PENERAPAN *HYBRID SHAPE TEXTUAL LOGIN* PADA *SMARTPHONE* ANDROID SEBAGAI KONTROL AKSES

Fajar Dimar Habibi[1)], Ni Putu Ayu Lhaksmi W[2)], Yose Supriyadi[3)]
[1,2]Teknik Persandian, Sekolah Tinggi Sandi Negara
[3]Manajemen Persandian, Sekolah Tinggi Sandi Negara
Jalan H. Usa Raya, Ciseeng,Bogor, 16120
HP: +628993824492
E-mail: fajardimarh@gmail.com[1)], ayulhaksmy@yahoo.com[2)], yose@stsn-nci.ac.id[3)]

Abstrak

Login memegang peran penting dalam mendapatkan akses informasi terhadap sistem. Pada skema login konvensional, pengguna hanya memberikan password dan username untuk mendapatkan akses. Hal tersebut rawan terhadap shoulder surfing dan kamera tersembunyi yang digunakan untuk merekam password. Sementara password berbasis teks, gambar dan biometric memiliki kelemahan terhadap brute force attack, dictionary attack, shoulder surfing dan membutuhkan sumber daya yang besar. Terdapat metode pair based text authentication yang digunakan untuk mengatasi shoulder surfing akan tetapi memiliki kekurangan dalam keefektifan dan keefisienan pada proses login. Pada penelitian ini dijelaskan mengenai skema hybrid shape textual login sebagai solusi dalam melakukan login pada aplikasi perangkat smartphone Android. Skema ini menggunakan bentuk pada kolom-kolom yang berisikan alfanumerik dan simbol acak yang dinamis untuk mengidentifikasi password pengguna. Berdasarkan analisis skema ini kuat terhadap serangan brute force attack dan shoulder surfing serta terbukti efektif, efisien dan kuat terhadap dictionary attack.

Kata kunci: *kontrol akses, hybrid shape textual login, shoulder surfing resistant*

Abstract

Login has important role to get an access to information on the system. In conventional login scheme, users simply provide a password and username to gain access. It has vulnerability to the shoulder surfing attack. Furthermore text-based password, images and biometric respectively are weak against brute force attack, dictionary attack, shoulder surfing attack and need huge resource. However, the pair based text authentication method can be used to overcome shoulder surfing attack but it lack of effectiveness and efficiency in the login process. This research explain the scheme of hybrid shape textual login as a solution. This scheme uses the form on the columns that contains dinamic alphanumeric and random symbol to identify user's passwords. Based on the analysis and testing that has been carried out, this scheme robust against brute force attacks, dictionary attacks and shoulder surfing attack and have a better level of effectiveness and efficiency.

Keywords: *access control, hybrid shape textual login, shoulder surfing resistant*

1. PENDAHULUAN

Berdasarkan riset yang dikeluarkan oleh *Sharing Vision* pada tahun 2013, penggunaan *Smartphone* Android di Indonesia mencapai 60%, angka tersebut mengungguli penggunaan *Operating System* lainnya, dengan pertumbuhan jumlah pengguna lebih dari 1, 5 juta per hari [1]. Penggunaan perangkat Android tidak hanya sekedar melakukan kirim terima SMS ataupun telepon. Penelitian terkait yang dilakukan oleh MoboMarket, dilansir oleh berita detik.com penggunaan Android juga digunakan untuk bermain–*game* (43%), *social media* (12%) dan fotografi (11%) serta aplikasi lainnya (34%) [2].

Kesuksesan Android di Indonesia memancing *hacker* untuk melakukan pencurian data pribadi seperti *username* dan *password*. Berdasarkan riset yang dikeluarkan oleh perusahaan *antivirus* Kaspersky bahwa 20.000 *smartphone* Android berbagai jenis dalam keadaan kritis terhadap pencurian data yakni sebesar 87,7% di seluruh dunia termasuk di dalamnya Indonesia [3]. Salah satu cara pencurian data yang populer yang pernah diterbitkan oleh perusahaan antivirus McAfee adalah serangan *shoulder surfing* terhadap data

pengguna [4]. Salah satu contoh kerugian akibat *shoulder surfing* yang dilansir oleh jagatreview.com pada awal tahun 2016 yakni seorang anak menghabiskan Rp 81 Juta untuk membeli barang dalam aplikasi pada *smartphone* ayahnya karena sang anak dapat melakukan *bypass* kode *pass* di dalam *smartphone* tersebut [5].

Untuk mengatasi permasalahan yang telah dipaparkan, terdapat beberapa metode pengamanan untuk melindungi *password* seperti *password* berbasis gambar ataupun *biometric* [6]. Metode tersebut memiliki beberapa kekurangan yakni metode *biometric* seperti sidik jari, iris mata, pengenalan wajah dan pola tanda tangan memiliki kelemahan yaitu sumber daya yang digunakan sangat besar serta membutuhkan biaya yang mahal [6]. Sedangkan, penggunaan *password* berbasis gambar memiliki kelemahan besar terhadap *shoulder surfing* [6]. *Smartphone* Android memiliki beberapa metode yang umum digunakan untuk mengamankan ponsel yakni PIN, Android *Unlock pattern* dan *biometric* [7]. Metode tersebut memiliki kelemahan yakni PIN dan *pattern* memiliki kelemahan yaitu mudah dilakukan *guessing password*, serta memiliki kerawanan terhadap *shoulder surfing* sedangkan pada metode biometrik memiliki kelemahan seperti yang telah dijelaskan sebelumnya [7].

Permasalahan serangan *shoulder surfing* dapat diatasi dengan metode *Pair Based Authentication Schemes.* Metode tersebut memiliki kekurangan yakni pengguna harus meng-*input*-kan dua kali panjang *password* yang didaftarkan (perpotongan baris dan kolom) sehingga waktu yang dibutuhkan untuk melakukan otentikasi lebih lama dibandingkan menggunakan metode otentikasi normal seperti PIN (*Personal Identification Number*) ataupun *password* [8]. Oleh karena itu, metode tersebut menyebabkan kesalahan pengguna dalam menekan tombol sebesar 45% dan kegagalan melakukan *login* mencapai 14% [8].

Berdasarkan hal tersebut diperlukan sebuah metode otentikasi yang dapat digunakan untuk mengamankan *smartphone* Android dari *bypass* sistem menggunakan *dictionary attack* serta mampu melindungi dari *shoulder surfing* yang memiliki tingkat keefektifan yang lebih baik dalam mengamankan *smartphone* Android. Untuk mengatasi permasalahan tersebut pada makalah ini akan diusulkan metode baru untuk mengatasi masalah *shoulder surfing* yang lebih efektif, efisien serta *user friendly* yaitu dengan *Hybrid Shape Textual Password* yang diadopsi dari [9] dengan melanjutkan usulan perbaikan penelitian dengan meningkatkan sisi keamanan yang dihasilkan dari *password*. *Hybrid Shape Textual Password* adalah skema yang berbasis bentuk pola dan *text* [9]. Setiap kolom diisi oleh karakter acak alfanumerik dan simbol yang dinamis dengan ukuran matriks 8 x 8. Ide dasar dari skema ini adalah index dari setiap karakter memetakan letak karakter pada tabel yang tersedia sehingga dapat membentuk pola yang digunakan sebagai *password*. Berdasarkan *survey*, penggunaan pola dipilih karena lebih cepat dan mudah diingat dibandingkan dengan metode otentikasi lainnya [10].

Dari latar belakang yang telah dipaparkan, pada makalah ini akan dipaparkan simulasi kontrol akses aplikasi *smartphone* berbasis Android yang efektif, efisien dan tahan terhadap *dictionary attack* serta *user friendly* dengan menggunakan skema *Hybrid Shape Textual Login.*

2. LANDASAN TEORI

2.1 Otentikasi

Menurut Menezez pada [11] tidak dibedakan antara identifikasi dan otentikasi entitas yakni teknik yang digunakan untuk menjamin satu pihak (dengan penambahan bukti yang asli) dari kedua belah pihak dapat memastikan terlibat langsung. Terdapat tiga basis metode otentikasi [12], yaitu:

a) *Something you know*. Merupakan metode otentikasi yang menggunakan tantangan dan respon dimana pihak yang akan diotentikasi harus merespon dengan pengetahuan yang mereka tau. Misalnya *password* standar, penggunaan *Personal Identification Number* (PIN). Metode ini merupakan metode yang paling mudah dari fase otentikasi.
b) *Something you have*. Metode ini merupakan faktor tambahan yang harus dimiliki oleh pihak yang ingin diotentikasi untuk membuktikan kebenaran identitas pengguna. Biasanya berupa aksesoris fisik yang biasa dibawa dan digunakan, misalnya kartu *magnetic-striped*, *chipcards*, ATM *card*, dan token.
c) *Something you are*. metode ini menggunakan karakteristik fisik manusia (biometrik) yang digunakan untuk membuktikan identitasnya misalnya tanda tangan, *fingerprint*, pola retina, geometri tangan, pengenalan suara.

Jika dilihat dari basis metode yang telah disebutkan di atas maka *hybrid shape textual login* termasuk dalam *something you know* karena berdasarkan sesuatu yang pengguna tahu.

2.2 Kontrol Akses

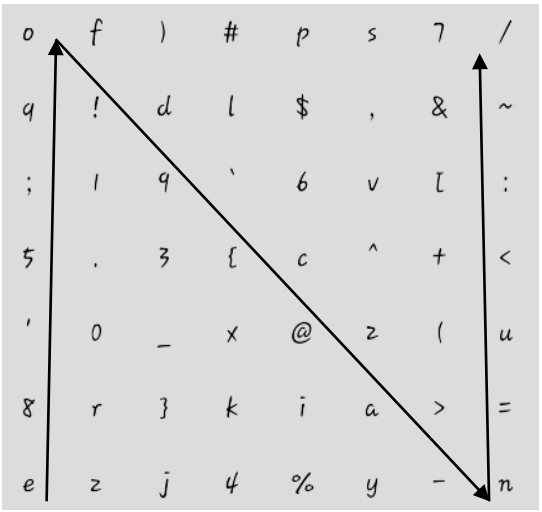
Kontrol akses adalah proses dalam mengatur dan mengendalikan pengguna untuk dapat melakukan akses terhadap sumber daya yang terdapat pada sistem [12].Terdapat tiga jenis model kontrol akses yaitu [12]:

a) *Discretionary Access Control* (DAC), kontrol akses ini memberikan pengguna kontrol secara keseluruhan terhadap objek yang mereka berikan akses kebebasan untuk mengontrolnya. Termasuk dalam hal ini *sharing* objek dengan pengguna lain. Sistem yang menggunakan model DAC ini adalah Standard UNIX dan Windows
b) *Mandatory Access Control* (MAC), kontrol akses jenis ini berdasarkan status pengguna dan label dari objek yang diberikan akses untuk diubah, label dari objek tersebut dapat berupa *confidential, secret, top secret.* Pengguna dapat melakukan pengaksesan terhadap objek dengan syarat mereka harus memiliki kewenangan yang setara dengan label.
c) *Role-Bases Access Control* (RBAC), kontrol akses jenis ini mendefinisikan bagaimana informasi tersebut dapat diakses berdasarkan peran dari penggunanya. Contohnya peran sebagai pengguna hanya diberikan akses terhadap akun yang dia miliki sedangkan sebagai administrator dapat mengubah keseluruhan akun yang telah terdaftar pada sistem.

Penerapan kontrol akses pada *hybrid shape textual login* ini dapat digunakan untuk membatasi pengguna dalam mengakses sistem sehingga hanya pengguna yang sah yang dapat melakukan akses terhadap aplikasi pada *smartphone* pengguna.

2.3 *Hybrid Shape Textual Login*

Hybrid Shape Textual Login merupakan skema yang diadopsi dari [9] dengan melanjutkan usulan perbaikan penelitian dengan meningkatkan sisi keamanan yang dihasilkan dari *password*. Skema ini berbasis bentuk dan *text* yang dapat diterapkan tidak hanya pada komputer biasa akan tetapi dapat juga diterapkan pada perangkat *mobile* [9]. Ide dasar dari skema ini adalah index dari setiap karakter yang memetakan antara letak dan karakter yang ada pada tabel yang tersedia. Untuk lebih mempersulit penyerang maka pada setiap kolom diisi oleh karakter acak alfanumerik dan simbol dengan ukuran matriks 8x8 yang akan diterapkan pada *smartphone* Android. Ukuran matriks tersebut dipilih karena cocok dengan ukuran layar *smartphone* di pasaran.



Gambar 1. Skema Password Hybrid Shape Textual Login

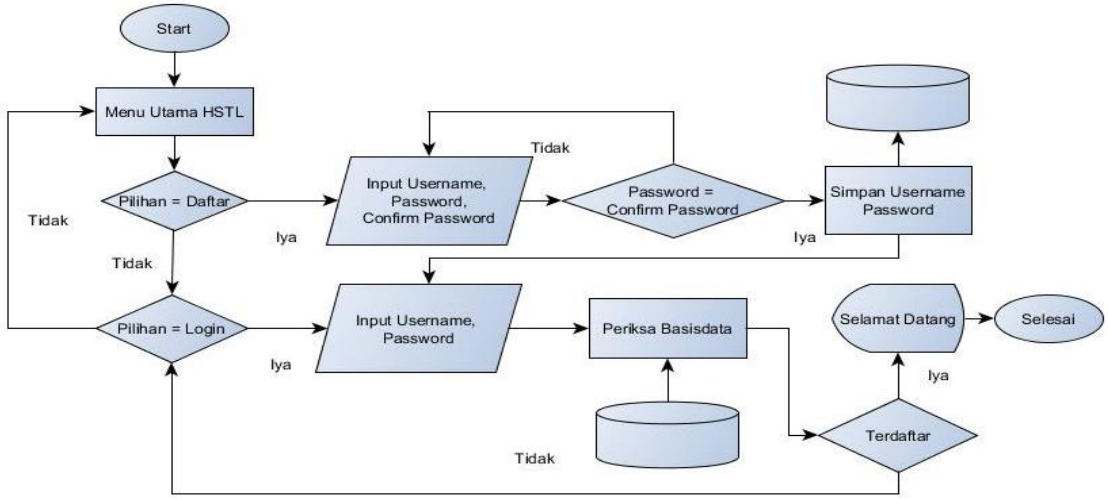
3. SIMULASI

Pada tahap ini akan disimulasikan aplikasi *Hybrid Shape Textual Login* menggunakan IDE (*integrated development environment)* Android Studio 2.1.2 dan dijalankan pada perangkat Android LG K8. Simulasi yang digunakan menggunakan basisdata SQLite yang sudah ada pada Android untuk menyimpan *password* pengguna.

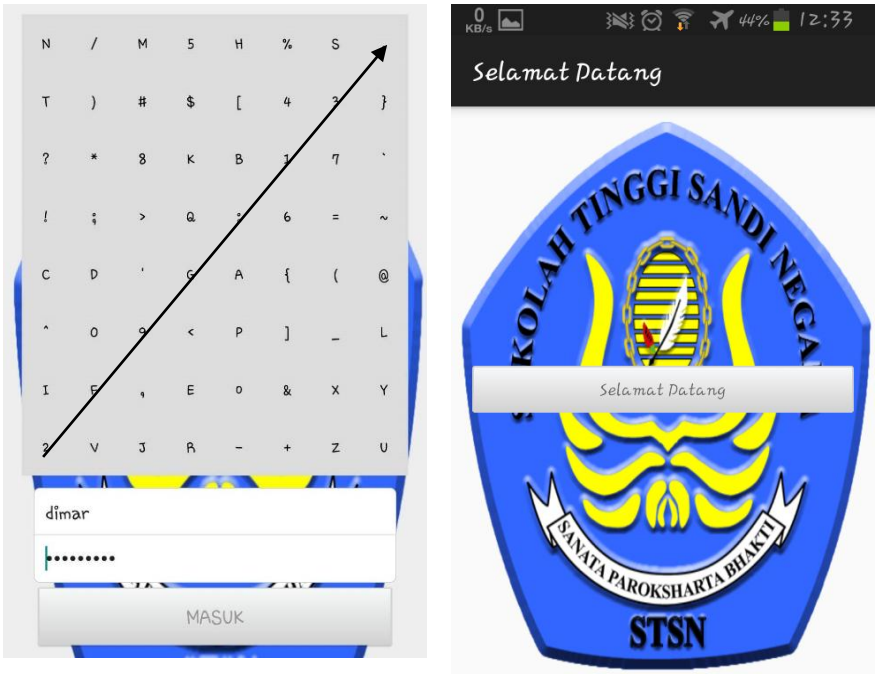
Pengguna dapat memasukkan *username* dan *password* yang dimilikinya ke dalam aplikasi. Pengguna disajikan sebuah tabel *password* yang berisi karakter acak *alfanumerik* dan simbol. Pengguna diharuskan memasukkan lokasi matriks yang membentuk pola sebagai *password* yang telah dipilih dengan karakter yang sesuai. Jika *password* yang telah didaftarkan sesuai dengan yang tersimpan pada *database* maka pengguna telah terotentikasi sehingga dapat masuk sistem.

Tujuan dari simulasi ini adalah memberi gambaran pengguna mengenai metode *Hybrid Shape Textual Login* yang dapat digunakan sebagai kontrol akses pada perangkat Android. Untuk mengetahui kerja sistem secara singkat dapat dilihat *flowchart* gambar 2. Adapun tahapan dalam implementasi ini yaitu:

a) Pengguna membuka aplikasi *Hybrid Shape Textual Login* dan akan disajikan menu MASUK dan DAFTAR. Pengguna dapat melakukan registrasi untuk mendaftarkan dirinya ke sistem dengan menekan DAFTAR. Sedangkan jika pengguna ingin masuk ke sistem maka dapat menekan MASUK.
b) Pada saat menekan DAFTAR pengguna akan disajikan *form* masukan data pengguna yakni *username, password, confirm password* yang harus diisi dengan benar. Jika pengguna salah dalam mengisi maka sistem akan menampilkan notifikasi kesalahan.
c) Pada saat menekan MASUK pengguna akan disajikan *form* masukan data pengguna yakni *username* dan *password*. Jika pengguna benar dalam mengisinya, maka sistem akan menampilkan tampilan selamat datang.



Gambar 2. Flowchart Sistem Simulasi Hybrid Shape Textual Login



Gambar 3. Tampilan Login dan Selamat Datang Aplikasi Hybrid Shape Textual Login

4. ANALISIS KEAMANAN DAN PENGUJIAN

4.1 Analisis Keamanan

a) Tahan Terhadap *Shoulder Surfing*
Pada fase login tidak menunjukkan bentuk yang digunakan secara langsung, maka *Hybrid Shape Textual Login* dapat dikatakan kuat dan tahan terhadap *shoulder surfing.* Salah satu cara agar

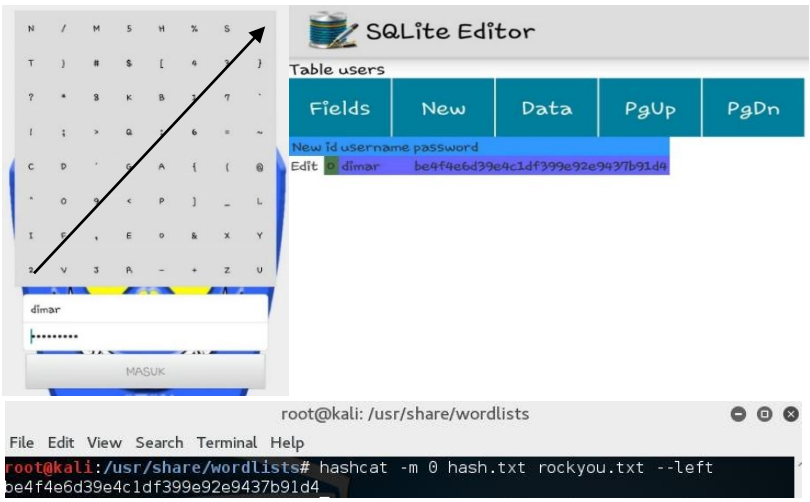
penyerang mendapatkan *password* adalah dengan merekam secara keseluruhan proses input *password* dan menganalisis tiap *input*. Hal tersebut dapat saja dilakukan akan tetapi membutuhkan sumber daya yang sangat besar karena dengan *password* yang tiap kali sesi *login* selalu mengalami perubahan

b) Tahan Terhadap *Bruteforce Attack*
Terdapat dua jenis *bruteforce attack* yang dilakukan yakni *bruteforce* terhadap *password* yang dimasukkan dan *bruteforce* terhadap pola yang dipilih.
Pada *bruteforce* terhadap *password*, penyerang akan mengalami kesulitan karena aplikasi ini memiliki *password* yang dinamis pada saat tiap kali sesi *login*. Karena setiap bentuk yang dipilih bisa bermacam – macam maka vektor karakter yang dipilih adalah "n" dan jumlah tabel adalah 8 x 8 maka jumlah percobaan yang harus dilakukan adalah $f = 64^n$
Pada *bruteforce* berbasis pada pola atau bentuk yang dipilih lebih efektif dilakukan dengan mengabaikan setiap kemungkinan teks *password* yang dipilih pengguna. Penyerang hanya perlu menerka bentuk yang dipilih oleh pengguna. Pada kenyataannya serangan ini sulit untuk dilakukan karena memiliki banyak bentuk (variasi pola) dalam sebuah matriks.

c) Tahan Terhadap *Dictionary Attack*
Jenis *dictionary attack* tidak dapat dilakukan pada *Hybrid Shape Textual Login.* Hal tersebut karena menggunakan *password* dinamis yang selalu berubah tiap kali sesi *login* dan tidak membentuk kata atau kalimat tertentu yang bisa digunakan untuk menyerang *password* pengguna. *Password* yang digunakan merupakan *password* yang membentuk pola pada matriks yang dipilih sehingga tahan terhadap *dictionary attack.*

4.2 Pengujian

Pada bagian ini *Hybrid Shape Textual Login* diuji tingkat efektif, efisien dan ketahanannya terhadap *dictionary attack* . Pada serangan *dictionary attack* digunakan SQLite Editor untuk mendapatkan basisdata yang tersimpan dan *tools* Hashcat pada Kali Linux yang sudah tersedia kamus *dictionary attack* (rockyou.txt) untuk mendapatkan *secret* pengguna [13]. Dapat dilihat pada gambar 4 bahwa *Hybrid Shape Textual Login* tidak menunjukkan *secret* pengguna sehingga terbukti tahan terhadap *dictionary attack.*



Gambar 4. Dictionary Attack pada Hybrid Shape Textual Login

Untuk mengetahui tingkat keefektifan dan keefisienan waktu proses *login* dari *hybrid shape textual login* dilakukan uji pengguna secara langsung. Aplikasi diujikan kepada 20 orang yang dijadikan sampel dan dibandingkan dengan hasil uji dari *pair based text authentication* dari penelitian yang telah dilakukan [8]. Adapun hasil uji dapat dilihat pada tabel 1.

Tabel 1. Perbandingan Pengujian Metode

Kriteria Pengujian	Normal	*Pair Based Text Authentication*	*Hybrid Shape Textual Login*
REKAPITULASI WAKTU LOGIN (DETIK)			
MAKS.	40,88	128,87	10,59
MIN	14,21	22.1	3,96
RATA RATA	24,89	47,14	5,97
REKAPITULASI KESALAHAN LOGIN (PROSENTASE)			
SALAH	-	14,63	0,00

Dapat dilihat pada tabel 1, *hybrid shape textual login* memiliki tingkat keefektifan dan keefisienan yang lebih baik dilihat dari segi waktu dan kesalahan melakukan *login*. Pada proses *login* pengguna lebih cepat dalam melakukan *login* dibandingkan dengan skema yang lain dan seluruh sampel dapat melakukan *login* tanpa adanya kegagalan.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penggunaan *login* konvensional yang berbasis teks saat ini banyak digunakan dalam sistem memiliki kerawanan terhadap *brute force attack, dictionary attack* dan *shoulder surfing*. Sedangkan, alternatif *login* seperti menggunakan *password* berbasis gambar serta *password* biometrik memiliki masalah yang telah disebutkan sebelumnya. Dapat disimpulkan pada penelitian ini *Hybrid Shape Textual Login* secara teori tahan terhadap *Shoulder Surfing* dan *Bruteforce Attack* dan telah terbukti kuat terhadap *Dictionary Attack* serta lebih efektif dan efisien dibandingkan dengan metode *pair based text authentication*.

5.2 Saran

Sampai dengan saat ini *login* menggunakan basis otentikasi *something you know* merupakan basis yang paling umum dan populer digunakan untuk mengakses sebuah sistem. Basis otentikasi tersebut juga diterapkan pada metode *Hybrid Shape Textual Login* yang dapat digunakan sebagai alternatif *login* pada sistem. Pada makalah ini metode *Hybrid Shape Textual Login* masih pada tahap simulasi, untuk pengembangan selanjutnya dapat dikembangkan dan diterapkan pada berbagai sistem *login* seperti *screenlock* Android, sistem *login* ATM dan lain sebagainya untuk menjamin kredensial yang pengguna di tempat publik agar tetap aman. Sebagai tambahan keamanan dapat digunakan juga *two factor authentication* dengan menggunakan basis otentikasi lainnya.

6. DAFTAR RUJUKAN

[1] Santoso, I., 2014. *Android yang Menggigit.* [Online] Available at: http://sharingvision.com/2014/05/android-yang-menggigit/ [Diakses 7 Maret 2016].

[2] Suryadi, A., 2015. *Potret Penggnuna Android Indonesia.* [Online] Available at: http://inet.detik.com/read/2015/01/15/115444/2804072/ [Diakses 5 Maret 2016].

[3] Ayubi, S. A., 2015. *Waspada! Ponsel Android Rentan Pencurian Data.* [Online] Available at: http://industri.bisnis.com/read/20151025/105/485772/waspada-ponsel-android-rentan-pencurian-data [Diakses 25 Februari 2016].

[4] Sicilliano, R., 2015. *Most Unwanted Criminals: Phissers, Shoulder Surfers and Keyloggers.* [Online] Available at: https://blogs.mcafee.com/consumer/family-safety/mostunwanted-criminals-phishers-shoulder-surfers-andkeyloggers/ [Diakses 24 Februari 2016].

[5] Suryawinata, F., 2016. *Anak 7 Tahun Habiskan 81 Juta Rupiah di Pembelian Dalam Aplikasi.* [Online] Available at: http://www.jagatreview.com/2016/01/anak-7-tahunhabiskan-81-juta-rupiah-di-pembelian-dalam-aplikasi/ [Diakses 1 April 2016].

[6] Kedar, P. S. & Bhusari, V., 2014. Using PBKDF2 Pair and Hybrid technique for Authentication. *International Journal of Emerging Research in Management &Technology,* 3(5), pp. 219-228.

[7] Harbach, M., Luca, A. & Egelman, S., 2016. *The Anatomy of Smartphone Unlocking A Field Study of Android Lock Screens.* San Jose, Association for Computing Machinery (ACM).

[8] Munandar, M., 2014. *Rancang Bangun Prototipe Kendali Akses Menggunakan Microcontroller dengan Menerapkan Metode Otentikasi Berbasis Pasangan Teks.* Tugas Akhir Tidak Diterbitkan penyunt. Bogor: Sekolah Tinggi Sandi Negara.

[9] Zheng, Z., Liu, X., Yin, L. & Liu, Z., 2010. A Hybrid Password Authentication Scheme Based on Shape and Text. *Journal of Computers,* 5(5), pp. 765 – 771.

[10] Verma, M. & Sood, M., 2015. Smarter Method for User Authentication in Mobile System. *International Journal of Advanced Research in Computer Science and Software Engineering,* 5(4), pp. 1122 -1128.

[11] Menezes, et al., 1996. *Handbook of Applied Cryptography.* Boca Ration: CRC Press.

[12] Conrad, E., Misenar, S. & Fedlman, J., 2012. *CISSP Study Guide.* 2nd penyunt. Waltham: Syngress.

[13] Dieterle, D. W., 2013. *Basic Security Testing With Kali Linux.* New York: CreateSpace Independent Publishing Platform.