IMPLEMENTASI *ONE TIME PASSWORD* DENGAN ALGORITMA *HASH* SHA-512 BERBASIS *WEB* UNTUK KEAMANAN DATA SISWA

Muhamad Nur Faizal Afrianto[1)], **Siswanto**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : 1411502907@student.budiluhur.ac.id[1)], siswanto@budiluhur.ac.id[2)]

Abstrak

Oleh karena itu suatu sistem informasi membutuhkan sebuah sistem login, namun penggunaan password pada saat login belum menjamin keamanan dan kerahasiaan sebuah data maupun informasi dan dirasa kurang efektif untuk keamanan hak akses karena penggunaan password yang statis sehingga mudah ditebak. Selain itu password juga dapat diketahui dengan cara sniffing atau penyadapan. Oleh karena itu SMAN 12 Tangerang membutuhkan sebuah sistem otentikasi lebih, yaitu berupa password unik untuk login yang hanya dapat digunakan sekali saja yang disebut One Time Password. Penggunaan telepon genggam yang meningkat, serta validasi nomer telepon atau kartu sim yang wajib terdaftar pada e-ktp agar sesuai dengan NIK dan KK semakin memperkuat otentikasi. Oleh karena itu dalam penelitian ini menggunakan telepon genggam sebagai penerima kode verifikasi yang dikirim melalui sms ke nomor telepon pengguna sebanyak enam digit, lalu kode yang telah diterima melalui sms kemudian dimasukkan ke permintaan kode pada saat setelah login dan sebelum input nilai untuk verifikasi, bila status kode One Time Password valid maka pengguna dapat masuk ke sistem informasi sebagai penggguna, namun bila status kode One Time Password tidak valid maka pengguna tidak dapat login, sehingga keamanan suatu sistem informasi dapat terjaga. Aplikasi ini berbasis web dengan bahasa pemrograman PHP dan MySQL sebagai database, dimana algoritma yang digunakan ialah Hash SHA-512. Dengan memberikan keamanan tambahan yang berupa password unik pada login pengguna diharapkan aplikasi yang dibuat dengan berbasis web ini dapat menjaga keamanan suatu informasi penting pada SMAN 12 Tangerang.

Kata kunci: *One Time Password, Hash,* SHA-512

1. PENDAHULUAN

Sistem informasi untuk keperluan sekolah saat ini semakin banyak, diantaranya sistem informasi penilaian siswa, sistem penilaian pada sekolah biasanya masih menggunakan Microsoft Office Excel, seperti yang terjadi pada SMAN 12 Tangerang. Namun penggunaan Microsoft Office Excel dirasa menyulitkan karena penggunaanya yang kurang *user friendly*. Oleh karena itu banyak sekolah-sekolah yang ingin mulai beralih menggunakan sistem informasi yang *user friendly*, salah satunya dengan menggunakan sistem informasi berbasis web seperti yang ingin dilakukan oleh SMAN 12 Tangerang. Dengan sistem informasi berbasis web pengguna merasakan kemudahan untuk pengolahan data. Pemanfaatan jaringan komputer untuk keamanan dalam sebuah sistem yang terintegrasi menjadi bagian yang sangat penting. Salah satu masalah yang di hadapi dalam keamanan pada jaringan komputer adalah bagaimana sistem dapat memastikan bahwa *user* yang mengakses data maupun informasi pada sistem tersebut adalah *user* yang benar-benar memiliki wewenang.

Penggunaan *password* pada saat *login* untuk mengakses sistem informasi juga menjadi sangat rentan keamanannya karena biasanya pengguna selalu menggunakan *password* yang sama (*password* statis) dan jarang sekali merubah atau memperbarui *password* secara berkala.

Proses *login* pada aplikasi ini akan dilakukan dalam dua langkah. Langkah yang pertama adalah *login* dengan *username*. Langkah yang kedua adalah *login* dengan memasukkan OTP. Alur kasus penggunaan fungsi ini adalah pengguna terlebih dahulu melakukan proses registrasi agar *username* terdaftar pada sistem. Kemudian pengguna memasuki halaman *login* yang pertama. Selanjutnya pengguna memasukkan *username*. Apabila *username* yang dimasukkan salah, pengguna telah gagal melakukan *login* tahap 1. Akan tetapi jika *username* yang dimasukkan benar, maka sistem akan mengarahkan pengguna ke halaman CAPTCHA. Apabila pengguna lolos dalam tes CAPTCHA maka sistem akan mengirimkan OTP ke aplikasi instant messaging. Selanjutnya pengguna harus memasukkan OTP yang telah dikirimkan di halaman *login* OTP yang telah disediakan. Apabila OTP yang dimasukkan benar, maka pengguna akan bisa memasuki sistem. Akan tetapi jika salah atau melebihi waktu yang diberikan, maka pengguna harus melakukan proses *login* dari awal [1].

Selain itu *password* juga dapat diketahui dengan cara *sniffing* atau penyadapan. Pengguna juga sudah terbiasa dengan sistem semacam ini sehingga waktu penyesuaian bisa diminimalkan [2].

Penelitian yang dilakukan dengan menggunakan metode *Secure Hash Algorithm* untuk mengimplementasikan OTP.[6] Ada pula yang mengimplementasikan OTP dengan Dual Channel.

[1] Dari beberapa penelitian tersebut, OTP dapat menjadi solusi yang cukup tepat dalam mengamankan data dalam sistem informasi penilaian sekolah.

Salah satu metode kriptografi, yaitu fungsi *hash* digunakan untuk dapat membuat sebuah *password* OTP dan untuk pemilihan karakternya dipilih secara acak dengan *Pseudo Random Number Generator*[3].

User atau komputer di ijinkan untuk mengakses sebuah sistem komputer dan seluruh sumber daya di dalamnya jika sudah di autentikasi oleh komputer yang bersangkutan. Untuk mengamankan sistem komputer dari *user* yang tidak berhak maka di perlukan mekanisme autentikasi yang kuat. Berikut adalah beberapa jenis autentikasi yang biasanya digunakan untuk mengamankan sistem komputer, yaitu *Username* dan *Password*, *Kerberos*, CHAP (*Challenge Handshake Authentication Protocol*), *Digital Certificates*, *Tokens, Multi-Factor Authentication, Mutual Authentication, Biometric*[4].

Teknologi digital yang digunakan sangat bervariasi dari yang berbasis GSM, *Time Division Multiple Access* (TDMA), hingga *Code Division Multiple Access* (CDMA) [5].

Dalam membangkitkan OTP ini akan diterapkan dengan metode *Hash* SHA-512. Fungsi *hash* dapat menerima masukkan string apa saja. Jika string menyatakan pesan *(message),* maka sembarang pesan M berukuran bebas dikompresi oleh fungsi *hash* H melalui persamaan: h=H(M). Keluaran fungsi *hash* disebut juga nilai *hash (hash-value)* atau pesan-ringkas *(message digest)*.. Untuk setiap h yang diberikan, tidak mungkin menemukan x sedemikian sehingga H(x)=h. Itulah sebabnya fungsi H dikatakan fungsi *hash* satu arah [3].

Beberapa keuntungan yang diperoleh dengan metode yang digunakan antara lain OTP dengan Hash SHA memiliki hasil yang tidak mungkin sama sehingga sulit ditebak oleh *hacker* dan lebih baik dibandingakan dengan hash MD5 [6].

Algoritma SHA menerima masukan berupa pesan dengan ukuran maksimum 264 bit (2.147.483.648 gigabyte) menghasilkan message digest yang panjangnya 160 bit. Lebih panjang dari *message digest* yang dihasilkan MD5 [6].

angkah-langkah pembuatan *message digest* dengan algoritma SHA-512 adalah sebagai berikut : Input pesan yang akan di *hash* SHA-512. Ubah pesan menjadi deretan biner. Penambahan bit-bit pengganjal, yaitu dengan menambahkan pesan dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 896 mod 1024. Ini berarti setelah menambahkan bit-bit pengganjal, kini panjang pesan adalah 128 bit kurang dari kelipatan 1024. Angka 1024 muncul karena algoritma SHA-512 memproses pesan dalam blok-blok yang berukuran 1024. Apabila terdapat pesan dengan panjang 24 bit, maka pesan tersebut akan tetap ditambahkan dengan 896-(24+1)=81 bit. Jadi panjang bit-bit pengganjal antara 1 sampai 896. Penambahan nilai panjang pesan semula, yaitu pesan ditambah lagi dengan 128 bit yang menyatakan panjang pesan semula. Apabila panjang pesan lebih besar dari 2128 maka yang diambil adalah panjangnya dalam modulo 2128. Dengan kata lain, jika pada awalnya panjang pesan sama maka K bit, maka 128 bit yang ditambahkan menyatakan K modulo 2128. Sehingga setelah proses kedua ini selesai dilakukan maka panjang pesan sekarang adalah 1024 bit.

2. METODE PENELITIAN

Dalam penulisan penelitian ini, digunakan metode pengembangan dengan model *Software Development Life Cycle* (SDLC) yaitu metode *waterfall*. Tahapan SDLC dengan metode *waterfall* meliputi tahapan pengumpulan data, analisis, desain, pembuatan program, pengujian dan implementasi. Berikut ini adalah rincian tahapan dalam pembuatan aplikasi.

(1) Pengumpulan Data
Mengumpulkan data yang dibutuhkan dari keseluruhan elemen sistem yang akan di aplikasikan ke dalam bentuk perangkat lunak, dan mengumpulkan data mengenai data siswa dan data penilaian siswa di SMAN 12 Tangerang, *One Time Password*, serta algoritma *Hash* SHA-512.

(2) Analisa Kebutuhan Aplikasi
Setelah mengumpulkan dan memperoleh data yang dibutuhkan, kemudian dipelajari dan dianalisa mengenai fungsi-fungsi apa saja yang diperlukan untuk mengimplementasikan aplikasi ini.

(3) Desain Perancangan Program
Merancang tampilan layar aplikasi seperti rancangan layar halaman home, profil, input data siswa, input nilai siswa, lihat data siswa serta cek nilai dengan pemodelan *OOAD (Object Oriented Analysis and Design)* dan *Unified Modelling Language (UML)* yang akan dibangun sesuai dengan kebutuhan aplikasi sehingga dapat mempermudah dalam proses pengkodean.

(4) Pengkodean
Dilakukan untuk memudahkan dalam mengimplementasikan rancangan aplikasi kedalam algoritma *Hash* SHA-512 dengan menggunakan bahasa pemrograman PHP.

(5) Pengujian
Pengujian dilakukan setelah aplikasi selesai dibuat dengan melakukan beberapa pengujian program dan mencari kesalahan pada program hingga tidak ada lagi kesalahan program dan program sudah berjalan sesuai dengan yang dirancang.

(6) Implementasi

Rancangan aplikasi yang sudah dibuat kemudian diimplementasikan dengan data yang sesungguhnya.

3. HASIL DAN PEMBAHASAN

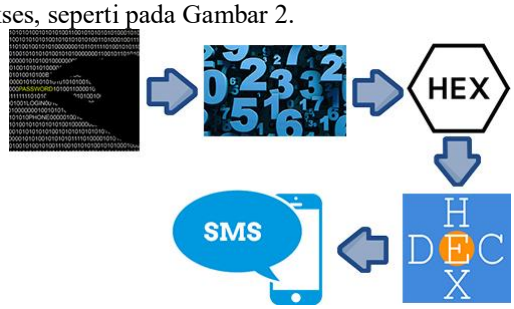
3.1 Proses Bisnis Aplikasi

Proses bisnis merupakan suatu rangkaian kegiatan yang saling terkait untuk menyelesaikan suatu masalah tertentu. Proses bisnis dalam penulisan ini akan menjelaskan contoh proses bisnis pada proses *login* yang dilakukan oleh *user Admin* dan Siswa seperti pada Gambar 1.

Gambar 1: Proses Bisnis Aplikasi

Tahapan masukan, proses dan hasil OTP sebagai berikut: *User* melakukan *login* dengan mengisi *username* dan *password*, *username* default untuk siswa adalah Nomor Induk Siswa. *User* menerima sms berisi kode verifikasi berupa angka sebanyak 6 digit. *User* memasukkan kode verifikasi ke form verifikasi yang muncul setelah melakukan *login*. Jika kode verifikasi sesuai maka *user* dapat masuk ke sistem informasi penilaian siswa.

Proses bisnis untuk men-*generate* kode OTP diambil dari parameter nomor telepon, *password* dan waktu akses, seperti pada Gambar 2.

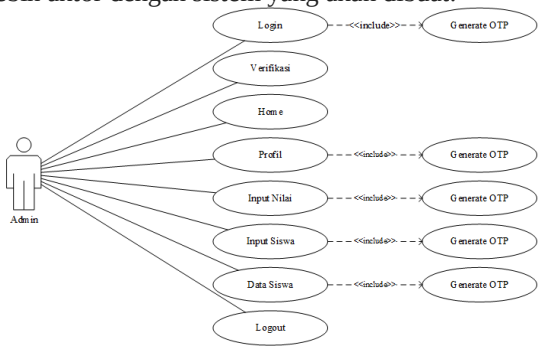


Gambar 2: Proses Bisnis Generate OTP

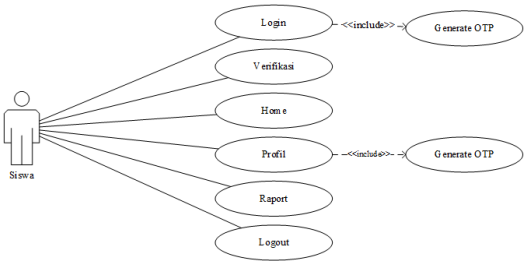
Tahapan proses untuk *generate* kode OTP adalah sebagai berikut: Mengambil data waktu akses, nomer telepon dan *password*. Mengacak data yang telah diambil menggunakan metode *Hash* SHA-512. Merubah hasil SHA-512 kedalam hexadecimal. Merubah hexadecimal kedalam decimal. Mengirim hasil decimal malalui SMS.

3.2 *Use case* Diagram

Use case diagram menggambarkan kelakuan (behavior) sistem yang akan dibuat. Mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang akan dibuat.



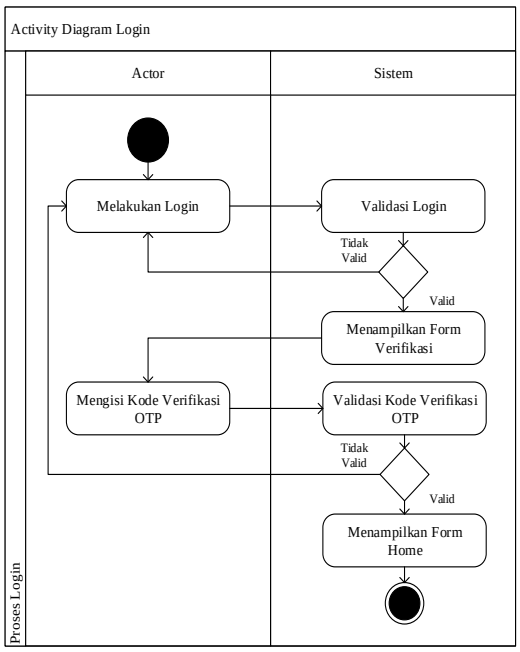
Gambar 3: Use Case Diagram User Admin



Gambar 4: Use Case Diagram User Siswa

3.3 Activity Diagram

Setelah memvisualisasikan sistem secara umum melalui *Use Case Diagram*, aktivitas di dalam sistem dapat diperjelas melalui *Activity Diagram*. Pada diagram ini, digambarkan aktifitas dari proses *login*, seperti pada Gambar 5.

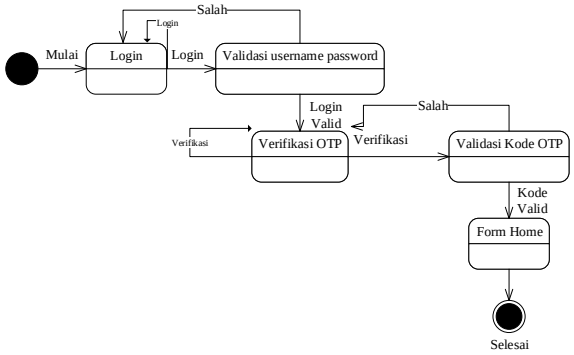


Gambar 5: Activity Diagram Login

3.3 *Statechart* Diagram

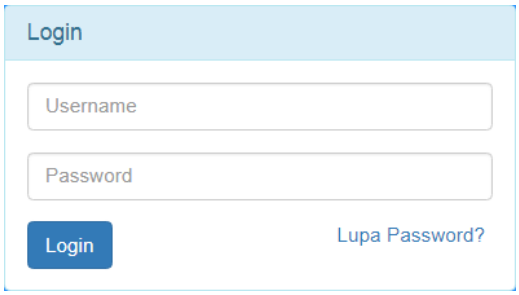
Di dalam menggambarkan urutan proses pada aplikasi ini, digunakan *Statechart* untuk

memperjelas aliran proses, statechart diagram menggambarkan transisi dan perubahan keadaan dari satu *state* ke *state* lainnya untuk suatu objek pada sistem sebagai akibat dari stimuli yang diterima. Berikut adalah *statechart* diagram pada proses *login*, seperti pada Gambar 6.



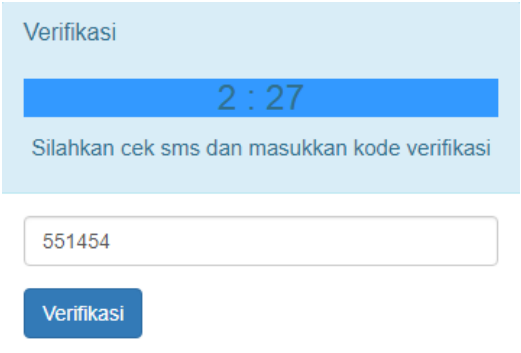
Gambar 6: Statechart Diagram Login

Pada saat mengakses web student SMAN 12 Tangerang, *user* melakukan *login* dengan memasukkan *username* dan *password*, seperti pada Gambar 7. Namun *username* dan *password* dapat diketahui jika dilakukan *keylogger*, *sniffing* dan sebagainya.



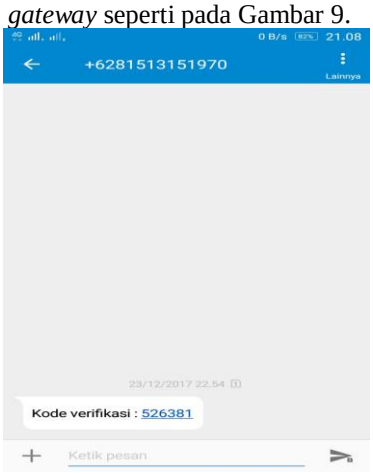
Gambar 7: Tampilan Form Login

Maka untuk pengamanan *login* ditambahkan metode verifikasi OTP yang dikirim melalui SMS ke nomor telepon pengguna. Selanjutnya pengguna harus memasukkan kode verifikasi OTP tersebut seperti pada Gambar 8.



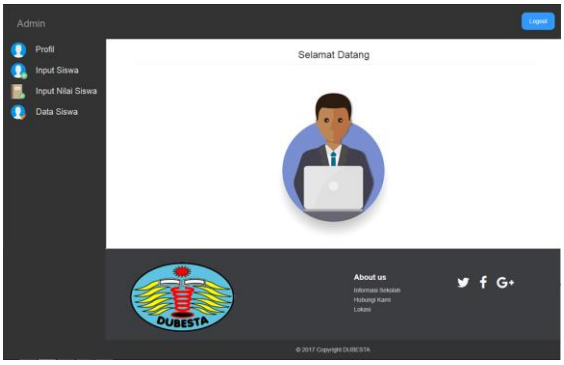
Gambar 8:Tampilan Form Input Kode Verifikasi OTP

Apabila selama dua menit 30 detik berlalu *user* belum memasukkan OTP, maka akan kembali ke halaman *login*. Hasil dari generate OTP dengan SHA-512 dikirim melalui SMS dalam rentang waktu sekitar maksimal tiga menit karena ketentuan dari *server* SMS *gateway* seperti pada Gambar 9.



Gambar 9: SMS Kode Verifikasi OTP

Berikut adalah Tampilan Layar *Form Home Admin*, terdapat pilihan beberapa menu yang dapat di akses Admin yaitu menu profil, *input* siswa, *input* nilai, serta data siswa, dapat dilihat pada Gambar 10.



Gambar 10: Tampilan Layar Form Home Admin

Berikut adalah Tampilan Layar *Form Home* Siswa, terdapat dua menu yaitu Profil dan Raport, dapat dilihat pada Gambar 11.

Gambar 11: Tampilan Layar Form Home Siswa

Dalam tabel pengujian akan terlihat hasil dari kode verifikasi, mulai dari *Login*, *Update* Profil, *Input* Siswa, *Input* Nilai Siswa, serta *Update* Data Siswa. Dalam pengujian ini juga terlihat perbedaan dari setiap kode verifikasi yang muncul yang menandakan bahwa kode verifikasi yang dikirim melalui SMS ke nomor telepon pengguna hanya berlaku satu kali.

Tabel 1: Hasil Uji Coba Pada Setiap Aktifitas

Proses	Waktu kode diterima	Kode yang diterima	Waktu input kode	Kode yang di input	Hasil
Login	23:35	114554	23:36	114554	Berhasil
Update Profil	23:38	252654	23:38	252654	Berhasil
Input Siswa	23:42	872710	-	-	Gagal
Input Nilai Siswa	23:52	684580	23:53	684580	Berhasil
Update Data Siswa	23:55	719075	23:55	684580	Gagal

Dari pengujian program yang dilakukan beberapa kali pada program yang dijelaskan pada tabel 1, menghasilkan keterangan seperti sebagai berikut: Proses *login* berhasil karena kode verifikasi yang di *input* sesuai dengan kode verifikasi yang dikirim melalui SMS, dan meng-*input* kode verifikasi sebelum 2 menit 30 detik berlalu. Proses *Update* profil berhasil karena kode verifikasi yang di *input* sesuai dengan kode verifikasi yang dikirim melalui SMS, dan meng-*input* kode verifikasi sebelum 2 menit 30 detik berlalu. Proses *Input* Siswa Gagal karena kesalahan jaringan internet dan sinyal provider sehingga kode verifikasi yang diterima melalui SMS terlambat sehingga tidak dapat meng-*input* kode verifikasi sesuai waktu(Verifikasi Time Out). Proses *Input* nilai siswa berhasil karena kode verifikasi yang di *input* sesuai dengan kode verifikasi yang dikirim melalui SMS, dan meng-*input* kode verifikasi sebelum 2 menit 30 detik berlalu. Proses *Update* data siswa gagal karena kode verifikasi yang di *input* tidak sesuai dengan kode verifikasi yang dikirim melalui SMS.

3.4 Kelebihan dan Kekurangan Aplikasi

Kelebihan Aplikasi :
Pengguna lain tidak akan bisa mengakses jika tidak mempunyai kode verifikasi yang dikirim melalui SMS ke nomor telepon pengguna. Keamanan hak akses lebih terjaga walaupun *password login* diketahui serta kode verifikasi yang dikirim melelui SMS ke nomor telepon pengguna hanya berlaku satu kali.

Kekurangan Aplikasi :
Hanya menggunakan algoritma SHA-512 untuk proses pembangkitan OTP dan belum dikombinasikan dengan algoritma lain. Pengguna harus memasukkan kode verifikasi sebelum batas waktu berakhir, karena jika SMS kode verifikasi tidak terkirim harus mengulang proses untuk mengirimkan SMS kode verifikasi.

4. KESIMPULAN

Berdasarkan dari uraian bab sebelumnya terhadap permasalahan dan aplikasi yang telah dikembangkan, maka dapat ditarik kesimpulan mengenai proses OTP terhadap masalah keamanan *web student* di instansi tersebut, antara lain:

Algoritma *Hash* SHA-512 dengan metode *One Time Password* dapat diimplementasikan pada aplikasi yang dibuat serta aplikasi dapat mengamankan data siswa dengan metode *One Time Password* yang dikirim melalui SMS ke nomor telepon pengguna untuk melakukan verifikasi saat mengakses aplikasi.

Implementasi *One Time Password* dengan Algoritma *Hash* SHA-512 Berbasis Web Untuk Keamanan Data Siswa Pada SMAN 12 Tangerang ini masih memiliki beberapa keterbatasan, sehingga untuk itu penulis menyarankan untuk pengembangan apliksai selanjutnya seperti :

Mengembangkan aplikasi dengan menambahkan metode atau algoritma lain serta menambahkan fungsi kirim ulang SMS jika SMS tidak terkirim untuk mendapatkan kode verifikasi baru agar pengguna tidak mengulang proses *login*.

5. DAFTAR PUSTAKA

[1] D. R. L.H, W. Wibisono, and B. A. Pratomo, "Pengembangan Mekanisme One Time Password dengan Menggunakan Strategi Dual Channel pada Aplikasi Web," *J. Tek. Pomits*, vol. 2, no. 1, pp. 1–6, 2013.

[2] W. S. Raharjo, I. D. E.K.Ratri, and H. Susilo, "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. April, pp. 127–136, 2017.

[3] 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," *BIT*, vol. 13, no. 1, pp. 64–73, 2016.

[4] M. R. Arief, "AUTENTIKASI, KENDALI AKSES, AUDIT SISTEM KEAMANAN JARINGAN KOMPUTER M. Rudyanto Arief," *DASI*, vol. 11, no. 3, pp. 73–76, 2010.

[5] A. Arif and P. Mandarani, "Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit Pada Sistem Keamanan Short Message Service (SMS) Berbasis

Android," *Teknoif*, vol. 4, no. 1, pp. 1–10, 2016.

[6] K. I. Santoso, "Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA," *Semin. Nas. Teknol. Inf. Komun. Terap. 2013*, no. November, pp. 204–210, 2013.