SISTEM PENILAIAN ONLINE MENGGUNAKAN KEAMANAN ONE TIME PASSWORD DENGAN ALGORITMA SHA 512 BERBASIS WEB

Akbar Tito Wicaksono[1)], Titin Fatimah[2)]
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : akbartitowic@gmail.com[1)], titin.fatimah@budiluhur.ac.id[2)]

Abstrak

Sistem penilaian online berbasis web semakin hari semakin banyak digunakan. Namun keamanan dalam sistem bersifat online sangat rentan terutama karena diakses oleh banyak orang. Dan sangat rawan bila diakses oleh orang yang tidak berkepentingan dalam aplikasi yang mengharuskan proses login terlebih dahulu. Biasanya orang akan menggunakan password yang mudah ditebak oleh orang lain atau menggunakan password statis yang tidak pernah diubah. Selain itu password juga dapat diketahui oleh pihak yang tidak bertanggung jawab dengan cara sniffing atau penyadapan. Hal ini membuat password tidak aman untuk mengakses sistem informasi. Oleh karena itu SMA Islamic Village Tangerang membutuhkan sistem penilaian online dengan keaman one time password yaitu sebuah sistem otentikasi berupa password unik dengan hanya sekali pakai. Oleh karena penggunaan telepon genggam saat ini semakin meningkat, maka penelitian ini memanfaatkan telepon genggam sebagai penerima kode verifikasi untuk mengimplementasikan one time password. Aplikasi ini berbasis web dimana algoritma yang digunakan adalah Hash SHA-512 serta menggunakan bahasa pemrograman PHP dan MySQL sebagai database. Kode verifikasi akan dikirimkan melalui telepon genggam pengguna. Bila kode verifikasi yang digunakan untuk login tidak sesuai dengan yang dikirim melalui pesan maka pengguna tidak bisa login sehingga sistem akan menjadi lebih aman. Sehingga menghasilkan keamanan saat login ke dalam aplikasi penialan online.

Kata kunci: One Time Password, Hash, SHA 512

1. PENDAHULUAN

Pada zaman modern penggunaan *web* sebagai sarana informasi semakin banyak digunakan di berbagai instansi pendidikan negeri maupun swasta. Salah satu yang menggunakan *web* sebagai media informasi adalah SMA Islamic Village.

Hal ini mempermudah siapa saja dalam mencari informasi yang telah diberikan. Keamanan dalam sebuah sistem terintegrasi akan memanfaatkan jaringan komputer sebagai bagian yang sangat penting. Salah satu masalah yang dihadapi adalah kurang maksimal pemanfaatan *web* dan pada sistem jaringan komputer adalah memastikan *user* yang *login* adalah *user* sesungguhnya.

Pada SMA Islamic Village selain sebagai media informasi, web juga bisa digunakan untuk menampilkan nilai siswa. Nilai sampai saat ini masih dipercaya sebagai salah satu tolak ukur keberhasilan siswa menempuh pendidikan di sekolah[1]. Namun dalam membangun sistem penilaian *online* perlu keamanan untuk menjaga web tersebut. Ada beberapa metode untuk sebuah otentikasi salah satunya berupa *password*.

Namun menggunakan *password* belum menjamin keamanannya. Salah satu contoh yang paling sederhana adalah seorang admin yang memiliki wewenang untuk mengakses *database* tentu akan dengan mudah dapat mengambil data atau informasi yang disimpan di dalam *database* tersebut bila sudah *login*.

Dalam pencegahan akses sistem ke dalam web bisa dilakukan dengan menggunakan cara otentikasi, salah satunya adalah dengan cara memakai password statis untuk menghindari pencurian oleh peretas. (Shaka, et al., 2016). Dan *password* dapat diketahui oleh para pihak yang tidak bertanggung jawab dengan cara meretas.

Otentikasi menggunakan *password* banyak digunakan oleh banyak orang. Namun pengguna kurang waspada terhadap pencurian *password*, misalnya menggunakan *password* yang sering digunakan seperti tanggal lahir, kota kelahiran, nama orang tua dan sebagainya. Beberapa penelitian telah dilakukan terkait dengan *One Time Password* (OTP) dengan berbagai metode. Dan dalam penelitian ini, digunakan algoritma SHA.

2. METODE PENELITIAN

Dalam penelitian ini, digunakan sebuah pengembangan metode dengan model *Software Development Life Cycle* (SDLC) yaitu metode *waterfall* yang meliputi tahapan perencanaan, analisis, desain, implementasi, pengujian, dan pemeliharaan. Berikut ini adalah rincian tahapan dalam pembuatan aplikasi.

a. Perencanaan dan Pengumpulan data

Merencanakan dan mengumpulkan data dibutuhkan dari berbagai macam elemen sistem yang akan dimasukan ke dalam *web* dengan sistem keamanan dan mengumpulkan data mengenai *web*

SMA Islamic Village, *One Time Password* dan algoritma SHA 512.

b. Menganalisa

Setelah mengumpulkan dan memperoleh data yang dibutuhkan, berikutnya mempelajari dan menganalisa tentang fungsi yang diperlukan untuk mengimplementasikan dan menguji aplikasi ini.

c. Desain dan Rancangan Program

Dalam pembuatan desain, akan merancang sebuah tampilan yang sesuai dan membuat agar mudah digunakan oleh user atau disebut *user friendly*.

d. Pengkodean

Pengkodean dilakukan untuk mempermudah untuk mengimplementasikan ke dalam aplikasi dan menggunakan algoritma SHA 512 dengan menggunakan bahasa pemrogramman PHP.

e. Implementasi

Rancangan aplikasi yang sudah dibuat diimplementasikan berdasarkan analisa masalah yang ada.

f. Pengujian

Setelah selesai membuat aplikasi akan dilakukan sebuah pengujian program untuk mencari kesalahan dalam program yang dibuat agar tidak ada lagi kesalahan pada program yang telah dibuat

Berikut ini adalah beberapa landasan teori yang digunakan dalam penulisan penelitian ini.

2.1 Proses Login

Login adalah proses dimana pengguna memasukkan *username* dan kata sandi untuk dapat mengakses sebuah sistem. Proses *login* pada aplikasi ini akan dilakukan dalam dua langkah, yang pertama dengan menggunakan *username* dan *password*, yang kedua dengan memasukan kode OTP.

Apabila kode verifikasi OTP yang dikirim oleh server sama dengan kode yang berada dalam tabel, barulah pengguna dapat mengakses laman web OTP yang disediakan untuk verifikasi otentifikasi pengamanan akun pengguna web setelah berhasil *Login* dan memasukkan dengan benar *username* dan *password*[2].

Dalam hal ini *username* adalah *userid* yang kemungkinan tidak akan diubah karena merupakan sebuah identitas unik yang merujuk ke *user* tertentu. Sedangkan *password* dapat diubah sesuai dengan kebutuhan, keduanya adalah pasangan yang tidak dapat dipisahkan. Jika kedua pengaman telah berhasil dan memenuhi syarat login maka user sudah memiliki hak untuk masuk ke dalam sistem.

2.2 Otentikasi

Otentikasi (*Authentication*) adalah proses untuk memastikan bahwa kedua ujung koneksi dalam keadaan benar atau sama. Seperti *password* pada umumnya, syarat agar otentikasi berhasil adalah *password* yang dikirimkan *client* harus sama dengan *password* yang disimpan di server.

Dalam permasalahan *password* untuk melakukan otentikasi tidak lagi cukup aman dan model otentikasi yang kuat sangat diperlukan contohnya seperti menggunakan perangkat seperti token (kode) dan sebuah kartu ATM. *Password* sebenarnya digunakan agar lebih aman untuk user tetapi tidak mahal bagi sang penyedia layanan untuk menyediakan keamanan. Namun untuk menghindari penggunaan perangkat tambahan ponsel diadopsi sebagai sebuah keamanan token. Salah satunya kemanan dengan midel otentikasi yang digunakan yaitu dengan menggunakan *One-Time Password* (OTP) yang digunakan untuk memverifikasi penggunanya[3].

2.3 Password

Password adalah sederet karakter berupa huruf, angka atau simbol yang bersifat rahasia yang dimiliki seseorang. *Password* biasanya bersifat statis atau tetap maksudnya, *password* tidak akan berubah sampai pemiliknya mengubahnya.

Orang akan mengubah *password* biasanya ketika merasa tidak aman atau telah terbongkar oleh orang lain atau ada *hacker* yang mencurinya. Contoh satu cara yang digunakan peretas untuk mengetahui atau mencari sebuah informasi akun milik seseorang adalah *sniffing*. *Sniffing* atau dalam bahasa lain pencurian *password* sering juga disebut *password sniffing*. Dalam hal ini adalah suatu teknik pencurian *password* dengan menggunakan bantuan *software* tertentu dengan mengambil sebuah informasi *remote login* seperti *username* dan *password*[2]. *Password* sifatnya sangat rahasia karena apa yang dienkripsi atau yang diberi *password* biasanya adalah hal-hal yang penting oleh karena itu *password* dikatakan hal yang sangat rahasia. Hanya pemilik sendiri yang boleh tahu, tapi tidak memungkinkan jika orang lain boleh tahu asal orang tersebut benar-benar diyakini tidak akan menyebabkan kerusakan pada *file* atau akun anda.

2.4 One Time Password

OTP merupakan metode otentikasi yang menggunakan *password* yang selalu berubah setelah setiap kali *login*, atau berubah setiap interval waktu tertentu[4]. Berbeda dengan penggunaan *password* statis, dalam OTP tidak akan pernah menggunakan kode yang sama setiap user login atau transaksi, sehingga bila ada pihak yang tidak berkepentingan dan tidak bertanggung jawab berhasil merekam *password* OTP yang sudah digunakan maka tidak perlu khawatir karena tidak dapat lagi menggunakan *password* tersebut karena sudah tidak berlaku lagi[5].

2.5 Fungsi Hash

Fungsi *hash* satu-arah (*One-way Hash*) atau hanya bisa dienkrip adalah fungsi sebuah *hash* yang

bekerja dalam satu arah saja, dalam pesan yang sudah diubah, dienkrip atau menjadi *message digest* tidak dapat dikembalikan lagi ke pesan semula. Dua pesan yang berbeda selalu dapat menghasilkan nilai *hash* yang berbeda[3].

a. Fungsi A bisa diterapkan menggunakan blok data dengan ukurarn berapa saja.
b. A menghasilkan sebuah nilai (h) dengan memiliki panjang tetap (*fixed-length output*).
c. A(x) dapat dihitung dalam nilai x yang diberikan.
d. Untuk bilangan a yang didapat, tidak menemukan x sedemikian hingga A(x)=h.
e. Untuk setiap x yang akan diberikan, tidak mungkin mencari y≠x sedemikian sehingga A(y)= H(x).
f. Tidak mungkin untuk mencari sebuah pasangan x dan y sedemikian sehingga menjadi A(x)= H(y).

2.6 *Secure Hash Algorithm* (SHA)

SHA adalah sebuah fungsi hash satu-arah yang dibuat oleh NIST dan biasa dipakai bersama dengan DSS atau disebut *Digital Signature Standard*. SHA juga dapat berdasarkan pada MD4 yang dibuat seseorang bernama Ronald L. Rivest dari MIT. Keamanan dalam SHA biasanya terletak pada sebuah rancangan SHA yang dibuat sedemikian rupa sehingga bila secara komputasi tidak mungkin dapat menemukan pesan yang berkoresponden dengan *message digest* yang diberikan.

Algoritma SHA biasanya akan menerima masukan berupa pesan maksimum 264 bit atau 2.147.483.648 *gigabyte* dan menghasilkan *message digest* yang panjangnya hanya 160 bit. Hal ini lebih panjang dari sebuah *message digest* yang dihasilkan MD5.

Algoritma SHA ini akan dapat digunakan dalam sebuah penelitian untuk membangkitkan kode OTP yang dikirimkan berupa pesan singkat untuk otentifikasi akses ke sistem. OTP biasanya dibangkitkan masukannya berupa ID (untuk admin diambil *field User*), Nomor telepon pengguna dari tabel database user dan waktu ketika user mengakses[2].

2.7 Algoritma SHA-512

Hash yang diciptakan oleh seseorang bernama Ron Rivest. Algoritma ini adalah sebuah pengembangan dari sebuah algoritma sebelumnya, yaitu algoritma SHA-0, SHA-1, SHA-256 dan SHA-384.

Berikut adalah contoh algoritma fungsi hash yang biasa digunakan antara lain MD4, SHA-1 dan MD5 yang merupakan pembaruan dari MD4.

SHA dapat dinyatakan aman, karena secara komputasi tidak dapat ditemukan isi pesan atau didekrip dari *message digest* yang dihasilkan, dan tidak dapat hasil dari dua pesan yang berbeda menghasilkan *message digest* yang sama. Setiap hal yang diubah dan terjadi pada pesan akan menghasilkan *message digest* yang berbeda[6]. Berikut adalah proses Algoritma SHA-512 :

- Start
- Inisialisasi 8 Hash value h[0..7]
- Inisialisasi 80 array konstanta bulat k[0..79]
- Masukkan message dengan panjang L bits
- Tambah '1' bit
- Tambah K '0' bits (dimana K minimal >= 0 agar L + 1 + K + 64 adalah kelipatan 512)
- Tambah L sebagai 64 bit big-endian integer
- Break message menjadi 'chunk' sebesar 1024 bit
- Inisialisasi array w[0..79]
- For (i=0;i<=chunk.size;i++) Then
- For(j=0; j<16;j++) Then
- Copy 'chunk' ke w[j]
- End Loop
- For (k=16;k<80;k++) Then
- s0 := (w[k-15] **rightrotate** 1) **xor** (w[k-15] **rightrotate** 8) **xor** (w[k-15] **rightshift** 7)
- s1 := (w[k-2] **rightrotate** 19) **xor** (w[k-2] **rightrotate** 61) **xor** (w[k-2] **rightshift** 6)
- w[k] := w[k-16] + s0 + w[k-7] + s1
- End Loop
- Inisialisasi a:= h0, b:=h1, c:=h2, d:=h3, e:=h4, f:=h5, g:=h6, h:=h7
- For (j=0;j<80;j++) Then
- S0 := (a **rightrotate** 28) **xor** (a **rightrotate** 34) **xor** (a **rightrotate** 39)
- maj := (a **and** b) **xor** (a **and** c) **xor** (b **and** c)
- temp2 := S0 + maj
- S1 := (e **rightrotate** 14) **xor** (e **rightrotate** 18) **xor** (e **rightrotate** 41)
- ch <- (e **and** f) **xor** ((**not** e) **and** g)
- temp1 := h + S1 + ch + k[j] + w[j]
- H:=g, g:=f, f:=e, e:=d + temp1, d:=c, c:=b, b:=a, a:=temp1 + temp2
- End Loop
- H0:= h0+a, H1:= h1+b, H2:= h2+c, H3:= h3+d, H4:= h4+e, H5:= h5+f, H6:= h6+g, H7:= h7+h
- End Loop
- digest := hash := h0.h1.h2.h3.h4.h5.h6.h7

- Return digest
- End

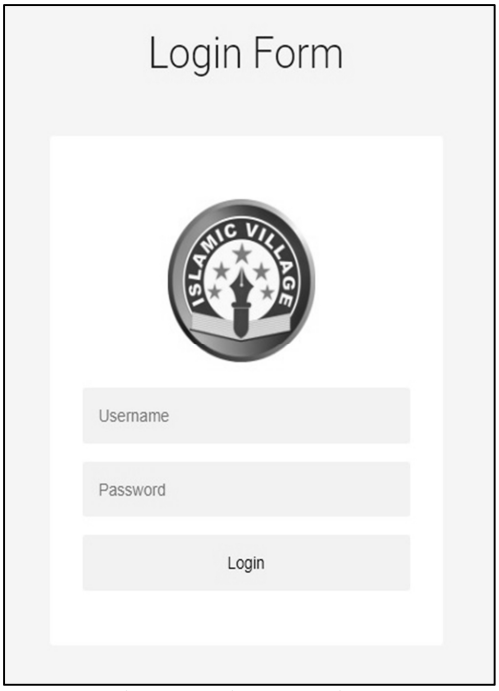
2.8 E-mail

Electronic mail atau disebut surat elektronik adalah sebuah layanan mengirim, menyimpan, dan menerima sebuah pesan melalui sebuah sistem komunikasi elektronik. Istilah surel meliputi sebuah sistem yang berdasarkan *Simple Mail Transfer Protocol* (SMTP) dan intranet yang dapat memungkinkan seorang pengguna dalam satu organisasi mengirimkan pesan kepada satu sama lain[7].

3. HASIL DAN PEMBAHASAN

3.1. Tampilan Layar Halaman Login

Halaman login akan tampil saat admin dan user menjalankan aplikasi ini dan harus mengisi username dan password agar dapat masuk ke dalam aplikasi.



Gambar 1: Tampilan Layar Halaman Home

3.2. Tampilan Layar Halaman Verifikasi

Berikut ini adalah tampilan layar halaman verifikasi yang berfungsi untuk user memasukkan kode verifikasi yang telah dikirim ke nomor handphone yang telah terdaftar.

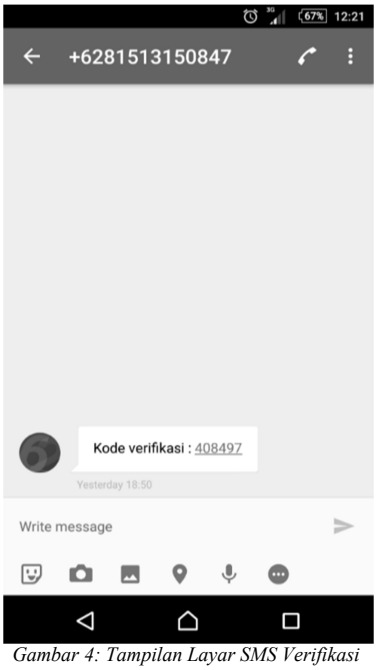
Gambar 2: Tampilan Layar Halaman Verifikasi

3.3. Tampilan Layar Message Box

Gambar 3: Tampilan Layar Message Box

3.4. Tampilan SMS Verifikasi

Berikut ini adalah tampilan Kode verifikasi akan dikirim melaui pesan ke nomor admin atau *user*, kode tersebut harus dimasukkan ke halaman verifikasi agar user dapat masuk ke dalam aplikasi.



Gambar 4: Tampilan Layar SMS Verifikasi

4. Tabel Pengujian

Table 1: Uji Coba OTP

No.	Waktu Login	Kode yang diterima	Waktu Saat Input Kode	Kode yang di input	Hasil
A	09:10	300246	09:11	300246	Berhasil
B	11:46	650368	11:49	650368	Gagal
C	12:56	351830	12:56	65038	Gagal
D	13:33	890503	13:33	890503	Berhasil
E	13:34	256980	13:40	256980	Gagal
F	17:21	133431	17:21	133431	Berhasil
G	17:22	858626	17:22	858626	Berhasil

OTP yang diinputkan menghasilkan kesimpulan sebagai berikut:

a. Berhasil karena memasukan kode verifikasi sebelum 2 menit dan meng*input* kode dengan benar.
b. Keterlambatan dalam menginput kode verifikasi karena lebih dari 2 menit sehingga harus menggunakan kode verifikasi baru.
c. Kesalahan penulisan dalam menginput kode verifikasi karena tidak sesuai dengan kode yang diterima.
d. Berhasil karena menasukan kode verifikasi sebelum 2 menit dan menginput kode dengan benar
e. Kesalahan pada jaringan internet dan sinyal *provider* saat *login* sehingga kode verifikasi diterima terlambat dan tidak bisa dimasukkan karena lebih dari 2 menit.
f. Berhasil karena menasukan kode verifikasi sebelum 2 menit dan menginput kode dengan benar.
g. Berhasil karena menasukan kode verifikasi sebelum 2 menit dan menginput kode dengan benar.

Keterangan di atas adalah hasil uji coba yang telah dilakukan beberapa kali untuk *login* ke dalam aplikasi.

4.1 Analisa Hasil Uji Coba Program

Dalam pembuatan aplikasi sistem penilaian *online* dengan keamanan data *One Time Password* menggunakan Algoritma SHA-512 memiliki beberapa kelebihan dan kekurangan pada aplikasi, berikut adalah kekurangan dan kelebihan aplikasi :

a. Kelebihan Aplikasi
   1) Bersifat *online* dan dapat diakses dimana saja dan bisa melalui handphone
   2) Mudah diakses karena berbasis *web*
   3) Pengguna lain tidak bisa masuk jika tidak memiliki kode verifikasi yang dikirim ke nomor pengguna
b. Kekurangan Aplikasi
   1) Akun admin bersifat permanen akibatnya jika admin sedang tidak aktif, tidak ada admin pengganti.
   2) Batas waktu verifikasi hanya 2 menit, oleh karena itu jika server atau jaringan pada ponsel bermasalah dan pesan masuk lebih dari 2 menit harus menggunakan kode verifikasi yang baru.

5. KESIMPULAN

5.1. Kesimpulan

Berdasarkan bab sebelumnya terhadap permasalahan aplikasi yang telah dikembangkan, maka dapat ditarik kesimpulan mengenai proses OTP dalam masalah keamanan *login* dan sistem penilaian *online* di instansi tersebut, antara lain :

a) Kode *One Time Password* hanya bisa dikirim dari *server* ke nomor *handphone* pengguna.
b) Penggunaan kode OTP dapat melindungi akun jika *password* yang digunakan *user* diketahui oleh orang lain.
c) Batas waktu kode yang diterima hanya 2 menit, jika memasukan kode verifikasi lebih dari 2 menit, kode tidak berlaku dan harus menggunakan kode yang baru..

5.2. Saran

Sistem Penilaian *Online* Menggunakan Keamanan *One Time Password* dengan Algoritma SHA-512 Berbasis Web masih memiliki beberapa keterbatasan. Sehingga disarankan untuk pengembangan selanjutnya seperti ditambahkan fitur untuk menambah admin, agar admin tidak bersifat permanen.

6. UCAPAN TERIMA KASIH

Dalam jalannya penyelesaian penelitian ini penulis ingin mengucapkan terima kasih banyak kepada berbagai pihak yang telah mendukung dan bantuannya, terutama kepada:

a) Allah SWT, yang selalu memberikan rahmat dengan nikmat dan hidayah-Nya hingga penulis dapat mengerjakan dan menyelesaikan penyusunan penelitian ini dengan baik.
b) Orang tua tercinta, yang telah membantu memberikan dukungan baik moral dan material, dan selalu memberikan doa restu, perhatian serta kasih sayangnya.
c) Bapak Prof. Dr. Sc. Agr. Ir. Didik Sulistyanto, selaku Rektor Universitas Budi Luhur.
d) Bapak Goenawan Brotosaputro, S.Kom, M.Sc, selaku Dekan Fakultas Teknologi Informasi Universitas Budi Luhur.
e) Bapak Joko Christian Chandra, M.Kom, selaku Ketua Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Budi Luhur.

f) Ibu Titin Fatimah, M.Kom selaku Dosen Pembimbing yang telah membantu serta memberikan saran-saran dalam penelitian ini.
g) Kepala Sekolah, Wakil Kepala Sekolah, Guru, serta Staf SMA Islamic Village Tangerang yang telah membantu dalam melakukan riset.
h) Teman-teman Fakultas Teknologi Informasi, dan seluruh rekan-rekan seperjuangan yang secara langsung dan tidak langsung membantu penulis dalam penyusunan Tugas Akhir ini dari awal memulai hingga selesai.
i) BEM FTI yang telah menyediakan tempat, dan memberikan semangat.
j) Rizaldi Rahman, Faldhy Mahdi, Miftah Budi, Lathanza, Denny, Maffudh, Nanda, Nindy, Dewi, Wahyu, Faisal, dan teman-teman yang tidak bisa disebutkan satu persatu yang secara langsung maupun tidak langsung memberikan arahan ketika menyelesaikan program, paper, dan memberi dukungan saat mengerjakan.
k) Giri Sarah Mustika yang menyemangati dan membantu mengarahkan ketika dalam penulisan paper.

7. DAFTAR PUSTAKA

[1] Nursahid, Riasti, B.K., and Purnama, B. E., 2015, "Pembangunan Sistem Informasi Penilaian Hasil Belajar Siswa Sekolah Menengah Atas (SMA) Negeri 2 Rembang Berbasis Web," in *Indonesian Journal on Networking and Security*, vol. 4, no. 2, pp. 54–63.

[2] Santoso, K. I., 2013, "Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA," in *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2013*, pp. 204–210.

[3] Santoso, K. I., Sediyono, E., and Suhartono, 2013, "Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasis SMS dengan Hash MD5," in *Jurnal Sistem Informasi Bisnis*, vol. 1, pp. 7–12.

[4] Musliyana, Z., Arif, T. Y., and Munadi, R., 2016, "Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia," in *Jurnal Rekayasa Elektrika*, vol. 12, no. 1, p. 21.

[5] Sakti, D. V. S. Y., Agani, N., and Hardjianto, M., 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 Berbasis Android," vol. 13, no. 1, pp. 64–73.

[6] Sembiring, J., 2013, "Analisis Algoritma SHA-512 Dan Watermarking Dengan Metode Least Significant Bit Pada Data," pp. 2–4.

[7] Nugroho, N. B., Azmi, Z., and Arif, S. N., 2016, "Aplikasi Keamanan Email Menggunakan Algoritma RC4," in *Jurnal SAINTIKOM*, vol. 15, no. 3, pp. 81–88.