IMPLEMENTASI ONE TIME PASSWORD DENGAN ALGORITMA SECURE HASH ALGORITHM 512 (SHA-512)

Lathanza Gala Rimba Semesta[1)], **Safrina Amini**[2)]
[1]*Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur*
[1.2]*Jl. Raya Ciledug, Petukangan Utara,, Jakarta Selatan 12260*
Telp. (021) 5853753, Fax. (021) 5853752
E-mail : lathanzalgrs@gmail.com[1)], Safrina.amini@budiluhur.ac.id[2)]

ABSTRAK

Pesatnya Perkembangan sistem informasi sekarang ini berpengaruh juga pada bidang akademik. Berbagai jenis aktivitas akademik telah dijalankan dengan memanfaatkan teknologi ini. Sistem informasi berbasis web salah satu yang sering di gunakan dalam aktivitas akademik, sistem informasi ini berjalan di atas jaringan berberapa komputer yang saling terhubung, hal ini membuat seluruh data atau informasi dapat dicuri dengan mudah oleh siapa saja padahal Keamanan merupakan salah satu aspek penting dari sebuah sistem informasi oleh karena itu, dibuatlah sistem login agar hanya user yang memiliki hak yang dapat masuk ke dalam sistem informasi tersebut, Proses login ialah proses di mana user memasukkan username dan password agar dapat mengakses sebuah sistem namun biasanya orang akan menggunakan password yang mudah ditebak atau menggunakan password statis. Oleh karena itu SMK Karya Bangsa membutuhkan sebuah sistem autentikasi berupa password unik yang hanya dapat dipakai sekali atau disebut One Time Password, hal ini ditujukan agar user terhindar dari serangan sniffing, sniffing merupkan suatu teknik pencurian data dengan bantuan perangkat lunak dengan mengambil informasi login seperti username dan password user. Mekanisme One Time Password ini dipadukan dengan Algoritma Secure Hash Algoritm-512 (SHA-512) untuk membangkitkan token dan juga membutuhkan saluran komunikasi lain yang terpercaya seperti SMS. Ketika pengguna mencoba masuk ke dalam sistem, service One Time Password akan mengirimkan kode verifikasi melalui saluran komunikasi sekunder tersebut, oleh karena itu service One Time Password ini mampu mencegah terjadinya sniffing yang dilakukan oleh peretas. Sehingga jika terjadi penyerangan, peretas hanya mampu mendapatkan nama pengguna saja tanpa kode verifikasi yang di kirimkan melalui saluran komunikasi yang berbeda tersebut untuk login dan mengakses sistem.

Kata Kunci : *Login*, *One Time Password*, *Hash*, SHA-512, *Sniffing*

1. Latar Belakang

Keamanan merupakan hal yang sangat penting dari sebuah sistem informasi tetapi banyak ditemukan masalah keamanan berada di urutan kedua, atau bahkan dianggap tidak perlu, misalnya saja apabila mengganggu performa sistem yang berjalan, faktor keamanan tersebut akan dikurangi atau dihilangkan. Pentingnya nilai sebuah informasi menyebabkan informasi yang diinginkan hanya boleh diakses oleh orang yang memiliki hak. Jatuhnya informasi ke tangan pihak yang tidak berhak dapat menimbulkan kerugian bagi si pemilik informasi, oleh karena itu keamanan yang terdapat pada sistem informasi yang digunakan harus dapat menjamin informasi tidak jatuh ke pihak yang tidak berhak. Pesatnya Perkembangan sistem informasi sekarang ini berpengaruh juga pada bidang akademik. Berbagai jenis aktivitas akademik telah dijalankan dengan memanfaatkan teknologi ini. Sistem informasi berbasis web salah satu yang sering di gunakan dalam aktivitas akademik, sistem informasi ini dapat diakses melalui jaringan komputer yang terhubung dengan internet oleh siapa saja, maka dari itu hal ini yang membuat seluruh data dan informasi dapat dicuri dengan mudah oleh siapa saja. Salah satu masalah keamanan yang terdapat dalam sistem informasi berbasis web adalah bagaimana sistem yang ada dapat memastikan *user* yang mengakses data maupun informasi pada sistem tersebut adalah *user* yang berhak dan memiliki wewenang. Ada beberapa metode untuk melakukan autentikasi pada sebuah sistem informasi, salah satunya adalah menggunakan *password*, namun kerahasiaan sebuah data maupun informasi masih belum bisa di katakan aman hanya dengan penggunaan *password* [1].

Banyak metode yang sering digunakan oleh peretas untuk dapat mengetahui *password* dari sebuah akun (*account*). Salah satu cara yang digunakan peretas untuk mengetahui informasi akun seseorang adalah *sniffing*. *Sniffing* adalah suatu teknik pencurian sebuah informasi dengan bantuan perangkat lunak dengan mengambil

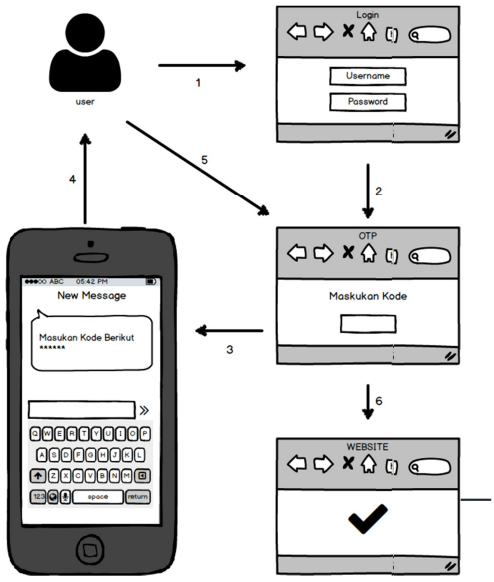
informasi dari *log* sistem seperti *username* dan *password* [7]. SMK Karya Bangsa Tangerang merupakan sekolah yang menggunakan sistem informasi berbasis web, namun selama ini para *user* hanya menggunakan *username* dan *password* untuk *login* dan mengakses web tersebut. Terlebih lagi sistem tersebut masih menggunakan protokol HTTP dalam proses pengiriman data informasi hal ini dapat mengakibatkan sistem rentan terhadap peretas yang berusaha mencuri informasi seperti *username* dan *password* untuk masuk ke web tersebut untuk mencuri data maupun mengubah data. Atas dasar tersebut penulis membangun sebuah mekanisme *One Time Password* (OTP) pada *website* di SMK Karya Bangsa, yakni kata sandi yang hanya bisa digunakan untuk sekali pakai oleh pengguna. Aplikasi ini ditujukan untuk meningkatkan pengamanan penggunaan kata sandi dari serangan *sniffing*. Mekanisme OTP membutuhkan saluran komunikasi lain yang terpercaya. Ketika pengguna mencoba masuk ke dalam sistem, *service* OTP akan mengirimkan kode verifikasi melalui saluran komunikasi sekunder tersebut, oleh karena itu *service* OTP ini mampu mencegah terjadinya *sniffing* yang dilakukan oleh peretas. Sehingga jika terjadi penyerang peretas hanya akan mampu mendapatkan nama pengguna saja tanpa kata sandi yang di kirimkan melalui saluran komunikasi yang berbeda tersebut untuk *login* dan mengakses sistem [6].

2. Analisis Masalah

Analisis masalah yang didapatkan berdasarkan rumusan masalah yang ada adalah sistem yang ada di SMK karya Bangsa saat ini masih memiliki kelemahan yaitu menggunakan *password* statis atau *password* yang sama sehingga mudah ditebak, diketahui, maupun disadap. Para peretas ini menggunakan cara yang dinamakan *sniffing* untuk mengetahui informasi akun seseorang, *sniffing* adalah suatu Teknik pencurian informasi dengan bantuan perangkat lunak yang dapat mengambil informasi dari aktivitas sebuah komputer. SMK Karya Bangsa Tangerang merupakan sekolah yang menggunakan sistem informasi berbasis web, namun selama ini para user hanya menggunakan *username* dan *password* statis (selalu sama) untuk *login* pada web tersebut dimana hal tersebut sangat rentan terhadap aksi *sniffing* yang dilakukan oleh peretas, misalnya apabila peretas mengirim *link* pada *user*, dan bila *link* tersebut diklik oleh user, link tersebut akan menuju halaman situs yang berisi *software* yang dapat melakukan *sniffing*. *Software* tersebut akan ter-*install* secara otomatis pada komputer *user*. Peretas melakukan *sniffing* pada komputer tersebut untuk menyadap data *username* dan *password* di SMK karya Bangsa. Setelah *username* dan *Password* didapat, peretas dapat masuk ke *website* tersebut melalu akun *user* yang berhasil di dapat lalu peretas tersebut bisa mengubah sampai merusak data yang ada sekalipun.

3. Penyelesaian Masalah

Dari Permasalahan di atas, penulis menyarankan untuk menggunakan metode pengamanan *One Time Password* pada *website* di SMK Karya Bangsa, dengan mengimplementasikan algoritma SHA-512 dengan menggunakan telepon seluler untuk menerima kode. Berdasarkan tujuan penelitian tersebut, maka metode penelitian yang digunakan dalam penelitian ini adalah metode *prototype*. Dengan melakukan evaluasi terhadap *prototype* yang dikembangkan, apakah *prototype* sudah sesuai dengan hasil yang diharapkan. Sehingga hasil penelitian dapat di terapkan. Penelitian ini menggunakan metode *One Time Password* berbasis sinkronisasi waktu (*Time-Synchronization*) yang akan berubah secara konstan pada interval waktu tertentu. Metode ini memerlukan sinkronisasi waktu antara server autentikasi dengan kode verifikasi yang akan dimiliki *user*. Waktu merupakan bagian terpenting dari algoritma pembangkit kode karena waktu adalah dasar dari Pembangkitan kode, oleh karena itu Ketika kode verifikasi dikirim, *user* hanya memiliki waktu beberapa menit untuk memasukkan kode verifikasi yang akan disinkronisasi dengan server autentikasi. Penelitian ini membutuhkan dua saluran komunikasi yaitu web server dan telepon seluler sehingga akan dibuat dua halaman web yaitu halaman *login* web dan halaman untuk verifikasi kode. Proses dari aplikasi yang akan dibuat dimulai dari pengisian *username* dan *password* pada halaman web. Web tersebut akan meng-*generate* kode yang akan digunakan sebagai kode verifikasi. Kode verifikasi tersebut dikirimkan ke nomor telepon *user* melalui SMS. *User* memasukkan kode yang telah di dapat ke halaman verifikasi. Pada Gambar berikut ini akan



menggambarkan sistematik penggunaan aplikasi yang akan dibuat.

Gambar 1 : Sistematik Aplikasi

Metode pembangkit kode *One Time Password* (OTP) pada penelitian ini menggunakan metode *Time-based One Time Password* (TOTP) dan algoritma *Hash* SHA-512. Sementara model yang digunakan untuk pembangkitan kode menggunakan *self-generated* dimana sistem akan menghasilkan sendiri kode. Kode OTP dibangkitkan berdasarkan waktu dan *username* pada saat OTP diminta dibangkitkan

4. Landasan Teori

4.1. Proses Login

Identifikasi, autentikasi dan otorisasi merupakan mekanisme dari proses login [4].

4.2. Proteksi *Password*

Ada beberapa upaya untuk mengamankan proteksi password, antara lain :

- *Salting*
  String password yang dimiliki user ditambahkan suatu *string* sehingga mencapai panjang *password* yang telah ditentukan.
- *One Time Password*
  Pasword bersifat yang dinamis, dimana *Password* yang dipakai oleh *user* untuk *login* akan diganti secara teratur berdasarkan waktu tertentu.
- *One Question & Long Answer*
  Cara ini mengharuskan user menyimpan satu atau beberapa pertanyaan beserta jawabannya. Pertanyaan dan jawaban tersebut biasanya tentang profil *user* seperti nama hewan peliharaan, dan lain sebagainya sehingga mudah untuk diingat dan juga *user* tidak perlu menuliskannya pada kertas.
- *Response*
  User diberikan kebebasan untuk menggunakan satu atau beberapa metode sekaligus untuk mengakses sistem [9].

4.3. One Time Password

One Time Password (OTP) adalah sebuah *password* atau biasa disebut dengan *token* yang hanya berlaku untuk sesi *login* [7]. Dengan kata lain *One Time Password* (OTP) merupakan metode autentikasi yang menggunakan *password* dinamis yang selalu berubah setiap *user* melakukan *login*, atau berubah setiap interval waktu tertentu [2].

4.4. Algoritma SHA

SHA merupakan salah satu dari banyak fungsi *hash*. SHA dikembangan oleh NSA (National *Security Agency*) dan diterbitkan oleh NIST (*National Institute of Standards and Technology)* pada tahun 1993 dan diberi nama SHA-0, setelah itu dua tahun kemudian pada tahun 1995 dipublikasikan SHA-1 generasi selanjutnya dan juga perbaikan dari kekurangan algoritma SHA-0. Pada tahun 2002 NIST mempublikasikan empat variasi *hash* lainnya, yaitu SHA-384, SHA-512, dan SHA-384, ketigany disebut sebagai SHA-2 [3].

4.5. SHA-512 (*Secure Hash Algorithm*-512)

Fungsi *hash* SHA-512 merupakan fungsi yang menghasilkan *output* sebesar 512 bit dan panjang blok 1024 bit. Terdapat 80 *looping* dalam algoritma ini. Proses *padding message* dilakukan dengan cara yang sama dengan algoritma SHA-1, namun besar hasil akhir pesan menjadi 1024 bit [5].

4.6. Cara Kerja SHA-512

Proses *padding* yang terjadi pada SHA-512 adalah:

- Mengubah pesan masukan menjadi Bilangan Biner
- Penambahan angka ‘1’ di akhir pesan
- Penambahan k bit ‘0’,dimana k adalah nilai minimum > = 0 sehingga pesan yang memiliki total 896 *mod* 1024.
- Tambahkan panjang pesan, dalam bit, sebagai 128-bit integer.

Berikut adalah fungsi hash yang digunakan pada setiap putaran [8]:

- Penjadwalan Pesan

$$w_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{(512)}(W_{t-2}) + W_{t-7} + \sigma_0^{(512)}(W_{t-15}) + W_{t-16} & 16 \le t \le 79 \end{cases}$$

- Inisialisasi

$$a = H_0^{(i-1)}$$
$$b = H_1^{(i-1)}$$
$$c = H_2^{(i-1)}$$
$$d = H_3^{(i-1)}$$
$$e = H_4^{(i-1)}$$
$$f = H_5^{(i-1)}$$
$$g = H_6^{(i-1)}$$
$$h = H_7^{(i-1)}$$

- Fungsi setiap putaran

$$T_i = h + \sum\nolimits_1 (e) + Ch(e.f.g) + K_j + w_j$$

$$T_i = \sum\nolimits_0 (a) + Maj(a.b.c)$$

$$h = g, g = f, f = e, e = d + T_1, d = c, c = b, b = a, a = T_1 + T_2$$

$$Ch(x,yz) = (x \wedge y) \oplus (x \wedge z)$$

$$Maj(x,yz) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

$$\sum_0(x) = ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x)$$

$$\sum_1(x) = ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x)$$

$$\sigma_0 = ROTR^{1}(x) \oplus ROTR^{18}(x) \oplus RSHIFT^{7}(x)$$

$$\sigma_1 = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus RSHIFT^{6}(x)$$

- Hitung nilai *Hash*

$$H_0^{(i)} = a + H_0^{(i-1)}$$

$$H_1^{(i)} = a + H_1^{(i-1)}$$

$$H_2^{(i)} = a + H_2^{(i-1)}$$

$$H_3^{(i)} = a + H_3^{(i-1)}$$

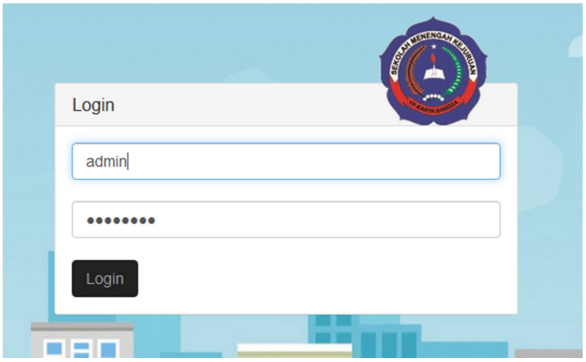
$$H_4^{(i)} = a + H_4^{(i-1)}$$

$$H_5^{(i)} = a + H_5^{(i-1)}$$

$$H_6^{(i)} = a + H_6^{(i-1)}$$

$$H_7^{(i)} = a + H_7^{(i-1)}$$

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_{03}^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$$



- Nilai akhir *Hash*

5. Pengujian Program

Berikut akan dilakukan simulasi pengujian program yang telah dibuat

5.1. Pengujian Pembangkitan Kode OTP

Pengujian untuk membangkitkan kode dilakukan dengan memasukkan *username* dan *password* yang dimiliki user pada *form login* seperti gambar berikut:

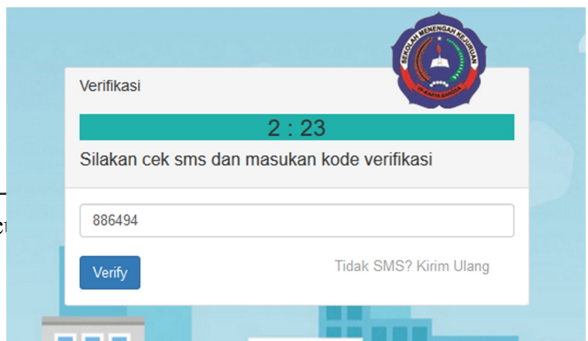
Gambar 2 : Form Login

Setelah user berhasil login secara otomatis kode OTP dibangkitkan oleh sistem lalu sistem akan mengirim kode tersebut lewat SMS kepada user seperti pada Gambar berikut ini:

Gambar 3 : Tampilan Layar SMS Pada User

5.2. Pengujian verifikasi kode OTP

Kode OTP 886494 memiliki masa aktif dua setengah menit kode tersebut dikirimkan sistem melalui SMS ke telepon selular *user*. Pengujian

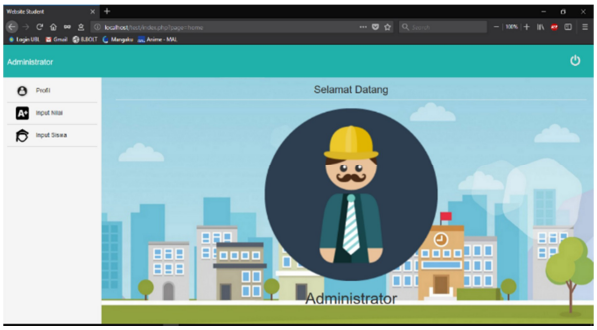


dilakukan dengan memasukkan kode OTP 886494 pada *website*. Seperti pada Gambar berikut ini:

Gambar 4 : Form Verivikasi

5.3. Tampilan Hasil Pengujian Halaman Utama *Website*

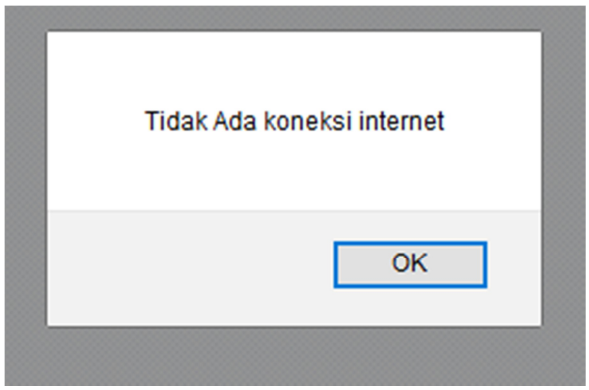
Pada Gambar berikut ini membuktikan bahwa kode OTP yang di *input* sinkron dengan kode OTP pada halaman *login website*.



Gambar 5 : Form Home

5.4. Pengujian tidak ada koneksi internet

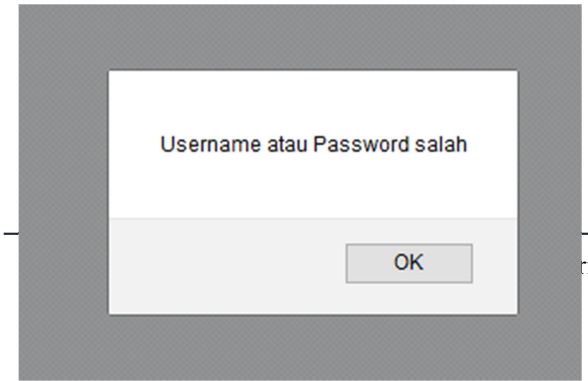
Pada Gambar berikut ini akan muncul *popup* "Tidak Ada Koneksi Internet" ketika koneksi internet mati.



Gambar 6 : Message box Tidak Ada Koneksi

5.5. Pengujian *Username* atau *Password* salah

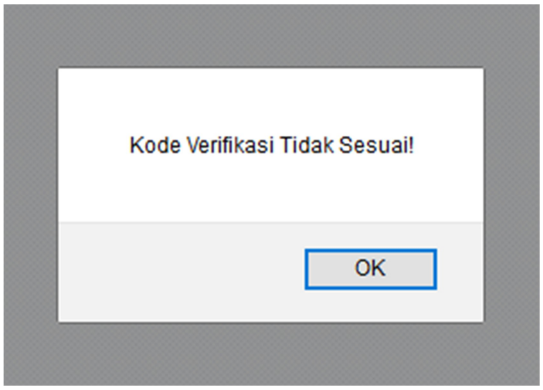
Pada Gambar berikut ini akan muncul *popup* "*Username* atau *Password* Salah" ketika *user* salah memasukkan identitas pada halaman *login* web.



Gambar 7 : Message box Username dan Password salah

5.6. Pengujian Kode OTP Salah

Pada Gambar berikut ini akan muncul *popup* "Kode OTP tidak sesuai". *Popup* ini akan muncul bila *user* memasukkan kode OTP yang salah



Gambar 8 : Message box Kode Verifikasi Tidak Sesuai

6. Evaluasi Program

6.1. Kelebihan Program

1) Dapat digunakan dimana saja karena bersifat *online*.
2) Mudah diakses karena berbasis *website*.
3) Mudah untuk digunakan.
4) Pengguna lain tidak akan bisa mengakses jika tidak mempunyai kode verifikasi yang dikirim melalui SMS ke nomor pengguna.

6.2. Kekurangan Program

1) Hanya menggunakan algoritma SHA-512 untuk melakukan proses pembangkitan OTP dan belum dikombinasikan dengan algoritma yang lain. Batas waktu memasukkan kode verifikasi hanya 2 menit 30 detik.

7. Kesimpulan

Berdasarkan hasil pengujian dan implementasi yang dilakukan di atas, maka penulis dapat mengambil beberapa kesimpulan sebagai berikut :

a. Implementasi *One Time Password* menggunakan algoritma SHA-512 dapat mengamankan *login website*.
b. Pengguna bisa menggunakan *username* dan *password* yang sama, jika terjadi penyadapan (*sniffing*), pelaku tetap tidak bisa mengakses sistem karena tidak mengetahui kode verifikasi yang dimiliki pengguna.
c. Token dari *One Time Password* ini hanya bisa dikirim ke nomer telepon pengguna, Sehingga hanya pengguna yang mengetahui kode tersebut.

8. Saran

Penelitian implementasi *One Time Password* ini masih terdapat kekurangan. Oleh karena itu, penelitian ini masih bisa dikembangkan sehingga dapat lebih bermanfaat untuk di kemudian hari. Berikut ini Saran untuk penelitian lebih lanjut yang dapat disampaikan penulis ialah:

a. Tidak hanya menggunakan algoritma SHA-512 saja untuk melakukan proses pembangkitan OTP, harus dikombinasikan dengan algoritma yang lain agar lebih aman. Aplikasi ini diharapkan dapat dikembangkan agar dapat *login* lebih aman lagi.
b. Aplikasi ini diharapkan dapat dikembangkan agar dapat *login* lebih aman lagi.

9. Daftar Pustaka

[1.] Mulyono, Hengky dan Rodiah, 2013, Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web, *Seminar Nasional Teknologi Informasi dan Multimedia*, pp. 35–40.

[2.] Musliyana, Zuhar, Arif, Teku Yuliar. dan Munadi, Rizal, 2016, Peningkatan Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus : SSO Universitas Ubudiyah Indonesia, 12(1), pp. 21–29. doi: 10.17529/jre.v12i1.2896.

[3.] Prasetyo, Tri Ferga. dan Hikmawan, Aris, 2012 Analisis Perbandingan Dan Implementasi Sistem Keamanan Data Menggunakan Metode Enkripsi RC4 SHA dan MD5, *Infotech*, 60(18), pp. 41–46.

[4.] Pribadi, Agus, 2014, Perancangan Keamanan Sistem Login Aplikasi Multiuser Dengan Algoritma Message Digest 5 (Md5), *Pelita Informatika Budi Darma*, pp. 172–175.

[5.] Putra, Pacu dan Winiarni, Reza, 2016 Perancangan Pengamanan Sistem Informasi Electronic Medical Record (Emr) Dengan Metode Sha-512 Studi Kasus Pada Klinik Jb Palembang, 2(1), pp. 212–215.

[6.] Rahma, Diam, Wibisono, Waskitho dan Pratomo, Baskoro Adi, 2013, Pengembangan Mekanisme One Time Password dengan Menggunakan Strategi Dual Channel pada Aplikasi Web, *Jurnal Teknik Pomits*, 2(1), pp. 1–6.

[7.] Santoso, Kartika Imam, 2013, Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA, *Seminar Nasional Teknologo Informasi & Komunikasi Terapan*, pp. 204–210.

[8.] Sembiring, Jakaria, 2013, Analisis Algoritma Sha-512 Dan Watermarking Dengan Metode Least Significant Bit Pada Data Citra, *Seminar Nasional Sistem Informasi Indonesia*, pp. 2–4.

[9.] Malik, J.J., 2009, BEST TOOLS HACKING & RECOVERY PASSWORD 1st ed. M. A. W, ed.,Yogyakarta: C.V ANDI OFFSET(Penerbit ANDI). Available at: https://books.google.co.id/books?id=u9Xc1bepSygC&printsec=frontcover&source=gbs_vpt_reviews#v=onepage&q&f=false.