah diperbaharui oleh *server*. Setelah diterima oleh *user*, diketahui bahwa bentuk kode yang dikirimkan berbentuk angka dan huruf contohnya ac3f58 yang digunakan untuk validasi dan memastikan kembali bahwa pengguna adalah orang yang sama, melakukan transaksi yang sama walaupun di waktu yang berbeda, dan memperoleh kode di akun gmail yang sama. Berdasarkan data yang dikirim melalui gmail dan *user* memasukan kode OTP, secara otomatis kode tersebut diverifikasi bersamaan dengan *user* menerima kode OTP. Hal ini dapat dilihat pada Gambar 2.

*One Time Password* adalah *password* sekali pemakaian yang dibangkitkan oleh sistem pemesan-an *online* yang diolah berdasarkan algoritma *One Time Password dan* komponen *secret key* peng-guna aplikasi ini, dengan masa berlaku (*expired*) yang sudah ditentukan dalam satuan detik. OTP tidak berlaku lagi apabila melewati batas waktu tersebut serta diganti dengan kode OTP yang baru atau deret angka berikutnya. OTP juga hanya berlaku untuk satu kali pemesanan saja.

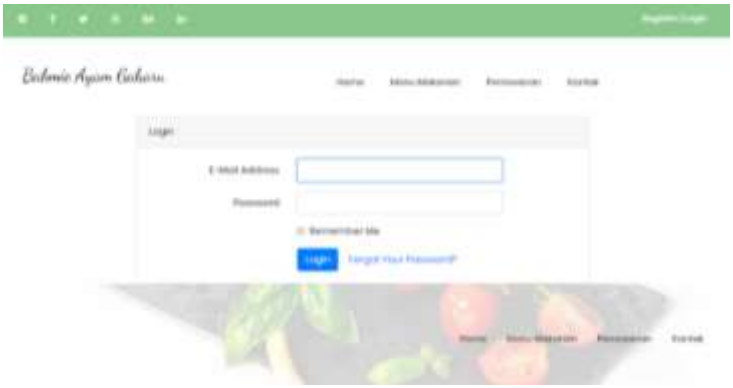



**Gambar 3.** Alur Mekanisme Proses *Send* OTP

### 3.4 Implementasi *Interface*

Implementasi antarmuka (*interface*) merupakan hasil nyata dari *user interface* yang sebelumnya telah dibuat pada tahap perancangan. Pada implementasi *interface* ini akan ditampilkan rancang halaman yang telah dibuat melalui program pengkodingan, di antaranya:

a. Implementasi *Input Login User*
*Interface* ini merupakan antarmuka proses *login* (masuk pada suatu halaman tertentu), di mana terdapat beberapa data yang harus diisi terlebih dahulu yaitu alamat email dan *password*.

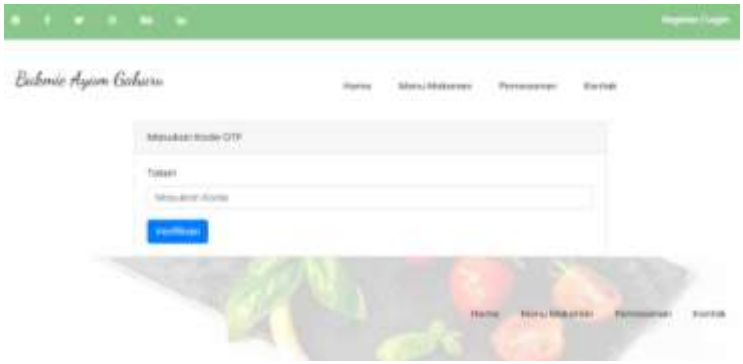


**Gambar 4.** Halaman *Input Login User*

b. Implementasi *Interface One Time Password*
Interface ini menjelaskan bahwa setelah melakukan registrasi atau *login* pembeli diharuskan memasukan kode OTP yang dikirimkan melalui gmail sebagai otentikasi tanda kepemilikan akun untuk melakukan pemesanan.


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

**JURNAL MEDIA INFORMATIKA BUDIDARMA**
**Volume 4, Nomor 4, Oktober 2020, Page 930-939**
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195



**Gambar 5.** Halaman *One Time Password*

c. *Generate* OTP pada Gmail Pembeli
*Output* yang dihasilkan adalah kode OTP di mana pembangkit kode ini dikirimkan melalui google mail sebagai kode verifikasi untuk memasuki halaman pemesanan pembeli


**Gambar 6**. *Generate* OTP pada Gmail Pembeli

## 4. KESIMPULAN

Berdasarkan penelitian yang dilakukan, maka penulis dapat mengambil kesimpulan bahwa pada aplikasi Pemesanan *Online* terdapat beberapa fungsi salah satunya proses *login* di mana pengguna diharuskan terlebih dahulu melakukan pendaftaran agar dapat mengakses halaman yang terdapat di aplikasi. Dengan diterapkannya mekanisme 2FA (*Two Factor Authentication*) pada proses *login* memberikan rasa aman dan rahasia bahwa *password* yang dimasukan tidak akan diketahui oleh orang lain dengan alur prosesnya, pembeli mendapatkan kode atau deret angka dengan bentuk acak sebagai wujud otentikasi pengguna yang sah. Pembangkit *2*FA yaitu TOTP dengan OTP ini yang menghasilkan *password* (kode) dinamis (berubah-ubah) dengan jangka waktu sekitar 10 menit. Sebagai dasar enkripsi yang terdapat dalam Metode OTP, enkripsi *Secure Hash Algorithm* 256 (SHA-256) mampu menghasilkan kode acak dengan menggunakan bantuan *pseudo random number* sehingga menghasilkan 6 digit nilai heksadesimal yang berarti sama dengan 48 bit dan kemungkinan maksimal terbesar mencapai 256 bit. Metode OTP dapat berjalan sesuai dengan kebutuhan, keinginan, dan perancangan serta penerapannya tidak hanya pada aplikasi pemesanan makanan ini saja melainkan dalam wujud lain berupa aplikasi yang lebih besar contohnya aplikasi ecommerce. Sebagai aplikasi, dibutuhkan suatu pengujian pula untuk mengukur sejauh mana aplikasi tersebut dapat bekerja, pengujian yang dilakukan menggunakan Metode Pengujian *Black Box* yang berfokus pada persyaratan secara fungsional perangkat lunak. Skenario pengujian lebih kepada tata cara atau mekanisme yang akan dilakukan untuk pengujian sistem dari awal hingga akhir dan pengujian sistem yaitu penerapan skenario dengan mendapatkan hasil pengujian berupa *output* yang dihasilkan dan penilaian dengan rentang nilai sekitar 95% - 100%. Rata-rata hasil yang dicapai sukses dan sesuai berdasarkan perancangan yang dilakukan. Diharapkan pula dipergunakannya Metode Akurasi yang jelas penerapannya terhadap Nilai *Hash* yang dihasilkan.

## REFERENCES

[1] R. Munadi, Z. Musliyana, and T. Y. Arif, "Kombinasi Waktu Sinkronisasi dan Nilai Salt untuk Peningkatan Keamanan pada *Single Sign-On*," Jurnal Nasional Teknik Elektro dan Teknologi Informasi, vol. 5, no. 3, pp. 201–206, August. 2016.
[2] D. V. S. Y. Sakti, N. Agani, and M. Hardjianto, "Pengamanan Sistem Menggunakan *One Time Password* dengan Pembangkit *Password Hash* SHA-256 dan *Pseudo Random Number Generator* (PRNG) *Linear Congruential Generator* (LCG) di Perangkat Berbasis Android," Jurnal BIT, vol. 13, no. 1, pp. 64–73, April. 2016.
[3] R. Doly Andika C, "Implementasi *One Time Password Mobile* Token dengan *Algorithm Secure Hash Algorithm* 1 (SHA1) pada *Login Website* Pusdaskrimti Kejaksaan Agung Republik Indonesia," Tugas Akhir, Fakultas Teknologi


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
**Volume 4, Nomor 4, Oktober 2020, Page 930-939**
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2195

Informasi., Universitas Budi Luhur., Jakarta, 2017.
[4] W. S. Raharjo *et al*., "Implementasi *Two Factor Authentication* dan Protokol *Zero Knowledge Proof* pada Sistem *Login*," Jurnal Teknik Informatika dan Sistem Informasi, vol. 3, no. 1, pp. 127–136, April. 2017.
[5] I. D. Id, Sukamto, and E. Mahdiyah, "Implementasi TOTP (*Time-Based One-Time Password*) untuk Meningkatkan Keamanan Transaksi E-Commerce," in Konferensi Nasional Sistem dan Informasi, STT Ibnu Sina, Batam, August 11 - 13, 2016, Pekanbaru, 2017, pp. 1-6.
[6] A. Y. Husodo *et al.*, "Sistem Keamanan Nilai Akademik *Online* Berbasis Kode *Hash* dengan Identitas Server Sebagai Parameter Validasi," Jurnal Sains Teknologi dan Lingkungan vol. 1, no. 1, pp. 8–14, 2015.
[7] R. Yusuf, E. Anggriawan, S. Tinggi, and S. Negara, "Penerapan Metode *Smart Authentication* dalam Layanan E-*Banking* Menggunakan *Two Channel Authentication* dan QR-*Code* pada Perangkat *Mobile*," Seminar Nasional Sistem Informasi Indonesia, November 2-3, 2015, Bogor, Sekolah Tinggi Sandi Negara, 2015.
[8] U. Ungkawa, I. A. Dewi, and K. R. Putra, "Implementasi Algoritma *Time-Based One Time Password* dalam Otentikasi Token Internet *Banking*," in Library Itenas, Bandung, 2015, pp. 2–11.
[9] A. Rosano, N. A. Farabi, and A. Kusumaningrum, "Perancangan Sistem Internet *Banking* (IBank) Menggunakan *One-Time-Password* (OTP) Untuk Pengamanan Transasksi (Studi Kasus Bank Mega, Tbk)," Jurnal AKRAB JUARA, vol. 3, no. 2, pp. 1-12, May. 2018.
[10] P. D. Pamungkas, "Rancang Bangun Sistem Verifikasi Data Dokumen," Jurnal INOVATE, vol. 03, no. 02, pp. 10–17, 2019.
[11] A. Afifudin, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) dan Metode *Two Factor Authentication* (2FA) untuk Verifikas Dokumen," Skripsi, Fakultas Teknik., Universitas Nusantara PGRI, Kediri., 2018.
[12] H. Sembiring, F. Y. Manik, and Tengkuzaidah, "Penerapan Algoritma *Secure Hash Algorithm* (SHA) Keamanan pada Citra," Medida Informasi Analisa dan Sistem, vol. 4, no. 1, pp. 33–36, Juni. 2019.
[13] I. Saputra and S. D. Nasution, "Analisa Algoritma SHA-256 Untuk Mendeteksi Orisinalitas Citra Digital," in Prosiding Seminar Nasional Riset *Infomation Science*, pp. 164–178, September. 2019.
[14] A. Y. Mulyadi, E. P. Nugroho, and R. R. J. P, "Implementasi Algoritma AES 128 dan SHA–256 dalam Pengkodean pada Sebagian *Frame* Video CCTV MPEG-2," Jurnal Teori dan Aplikasi Komputer, vol. 1, no. 1, pp. 33–39, Maret. 2018.
[15] M. Naufal and Purwanto, "Implementasi Keamanan *Login* dengan Metode *One Time Password* (OTP) Menggunakan Fungsi *Hash* Algoritma SHA-512 pada SMP Negeri 3 Tangerang Selatan," Jurnal Skanika, vol. 1, no. 1, pp. 335–339, Maret. 2018.
[16] N. Istiqamah, "Sistem Keamanan E-*Voting* Menggunakan Fungsi *Hash* dan Algoritma *One Time Pad*," Skripsi, Fakultas Teknik., Universitas Negeri Semarang., Jawa Tengah., 2016.
[17] U. P. S. Perdana, "Pemanfaatan Telegram Boot API dalam Layanan Otentikasi Tanpa *Password* Menggunakan Algoritma T*ime-based One-Time Password* (TOTP)," Skripsi, Fakultas Teknik., Universitas PGRI., Kediri., 2016.
[18] K. I. Santoso, "Dua Faktor Pengamanan *Login* Web Menggunakan Otentikasi *One Time Password* dengan *Hash* SHA," in Seminar Nasional Teknologi Informasi dan Komunikasi Terapan, pp. 204–210, November. 2013.
[19] P. S. Rahmat, "Penelitian Kualitatif," Equilibrium, vol. 5, no. 9, pp. 1-8, Juni 2009.
[20] Y. Anugrah, M. H. H. Ichsan, and A. Kusyanti, "Implementasi Algoritme SHA-256 Menggunakan Protokol MQTT pada Budidaya Ikan Hias," vol. 3, no. 4, pp. 4066-4074, April. 2019.
[21] Pratiwi and D. Atmojo. WP, "Peningkatan Keamanan Data dengan Metode *Cropping Selection Pseudorandom*," Jurnal TICOM, vol. 4, no. 3, pp. 132–138, Mei. 2016.
[22] Hamid, "Analisis Keamanan Aplikasi E-mail Bawaan Android dan Gmail pada Jaringan Nirkabel," Jurnal Teknoin, vol. 23, no. 2, pp. 125–136, Juni, 2017.


Submitted: **14/05/2020**; Accepted: **03/09/2020**; Published: **20/10/2020**