BERBAGAI MACAM PENGUNCI LAYAR *(LOCK SCREEN)* *SMARTPHONE*

Dimas Agung Yulianto[1)]
[1)]Pekerja serabutan di bidang komputer *(masteknisi.com)*
agung.dimas@gmail.com

Abstrak

Pemakai smartphone sudah mencapai jumlah yang banyak dan sangat membantu dalam aktifitas sehari-hari. Data-data krusial (baik yang bersifat pribadi maupun bisnis) pada smartphone perlu dilindungi agar tidak jatuh ke sembarang orang. Salah satu pengamanan dasar pada smartphone adalah pengunci layar (lock screen). Penelitian ini mengkaji beberapa teknologi pengunci layar yang sudah muncul dipasaran mulai dari penggunaan, karakteristik, kemampuan dan kelemahannya. Metodologi yang digunakan dalam penelitian ini adalah subjektivitas, yaitu didasarkan pada pengalaman pribadi dan bacaan dari sumber-sumber di daftar pustaka. Hasilnya pengunci geser (slide lock) adalah pengunci yang minimal sebaiknya dipakai oleh para pengguna smartphone. Kemudian pengunci sidik jari (finger print) mempunyai nilai yang tinggi baik dalam tingkat keamanan maupun kemudahan penggunaan. Sedangkan pengunci PIN genie disarankan untuk pengguna yang menginginkan tingkat pengamanan tinggi tetapi bisa dipasang pada berbagai jenis Android (dari yang murah sampai yang mahal).

Kata Kunci : *pengamanan, smartphone, pengunci layar*

1. PENDAHULUAN

MENRISTEKDIKTI Mohamad Nasir menyebutkan jumlah pengguna smartphone di Indonesia mencapai sekitar 25% dari total penduduk atau sekitar 65 juta orang [3]. Hampir setiap orang yang mempunyai *smartphone* akan menggunakannya dalam menjalani kesehariannya. Oleh karena itu berbagai data penting banyak yang tersimpan dalam *smartphone.* Data sensitif baik yang bersifat pribadi maupun bisnis yang ada dalam *smartphone* membuatnya penting untuk ditambahkan sistem pengamanan mengingat informasi dan perangkat *smartphone* yang rentan hilang, dicuri atau dirusak oleh pihak-pihak yang berusaha mencari keuntungan. Pertahanan awal pengamanan perangkat *smartphone* adalah pengunci layar *(lock screen),* pada umumnya berbasis pengaman PIN atau *password* [6]. Pengunci layar adalah sistem pengamanan yang dipasang pada *smartphone* berbentuk layar virtual yang mengunci *smartphone* sehingga tidak bisa difungsikan secara utuh fitur-fiturnya, tetapi ada kalanya beberapa fitur masih bisa diakses tanpa harus membuka pengunci layar.

Sebuah survey yang dilakukan bulan Mei 2016 menunjukkan data pengunci layar yang dipakai oleh para pengguna *smartphone* terbagi menjadi 25% menggunakan Nomor PIN, 23% menggunakan sidik jari, 9% menggunakan *password*, 9% menggunakan pengunci pola, 2% menggunakan pengunci jenis lain dan 28% sisanya tidak menggunakan pengunci layar [4]. Angka 28% yang tidak menggunakan pengunci layar merupakan hal yang sangat disayangkan sekali mengingat otentikasi keamanan dari sisi perangkat adalah sebuah keharusan dalam rangka mencegah penggunaan oleh orang-orang yang tidak berhak [5]. Makalah ini mengevaluasi beberapa pengunci layar

yang diharapkan dapat digunakan sebagai salah satu sumber bacaan tentang pemilihan pengunci layar.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan subjektif atau didasarkan pada penilaian penulis, data yang dikumpulkan berupa kata-kata, gambar, pengalaman pribadi dan bukan angka-angka. Sehingga penelitian ini dapat dikatakan sebagai penelitian yang tidak sepenuhnya ilmiah. Beberapa pengunci *smartphone* dalam penelitian ini sudah pernah penulis gunakan. Beberapa pengunci yang tidak penulis coba, penilaiannya didasarkan pada pemikiran logis penulis, bacaan dan sumber referensi yang dirujuk dalam daftar pustaka.

3. PEMBAHASAN

Sebagian besar pengunci layar yang dipakai adalah pengunci nomor PIN, pengunci pola Android dan pengunci *biometric* (contoh Apple *Touch* ID dan *Face Recognition* Android) [2]. Pengguna pengunci layar yang semakin banyak menandakan bahwa faktor keamanan merupakan sesuatu yang penting [2]. Pengunci layar sedianya mampu mencegah agar *smartphone* tidak bisa diakses oleh orang yang tidak berhak, mudah saat dioperasionalkan, mengurangi beban otak dalam penggunaannya (contoh proses mengingat nomor PIN) dan cepat saat proses otentikasi [2]. Berikut ini adalah beberapa pengunci layar yang sudah muncul dipasaran :

a. *Slide Lock* (Pengunci Geser)

Slide Lock adalah sistem pengunci layar berbasis geser menggunakan jari yang diarahkan sesuai perintah dari sistem operasi. Kunci akan terbuka saat penggeseran sudah dilakukan dengan benar. Pengunci jenis ini adalah pengunci yang banyak diterapkan pada perangkat Android [6]. Terdapat beberapa variasi pada arah geser seperti ke kiri, kanan, atas atau bawah. Pengunci geser sejauh ini adalah metode pengunci paling rawan karena siapapun yang bertemu pengunci jenis ini maka akan mampu membukanya [1]. Disamping itu masih ditemukannya beberapa kasus jika salah dalam melakukan penggeseran maka layar tetap bisa terbuka [6]. Ada juga kejadian dimana *smartphone* yang diletakkan di saku celana atau jaket, gesekan sedikit saja bisa jadi akan membuka kunci ini [7].

b. *Password* (Kata Sandi)

Pengunci *password* merupakan sistem pengunci yang juga diterapkan pada sistem keamanan komputer. Pengunci ini dinilai sebagai salah satu pengunci yang dinilai aman karena memungkinkan pengguna untuk memakai kombinasi *password* yang rumit sehingga diharapkan sulit diterka oleh hacker [5]. Kombinasi *password* yang disarankan terdiri dari penggunaan huruf kapital, huruf kecil, angka dan karakter-karakter unik (*,$,&,#,^). Konsekuensi dari penggunaan kombinasi yang rumit adalah waktu yang lama saat pengetikan *(input password)* tersebut. Syarat agar *password* tetap sederhana dan punya pengamanan yang kuat adalah menggunakan kombinasi yang cukup rumit, cepat saat pengetikan (*input password)* dan mudah diingat. Ada resiko dimana pengguna lupa *password*-nya sehingga

tidak bisa mengakses *smartphone*. Sayangnya hanya ada sedikit cara untuk mengembalikan data-data pada *smartphone* yang lupa kata sandi yang kemudian direset ulang. Reset ulang dipilih karena hal tersebut merupakan cara termudah untuk menghilangkan *password* [1].

Gambar 1. *Pattern Lock* (Pengunci Pola), PIN *Number* dan *Password*

c. *Personal Identification Number* - PIN (Nomor PIN)

Pengunci jenis PIN adalah salah satu yang populer digunakan diantara pengguna *smartphone* [6]. PIN biasanya terdiri dari kombinasi 4 digit angka dari angka 0 - 9. Pengunci nomor PIN lebih mudah digunakan daripada pengunci password karena jumlah angkanya yang lebih sedikit. Timbal baliknya pengunci ini lebih mudah dibobol oleh *hackers* karena kemungkinan kombinasi yang digunakan akan semakin sedikit. Program penebak password *(decipher)* membutuhkan waktu tidak begitu lama untuk mencari kombinasi yang benar [6].

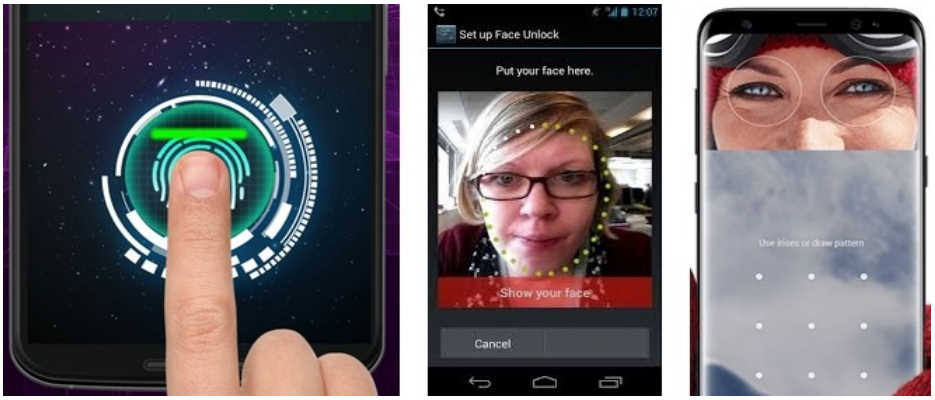
d. *Pattern Lock* (Pengunci Pola)

Pengunci pola banyak digunakan sebagai cara untuk otentikasi dan otorisasi pada perangkat android [7]. Pengunci pola merupakan salah satu cara termudah untuk mengamankan perangkat *smartphone*. Studi psikologi menunjukkan bahwa otak manusia lebih baik dalam mengingat dan mengingat-ingat informasi visual daripada angka atau huruf [1]. Pengguna cukup menggambar pola garis diantara 9 titik, bisa garis sederhana diantrara 2 titik sampai ke pola yang rumit terdiri dari banyak garis. Jenis pengunci berbasis visual ini sangat populer digunakan karena lebih cepat daripada memasukkan password dan hampir menyamai keceptan memasukkan pengunci PIN [6].

Keuntungan metode pengunci ini adalah pengguna hanya tinggal menyentuhkan jari sekali kemudian menggambar pola kunci tanpa menariknya dari layar. Pengunci ini akan lebih efektif saat digunakan oleh orang-orang yang punya kecenderungan menyukai gambar atau pengguna otak kanan. Berbeda dengan pengunci nomor PIN dan *password,* pengunci pola tidak mudah diingat dan lebih mudah untuk dilupakan, bahkan terkadang pola kunci yang 5 menit lalu sudah dibuat bisa saja lupa bentuknya.

e. *Biometric*

Pengunci *biometric* mendasarkan pada natural bawaan fisik manusia oleh karenanya pengunci ini dikatakan sebagai pengunci terbaik [6]. Bawaan fisik manusia yang dapat dijadikan pengunci *biometric* adalah sidik jari, wajah dan iris mata. Menggunakan salah satu dari 3 jenis pengunci *biometric* membebaskan penggunanya dari mengingat-ingat kunci karena semuanya sudah hadir dengan ciri khas masing-masing yang merupakan bawaan sejak lahir. Oleh karenanya *hacker* akan kesulitan dalam meretas *smartphone* yang menggunakan pengunci *biometric,* tetapi pada kenyataannya dan dengan ketekunan maka pengamanan *biometric* tetap dapat diretas oleh *hacker* [6].



Gambar 2. *Biometric* (*fingerprint, face unlock* dan *iris scan*)

- ***Fingerprint*** **(sidik jari)**

Teknologi pembaca sidik jari sekarang banyak sekali ditemukan di perangkat-perangkat *smartphone* terbaru dan biasanya terdapat pada *smartphone* yang tergolong mahal. Pengunci ini disebut sebagai teknologi yang efisien karena cukup dengan menempelkan jari tangan ke layar/pembaca sidik jari maka otomatis layar akan terbuka. Pembaca sidik pada *smartphone* dapat ditemukan di bagian belakang perangkat, pada *home button,* pada layar utama, atau pada sisi samping perangkat.

- ***Face Recognition*** **(pengenal wajah)**

Teknologi pengunci berbasis wajah merupakan teknologi yang tergolong baru pada lingkungan perangkat Android. Wajah manusia berbeda-beda karena masing-masing mempunyai ciri, lekukan dan kerutan yang berbeda. Perangkat lunak kemudian menyimpan ciri khas tersebut ke tempat penyimpanan *(database)* sekaligus membuat kode uniknya.

Dirasakan bahwa pengunci berbasis wajah ini tidak begitu efisien, meskipun begitu metode ini masih menjadi metode yang praktis untuk otentikasi [6]. Pengguna juga menemukan bahwa dalam beberapa kondisi tertentu wajahnya tidak dikenali. Seperti pada kondisi kurang cahaya, perubahan model rambut, dan pemakaian kacamata. Proses pengenalan wajah mengharuskan pengguna harus benar-benar meletakkan dengan tepat *smartphone* didepan wajahnya agar program bisa melakukan pencocokan. Proses ini berlangsung lambat dan terasa merepotkan [6].

- ***Iris Scan* (pembaca iris mata)**

  Pengunci iris mendasarkan pada penangkapan pantulan cahaya dari mata pengguna sehingga ciri khas iris mata bisa ditangkap. Cahaya yang memantul dari mata digunakan kamera untuk menangkap ciri khas iris lalu disimpan dalam *smartphone*. Proses otentikasi dilakukan dengan menahan *smartphone* sedemikian rupa sehingga bisa membaca iris mata pengguna. Pembaca iris mata kemudian memferivikasi apakah ada kecocokan dengan data di *database,* jika ada kecocokan maka layar akan terbuka.

f. Android *Smart Lock*

Merupakan metode pengunci yang tergolong baru pada sistem operasi Android. Pengunci ini kemudian populer terutama di kalangan orang-orang yang baru mengenal pengunci *smart lock*. Metode otentikasi ini melibatkan adanya alat khusus yang sudah disiapkan sebelumnya seperti perangkat *bluetooth,* alat berbasis NFC *(Near Field Communication),* sinyal *hotspot,* GPS atau alat lain yang dapat berkomunikasi dengan sistem operasi Android. Secara otomatis layar akan terbuka saat perangkat-perangkat khusus tersebut berada di jangkauan. Jika menggunakan basis GPS maka perangkat Android akan terbuka otomatis saat berada di lokasi-lokasi yang sudah ditentukan dan otomatis mengunci jika di luar lokasi tersebut. Metode otentikasi *smart lock* GPS dirasa cocok untuk pengguna yang tidak begitu memerlukan sekali akan pengamanan saat berada di tempat tertentu yang dirasa aman dengan lingkungan sekitarnya. Pengunci *smart lock* membuat setiap penggunanya hanya dapat menggunakan *smartphone* saat berada dekat dengan alat-alat khusus tersebut. *Smart lock* juga dapat diatur agar terbuka pada jam-jam tertentu dan mengunci pada jam tertentu.

Gambar 3. Android *Smart Lock,* PIN *Genie* dan *Gesture Unlock*

g. *Gesture Unlock (waving)*

Beberapa produsen memberikan sensor pada Andoid untuk mengukur jarak sehingga hal tersebut bisa digunakan untuk membuka pengunci layar berdasarkan pada gerakan tangan atau jari pada arah yang sudah ditentukan. Contoh membuka layar dengan metode ini adalah dengan memberi usapan ringan mengambang di atas layar. Ada kalanya saat membuka *gesture unlock* terkadang perlu dilakukan berkali-kali karena tidak setiap saat pembaca jarak

Android bekerja dengan baik atau gerakan tangan tidak berada pada posisi yang tepat [6].

h. *Shake Unlock*

Metode pembuka layar dengan menggoyangkan ke-kanan-kiri *smartphone* untuk membukanya. Metode ini menggunakan sensor *accelerometer* dari *smartphone* untuk mengukur perpindahan gaya gravitasi. Merupakan salah satu metode pembuka kunci yang ada di Android, tetapi pembuka kunci jenis ini tidak banyak digunakan oleh para pengguna Android. Pembuka kunci ini biasanya juga dipasang bersamaan dengan pengunci jenis lain sebagai cadangan jika gagal membuka setelah beberapa kali percobaan menggoyangkan *smartphone* sehingga tidak perlu melakukan reset *smartphone*.

i. PIN *Genie*

Metode pengunci PIN *Genie* disediakan oleh pengembang *software* pihak ke-3 (tidak sepaket dengan sistem operasi). Merupakan pengembangan dari pengunci nomor PIN. Metode ini memunculkan 4 kelompok angka yang masing-masing terdiri dari 3 angka, dimana angka yang muncul selalu acak dan tidak berada pada posisi/kombinasi yang sama. Kemudian pengguna memasukkan 4 nomor PIN yang sudah ditentukan untuk membuka layar *smartphone*. Pengacakan dan penggabungan angka-angka akan membuat sulit seseorang yang ingin mengetahui kuncinya karena jika terlihat oleh orang lain maka orang tersebut masih harus melakukan prediksi satu angka dari 3 angka yang muncul pada 4 kelompok angka. Metode ini tergolong mudah dioperasionalkan dengan tingkat keamanan yang cukup tinggi [6]. Tetapi metode ini hanya menyediakan beberapa angka yang sudah ditentukan oleh program (tidak bisa diatur oleh pengguna) dan pengguna masih harus melakukan "pembacaan" pada 3 kombinasi angka di 4 kelompok angka yang muncul.

Jenis Pengunci Layar	Kemudahan Pemakaian	Jenis *Hardware*	Tingkat Pengamanan	Kecepatan Otentikasi	Lama Pengaturan Awal	Keharusan Mengingat sandi/kunci
Slide Unlock	mudah	tidak	rendah	cepat	cepat	tidak
Password	mudah	tidak	tinggi	sedang	sedang	ya
Nomor PIN	mudah	tidak	tinggi	cepat	cepat	ya
Pattern	mudah	tidak	sedang	cepat	sedang	ya
Fingerprint	mudah	ya	tinggi	cepat	lama	tidak
Face Recog.	sulit	tidak	tinggi	lama	lama	tidak
Iris Scan	sedang	ya	tinggi	lama	lama	tidak
Smart Lock	mudah	tidak	sedang	cepat	lama	tidak

Shake Unlock	mudah	tidak	sedang	sedang	lama	tidak
Gesture Lock	sedang	tidak	rendah	lama	lama	tidak
PIN *genie*	sulit	tidak	tinggi	cepat	lama	ya

4. SIMPULAN

Pengunci layar datang dengan berbagai karakteristik, kemampuan dan persyaratannya masing-masing. Kebutuhan tingkat pengamanan, jenis perangkat *(hardware) smartphone,* kompleksitas dan kemudahan operasional pengunci layar baiknya digunakan sebagai faktor untuk memilih.

Pada *smartphone* seminimal mungkin diberi pengunci geser *(slide lock)* untuk mencegah terjadinya hal-hal yang bersifat ketidaksengajaan. *Slide lock* dipilih karena tidak rumit dan mudah dioperasionalkan. Jika ingin benar-benar mengamankan perangkat *smartphone* maka pengunci jenis sidik jari *(finger print)* dapat dipilih karena kunci ini berbasis *biometric* dan dalam mengoperasikannya tergolong mudah, sayangnya teknologi ini lebih banyak ditemukan pada *smartphone* kelas atas. Pada skala menengah dimana diperlukan pengunci dengan tingkat keamanan yang tinggi tetapi dapat diinstal pada berbagai jenis *smartphone* (murah hingga mahal) maka pengunci PIN *genie* dapat dipilih. PIN *genie* dipilih karena tidak memerlukan alat tambahan dan tidak harus *smartphone* yang mahal, tetapi metode ini mengharuskan penggunanya untuk mengingat 4 kombinasi angka pengunci dan melakukan "pembacaan" tiap kali akan membuka kunci.

5. DAFTAR PUSTAKA

Angeli, Antonella De., Coventry, Lynne., Johnson, Graham., Renaud, Karen., (2005), Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems, International Journal of Human-Computer Studies - Special isssue: HCI research in privacy and security is critical now, Volume 63, Issue 1-2 July 2005, Pages 128 – 152

Harbach, Marian., Luca, Alexander De., Egelman, Sarge., (2016), The Anatomy of SmartPhone Unlocking, *presented at* Computer Human Interaction (CHI). 7-12 May. San Jose, CA, USA.

Nasir, Mohamad. (2017), Smartphone Rakyat Indonesia, Diakses dari https://www.dikti.go.id/smartphone-rakyat-indonesia-2/

Pew Research Center, (2016), 28% of Smartphone Owners Have No Lock Screen on Their Phones, diakses dari http://assets.pewresearch.org/wp-content/uploads/14/2017/01/23092125/PI_01.26.cyber-02-02.png

Putri, Alifa Nurani., A., Yudistira Dwi W., Akbar, Saiful. (2016), A Continuous Fusion Authentication for Android based on Keystroke Dynamics and Touch Gesture, IEEE paper 978-1-5090-5671-2/16/$31.00

Thakur, Yash., Chauhan, Ravi Raj., (2017), A Survey on Lock Screen for User Authentication Method in Android, *presented at* International Journal

on Recent and Innovation Trends in Computing and Communication (IJRITCC). May 2017. ISSN: 2321-8169 / 965-970

Ye, Guix., Tang, Zhanyong., Fang, Dingyi., Chen, Xiaojiang., Kwang, In Kim., Taylor, Ben., Wang, Zheng. (2017). Cracking Android Pattern Lock in Five Attempts, *presented at* The Network and Distributed System Security (NDSS) Symposium. 26 February - 1 March 2017. San Diego, CA, USA. ISBN 1-1891562-46-0. http://dx.doi.org/10.14722/ndss.2017.23130