Kesadaran akan Ancaman Serangan Berbasis *Backdoor* di Kalangan Pengguna *Smartphone* Android

Muhammad Raffi Akhyari
Program Studi Informatika – Program Sarjana
Universitas Islam Indonesia
Yogyakarta, Indonesia
muhammad.akhyari@students.uii.ac.id

Ahmad R. Pratama
Jurusan Informatika
Universitas Islam Indonesia
Yogyakarta, Indonesia
ahmad.rafie@uii.ac.id

Abstract*—Sebuah teknologi berkembang semakin pesat. *Smartphone* merupakan salah satu perkembangan yang cukup pesat dalam kemajuannya di bidang teknologi era industri 4.0 ini. Di balik segala kemudahan dan fleksibilitas *smartphone* yang ditawarkan, terdapat juga berbagai macam risiko keamanan yang dimanfaatkan para peretas untuk mengakses *smartphone* pengguna dengan menggunakan *framework* berbasis *backdoor* sebagai serangan yang digunakan peretas untuk mencuri data dan informasi pengguna. Dikarenakan faktor manusia adalah salah satu unsur penting dalam keamanan siber dan informasi, kesadaran akan keamanan pun menjadi suatu hal yang penting. Tujuan penelitian ini mengukur tingkat kesadaran keamanan di kalangan pengguna *smartphone* android berdasarkan faktor-faktor demografis penggunanya. Dari hasil pengukuran berdasarkan pendekatan model Kruger dan Kearney, secara umum tingkatan-tingkatan kesadaran keamanan pengguna *smartphone* android dapat dikatakan rata-rata cukup baik dengan beberapa peluang peningkatan di sisi *Knowledge* (pengetahuan), *Attitude* (sikap), dan *Behavior* (perilaku), utamanya yang terkait dengan area fokus *Backdoor, Hardware, Android OS* yang masih lebih rendah jika dibandingkan dengan area fokus *Apps,* dan *Permission*. Selain itu, dari hasil analisis menggunakan analisis regresi linear berganda, penelitian ini menemukan hasil yang signifikan pada kategori demografis Jenis Kelamin. Hasil dari penelitian ini dapat dimanfaatkan untuk merancang berbagai jenis intervensi atau kebijakan khusus dalam rangka meningkatkan kesadaran keamanan sebagai bentuk literasi digital di semua kalangan pengguna *smartphone* android di Indonesia.

Keywords—Smartphone, Kesadaran Keamanan, Backdoor, Android, Literasi Digital

I. PENDAHULUAN

Kejahatan pada dunia siber sudah menjadi hal yang biasa sejak berkembangnya sebuah teknologi. Banyak sekali para *hacker* atau peretas yang menggunakan kemampuannya untuk melakukan hal yang merugikan orang lain dengan mencuri data dan informasi pengguna pribadi untuk kepuasan ataupun modus finansial. Salah satu bentuk faktor yang menjadi pemicu terjadinya pelanggaran informasi dan privasi adalah karena para pengguna *smartphone* memiliki *security awareness* atau kesadaran keamanan yang tidak mumpuni dalam menggunakan *smartphone* dengan baik dan aman. Beberapa dari mereka memiliki pengetahuan yang cukup mumpuni dalam penggunaan *smartphone* tetapi mereka tidak menerapkannya dengan baik dan aman[1].

Seiring berjalannya masalah umum yang sering terjadi pada sistem operasi salah satunya *smartphone*. Masalah yang timbul yaitu serangan *backdoor* yang mengancam sistem operasi android. *Backdoor* dalam dunia *hacker* disebut sebagai pintu belakang yang dapat diakses dengan mudah, dan dengan mudah meninggalkan jejak dari *vulnerability* android tersebut. *Backdoor* pada awalnya digunakan para *programmer* komputer sebagai mekanisme perizinan mereka untuk mendapatkan hak akses khusus ke dalam program mereka, namun banyak ditemukan para *hacker* atau peretas yang memanfaatkan *backdoor* sebagai senjata untuk memasuki celah sistem pada *smartphone*[2].

Setiap individu perlu memahami bahwa kewaspadaan dalam keamanan siber perlu ditingkatkan dengan literasi digital. Literasi digital merupakan hal penting yang dibutuhkan untuk dapat berpartisipasi di dunia era digital sekarang. Alasannya karena setiap orang berkehendak untuk bertanggung jawab terhadap bagaimana cara menggunakan teknologi untuk berinteraksi dengan lingkungan sekitarnya. Dalam hal ini, bentuk yang dimaksud yaitu, menciptakan, mengelaborasi, mengomunikasikan, dan bekerja sesuai dengan aturan dan etika, dan memahami perkembangan teknologi yang cepat ini[3]. Dalam penelitian ini, pertanyaan yang akan dijawab adalah seberapa besar kesadaran keamanan yang dimiliki oleh para pengguna *smartphone* android di Indonesia dan apakah faktor demografis seperti jenis kelamin, usia, lokasi, pendidikan, adopsi teknologi informasi dan penghasilan berpengaruh pada perbedaan tingkat kesadaran keamanan tersebut. Penelitian ini diharapkan dapat berkontribusi untuk memberikan gambaran tingkat kesadaran keamanan sebagai bentuk literasi digital di kalangan pengguna *smartphone* Android di Indonesia.

II. KAJIAN PUSTAKA

Dalam menghadapi sebuah kejahatan pada dunia *cyber* dan pencurian informasi secara ilegal, orang-orang berusaha untuk mencegah tindakan-tindakan kriminal terkait pencurian informasi, dan berusaha meminimalisir kebocoran atau pencurian akibat celah yang dimanfaatkan oleh para pencuri yang biasa disebut *hacker* atau peretas [4].

Menurut Von Solms dan Cervone, dalam meminimalisir risiko pada pelanggaran terhadap keamanan informasi, sangat penting bagi setiap organisasi terutama pengguna untuk menerapkan rencana atau strategi keamanan informasi. Karena bagi Namjoo, pencegahan yang dilakukan setelah terjadinya suatu pelanggaran keamanan informasi, bisa menjadi sangat terlambat[5]. Whitman dan Mattord menyampaikan bahwa manusia adalah titik terlemah dalam keamanan informasi. Suatu organisasi bisa saja memiliki sebuah teknologi terbaik yang mereka punya, dengan menggunakan perlindungan *firewall, intrusion detection system* (IDS), sistem biometrik dan lain sebagainya, namun organisasi tersebut harus mengetahui apakah setiap karyawan

dapat dipercaya, karena karyawan sendiri merupakan celah keamanan data dan informasi pada setiap organisasi[6]. Adapun Harris dan Maymi menyatakan bahwa suatu keamanan dalam organisasi itu tergantung pada teknologi dan manusia. Manusia merupakan titik terlemah dalam rantai keamanan seringkali menyebabkan pelanggaran keamanan dan kebocoran terhadap sistem dan menyebabkan kehilangan data dan informasi. Jika pengguna dapat memahami sistem dengan baik, maka insiden-insiden keamanan dapat diminimalkan[7].

Kesadaran keamanan informasi merupakan suatu proses yang bersifat dinamis terkait dengan tantangan dan risiko yang terus berubah, sehingga kesadaran terhadap keamanan informasi harus diukur dan dikelola sesuai dengan bentuk perubahan dan perkembangan risiko. Kesadaran keamanan juga harus dilakukan secara terus menerus, dan berkesinambungan menjadi bagian dari budaya organisasi atau perusahaan. Adapun Schlienger dan Teufel menyatakan bahwa tujuan yang diharapkan dari kesadaran keamanan informasi, yaitu: pengguna "menjadi sadar", kemudian "tetap sadar" dan akhirnya "sadar" terhadap kesadaran keamanan[8]. Untuk mengetahui tingkat kesadaran keamanan informasi pengguna, Kruger dan Kearney membangun suatu model yang dapat digunakan sebagai media pengukuran untuk kesadaran keamanan. Pengukuran tersebut dilakukan pada tiga aspek yang meliputi, di antaranya: pengetahuan *(knowledge),* sikap, (*attitude),* dan perilaku *(behaviour)*. Berdasarkan tiga aspek tersebut, dibagi kembali menjadi lima area fokus. Setiap fokus yang ada, akan dibagi menjadi beberapa faktor dan kemudian dibagi kembali dengan subbagian. Model ini dikenal dengan nama KAB *(Knowledge-Attitude-Behaviour)* Model[8].

Android adalah pemimpin pasar dalam eksplorasi sistem operasi seluler. Android didirikan sejak tahun 2003 di tangan Android Inc, yang telah diakuisisi oleh Yahoo pada tahun 2005[9]. Sejak awal, sistem operasi dirancang untuk dianggap sebagai *platform* seluler yang tidak hanya kaya fitur, kuat dan seluler, tetapi juga *open source*[10]. Seperti yang dirancang, Android dapat di-*install* pada berbagai perangkat *smartphone* yang mendukung serta memiliki *built in* dengan banyak teknologi perangkat lunak canggih. Android dibayangkan dan dibuat dengan model keamanan berlapis-lapis yang memungkinkan keserbagunaan yang penting dalam sistem terbuka, sekaligus memberikan perlindungan bagi pengguna dan aplikasi. Di balik keserbagunaan yang penting dalam sistem terbuka, dan model keamanan yang berlapis-lapis, android dapat dengan mudah diserang oleh *backdoor*[11].

Banyak masalah yang sering terjadi pada sistem jaringan komputer dan sistem operasi yaitu salah satunya *backdoor*. *Backdoor* dalam dunia *hacker* memiliki arti sebagai pintu atau akses belakang apabila seseorang berhasil memasuki pintu tersebut maka tamu tersebut dapat meninggalkan akses pada sistem. *Backdoor* pada awalnya dibuat oleh para *programmer* komputer atau android sebagai jalannya mekanisme untuk mengizinkan mereka agar dengan mudah mendapatkan akses khusus ke dalam program mereka. Dikarenakan suatu serangan dapat datang kapan saja seperti pada beberapa kasus pencurian data karena serangan *backdoor*, maka dibutuhkan suatu sistem keamanan yang dapat memonitor suatu paket data yang akan masuk, apakah itu termasuk sebuah serangan atau bukan[2].

Kesadaran keamanan dalam diri pengguna ketika menggunakan *smartphone* android akan dapat mengurangi risiko terjadinya serangan *backdoor* dan dapat mengurangi risiko pencurian data yang bisa saja terjadi. Pengguna yang baik perlu untuk memahami betul segala risiko yang bisa saja terjadi, apalagi terkait masalah penggunaan *smartphone* android yang biasa digunakan dalam kehidupan sehari-hari. Tentu saja ini sangat erat kaitannya dengan penelitian yang kami lakukan yang berfokus pada kesadaran keamanan yang dimiliki oleh pengguna ketika menggunakan *smartphone* android dari serangan berbasis *backdoor* melalui model Kruger dan Kearney serta hasil analisis regresi linear berganda untuk mencari tahu faktor yang kemungkinan besar berpengaruh yang datanya akan disajikan pada penelitian ini.

III. METODE

A. Desain Riset

Penelitian ini dilakukan menggunakan data yang telah dikumpulkan melalui survei secara daring. Survei disebar melalui jejaring media sosial yang akan diisi oleh berbagai responden dari berbagai macam daerah, usia, tingkat pendidikan, penghasilan, dan lain sebagainya. Data yang telah dibersihkan akan dianalisis secara kuantitatif menggunakan model *Information Security Awareness* (ISA) yang dikembangkan oleh Kruger dan Kearney[8] yang telah diadopsi agar sesuai dengan konteks kesadaran keamanan pengguna *smartphone* akan serangan berbasis backdoor di Indonesia. Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu *Knowledge* (Pengetahuan) yang mengukur apa pengguna *smartphone* di Indonesia ketahui tentang keamanan dan privasi, *Attitude* (Sikap) yang mengukur bagaimana perasaan pengguna *smartphone* tentang keamanan dan privasi, dan *Behavior* (Perilaku) yang mengukur apa yang pengguna *smartphone* lakukan terkait isu-isu keamanan dan privasi[1]. Untuk masing-masing dimensi, terdapat lima area fokus keamanan, yaitu *Backdoor, Hardware, Android OS, Apps, Permission.*

B. Pengumpulan Data

Dalam penelitian ini, pengumpulan data dilakukan secara online melalui kuesioner via Google Forms yang disebar melalui media sosial Line, WhatsApp, Facebook, Instagram, dan Twitter. Popuulasi dari penelitian ini adalah seluruh pengguna *smartphone* android di Indonesia. Kuesioner disebarkan selama dua minggu dari tanggal 25 September 2020 sampai 6 Oktober 2020 dan berhasil mengumpulkan total responden sebanyak 396 orang yang kemudian tidak ada pengurangan dalam total responden, dikarenakan hanya terdapat kesalahan dalam pengisian kuesioner, sehingga tetap 396 orang setelah dilakukan proses pembersihan data.

C. Instrumen Penelitian

Dalam penelitian ini terdapat beberapa pertanyaan terkait demografi, yakni jenis kelamin, usia, lokasi yang meliputi pulau, provinsi, dan kabupaten/kota, pendidikan terakhir, penghasilan bulanan, dan adopsi teknologi informasi. Selanjutnya, tedapat total 36 pertanyaan untuk mengukur kesadaran keamanan yang dikembangkan dengan mengikuti model Kruger dan Kearney berlandaskan teori psikologi sosial. Menurut Kruger dan Kearney, dengan melalui teori psikologi sosial akan dibagi menjadi tiga komponen untuk mengukur objek yaitu, *cognition, affection,* dan *behavior*[8]. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai Knowledge (pengetahuan seseorang), Attitude (sikap seseorang), dan Behaviour (perilaku seseorang)[1]. Dari 36 pertanyaan tersebut dibagi

menjadi masing-masing 12 pertanyaan setiap dimensinya, dimulai dari *Knowledge*, *Attitude*, dan *Behaviour*. Kemudian pertanyaan-pertanyaan tersebut akan dijawab dengan memilih 1 pilihan dari 3 opsi yang telah disediakan, yaitu benar, salah, dan tidak tahu. Tetapi khusus untuk dimensi *behavior* hanya tersedia 2 pilihan yaitu benar dan salah. Berikut keseluruhan 36 pertanyaan yang digunakan untuk mengukur tingkat kesadaran keamanan dapat dilihat pada Tabel 1.

Tabel 1. Contoh Pertanyaan

Dimensi	Pertanyaan	Opsi Jawaban
Knowledge	1. *Smartphone* berbasis Android berpotensi mendapatkan serangan berbasis *backdoor* yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna. 2. Proses *rooting* sistem operasi Android dapat meningkatkan risiko serangan berbasis *backdoor*. 3. Penggunaan aplikasi yang tidak diunduh dari Google Play Store atau repositori resmi lainnya dapat meningkatkan risiko serangan berbasis *backdoor*. 4. Beberapa *smartphone* Android tertentu sudah tertanam atau diselipkan *backdoor* perangkat keras pada *firmware* sejak dari pabrikannya. 5. *Smartphone* yang aman digunakan adalah yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM atau "Original Equipment Manufacture" atau juga bisa disebut barang *original*. 6. *Smartphone* yang tidak dikunci dengan *lockscreen* atau biometrik dapat memperbesar peluang terjadinya serangan berbasis *backdoor*. 7. Penggunaan sistem operasi tidak resmi (Custom ROM) dapat memperbesar peluang terjadinya serangan berbasis *backdoor*. 8. *Update* versi sistem operasi Android secara teratur dapat meningkatkan keamanan dari serangan berbasis *backdoor*. 9. *Update* aplikasi secara teratur dapat meningkatkan keamanan dari serangan berbasis *backdoor*. 10. Sebelum *install* suatu aplikasi (termasuk dari Google Play Store atau repositori resmi lainnya), perlu dipertimbangkan hak akses apa saja yang dibutuhkannya untuk berjalan. 11. Pengecekan secara berkala akan hak akses semua aplikasi yang telah di-*install* dapat mencegah serangan berbasis *backdoor*. 12. Tidak semua hak akses yang diminta aplikasi perlu diizinkan demi mencegah serangan berbasis *backdoor*	• Benar • Salah • Tidak Tahu
Attitude	1. Saya sadar bahwa *smartphone* berbasis Android berpotensi mendapatkan serangan berbasis *backdoor* yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna. 2. Saya sadar bahwa proses *rooting* sistem operasi Android dapat meningkatkan risiko serangan berbasis *backdoor*. 3. Saya sadar bahwa penggunaan aplikasi tidak diunduh dari Google Play Store atau repositori resmi dapat meningkatkan risiko serangan berbasis *backdoor*. 4. Saya sadar bahwa beberapa *smartphone* Android tertentu sudah tertanam atau diselipkan *backdoor* perangkat keras pada *firmware* sejak dari pabrikannya. 5. Saya sadar bahwa *smartphone* yang aman digunakan adalah yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM (Original Equipment Manufacture) atau juga bisa disebut barang *original*. 6. Saya sadar bahwa *smartphone* yang tidak dikunci dengan *lockscreen* atau biometrik dapat memperbesar peluang terjadinya serangan berbasis *backdoor*. 7. Saya sadar bahwa penggunaan sistem operasi tidak resmi (Custom ROM) dapat membuka peluang lebih besar akan terjadinya serangan berbasis *backdoor*. 8. Saya sadar bahwa *update* versi sistem operasi Android secara teratur dapat meningkatkan keamanan dari serangan berbasis *backdoor*. 9. Saya sadar bahwa *update* aplikasi secara teratur dapat meningkatkan keamanan dari serangan berbasis *backdoor* 10. Saya sadar untuk mempertimbangkan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum meng-*install* nya (termasuk dari Google Play Store atau repositori resmi lainnya) 11. Saya sadar untuk melakukan pengecekan secara berkala akan hak akses semua aplikasi yang telah ter-*install* demi mencegah serangan berbasis *backdoor*. 12. Saya sadar bahwa tidak semua hak akses yang diminta aplikasi perlu saya berikan demi mencegah serangan berbasis *backdoor*.	• Benar • Salah • Tidak Tahu
Behaviour	1. Saya terbiasa untuk melakukan langkah-langkah pencegahan atas serangan berbasis *backdoor* di *smartphone* Android saya. 2. Saya terbiasa untuk tidak melakukan proses *rooting* sistem operasi Android. 3. Saya terbiasa untuk tidak menggunakan aplikasi yang tidak diunduh dari Google Play Store atau repositori resmi lainnya.	• Benar • Salah

	4. Saya terbiasa untuk tidak menggunakan *smartphone* Android tertentu yang berpotensi telah tertanam atau diselipkan *backdoor* perangkat keras pada *firmware* sejak dari pabrikannya. 5. Saya terbiasa untuk hanya menggunakan *smartphone* Android yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM (Original Equipment Manufacture) atau juga bisa disebut barang *original*. 6. Saya terbiasa menggunakan *lockscreen* atau biometrik di *smartphone* Android saya. 7. Saya terbiasa untuk tidak menggunakan sistem operasi tidak resmi (Custom ROM) yang bisa memperbesar peluang terjadinya serangan berbasis *backdoor* 8. Saya terbiasa untuk melakukan *update* versi sistem operasi Android secara teratur. 9. Saya terbiasa untuk melakukan *update* aplikasi secara teratur. 10. Saya terbiasa melakukan pertimbangan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum meng-*install*nya, termasuk dari Google play Store atau repositori resmi lainnya. 11. Saya terbiasa untuk melakukan pengecekan secara berkala akan hak akses semua aplikasi yang telah ter-*install* di *smartphone* saya. 12. Saya terbiasa untuk tidak begitu saja memberikan semua hak akses yang diminta oleh aplikasi apapun yang berjalan di *smartphone* saya.	

D. Analisis Data

Data yang telah dikumpulkan untuk penelitian ini akan dianalisis secara kuantitatif. Pertama, dilakukan perhitungan skor kesadaran keamanan untuk masing-masing responden berdasarkan jawaban dari instrumen yang digunakan untuk mengukur tingkat kesadaran keamanan. Untuk pilihan pada pertanyaan yang dijawab akan diberi bobot nilai yaitu, Benar = 10, Salah = 5, Tidak Tahu = 0. Setelah mendapatkan nilai bobot setiap jawaban pada pertanyaan, nilai bobot tersebut akan digunakan untuk menghitung setiap pertanyaan setiap dimensinya dan dibagi dengan beberapa fokus area yang telah ditentukan.

Kemudian, pembobotan tersebut dilakukan untuk menghitung kesadaran dengan pendekatan *Analytical Hieracrhy Process* (AHP) [12]. Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi secara subjektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen[1]. Setiap dimensi akan memiliki bobot masing-masing yang digunakan dalam perhitungan kesadaran atau *awareness*. Berikut pembagian total bobot untuk dimensi dan area fokus yang dapat dilihat pada Tabel 2. dan Tabel 3.

Tabel 2. Pembagian Bobot Dimensi

Dimensi	Bobot
Knowledge	30%
Attitude	20%
Behavior	50%

Tabel 3. Pembagian Bobot Area Fokus

Area Fokus	Pertanyaan
Backdoor	1,2,3,4
Hardware	4,5,6
Android OS	2,7,8
Apps	3,9,10
Permission	10,11,12

Dari data yang telah dikumpulkan melalui Google Forms tersebut, didapatkan 396 responden yang telah mengisi survei tersebut. Sebelum dilanjutkan untuk perhitungan, data harus dicek kembali untuk memastikan kebenaran data tersebut, maka dilakukan terlebih dahulu pembersihan data. Pembersihan data bertujuan untuk menghapus data yang terindikasi sebuah duplikasi atau data yang sama persis terdapat 2 atau lebih data pengisiannya. Selain itu pembersihan data bertujuan untuk membenarkan beberapa kesalahan penginputan responden yang dibutuhkan, sehingga dapat menyesuaikan dengan kriteria responden yang dibutuhkan dalam penelitian ini. Setelah melakukan proses pembersihan data, dari 396 data yang dikumpulkan, proses pembersihan yang dilakukan yaitu hanya memperbaiki beberapa kesalahan data yang dimasukkan oleh responden, selebihnya tidak ada data duplikasi atau terdapat 2 atau lebih data dalam pengisiannya.

Dari hasil perhitungan tingkat kesadaran yang didapatkan merupakan nilai yang dapat merepresentasikan tingkat kesadaran dalam penggunaan *smartphone* android, baik secara keseluruhan responden penelitian, individu, maupun kelompok individu yang akan dievaluasi sesuai kriteria yang tertera pada Tabel 4. yang merupakan hasil penyesuaian dari model Kruger dan Kearney khusus untuk penelitian ini.

Tabel 4. Kriteria Kesadaran

Kriteria	Nilai (%)	Keterangan
Baik	85 – 100	Sudah baik, perlu dipertahankan
Rata-Rata	75 – 84	Cukup baik, namun masih terbuka peluang ditingkatkan
Buruk	Kurang dari 75	Perlu perhatian khusus untuk upaya peningkatan

Selanjutnya, untuk mengukur skala perbedaan tingkat kesadaran keamanan antar setiap kelompok demografi yang berbeda sekaligus menginvestigasi pengaruh perbedaan faktor demografis tersebut, akan dilakukan analisis lanjutan berupa regresi linear berganda *(Multiple Linear Regression)* dengan metode OLS *(Ordinary Least Squares)* dengan nilai atau skor kesadaran keamanan sebagai DV (*Dependent Variable*) dan berbagai faktor demografi responden sebagai IV *(Independent Variables).*

IV. HASIL & PEMBAHASAN

Tabel 5 berisikan informasi karakteristik 396 orang responden dalam penelitian ini setelah melalui proses pembersihan data. Informasi tersebut telah disajikan dalam berbagai kategori sesuai informasi demografi yang meliputi jenis kelamin, usia, lokasi, pendidikan, penghasilan bulanan dan adopsi teknologi informasi. Dari segi jenis kelamin, survei ini didominasi oleh laki-laki sekitar 52,8% dan perempuan yaitu 47,2%. Dari segi usia, survei ini didominasi oleh responden dengan rentang usia 20-24 tahun yang mencapai 75% dari total responden. Hal ini bisa disebabkan karena mayoritas usia pada sekitar 20 sampai 24 tahun adalah pelajar atau mahasiswa yang sedang menempuh pendidikan pada tahun 2020 yang biasanya identik dengan sebutan kaum *milenial*. Kaum *milenial* umumnya beradaptasi dengan cepat terhadap perkembangan teknologi baru seperti *smartphone*. Remaja berumur kurang dari 20 tahun merupakan salah satu pengguna terbesar *smartphone* dengan persentase 20,9%, jauh lebih besar dibandingkan dengan masyarakat berumur 25 tahun ke atas yang menduduki persentase 4,04%.

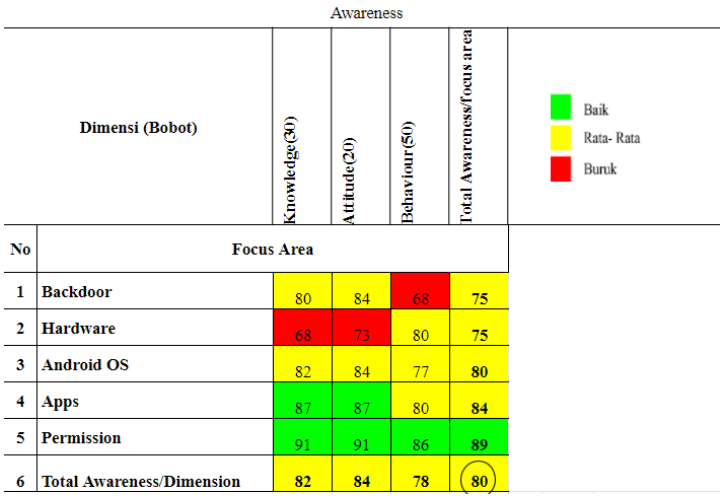
Tabel 5. Karakteristik Responden

	Karakteristik	
	Jumlah	**Persen**
Jenis Kelamin: Laki-Laki	209	52,8%
Perempuan	187	47,2%
Usia: <20	83	20.9%
20 – 24	297	75,0%
≥ 25	16	4,04%
Asal Daerah: Kota	192	48,5%
Kabupaten	204	51,5%
Pulau: Jawa	286	72,3%
Non Jawa	110	27,7%
Pendidikan: Belum lulus Kuliah	345	87,1%
Sudah Lulus Kuliah	51	12,9%
Penghasilan Bulanan: < 1 Juta	207	52,3%
≥ 1 Juta	189	47,7%
Adopsi TI: Early Adopter	90	22,7%
Majority	235	59,3%
Laggard	71	22,7%

Selanjutnya dari segi asal daerah, mayoritas responden berasal dari daerah kabupaten yang mencapai 51,5% dibandingkan dengan responden yang berasal dari kota. Responden yang berasal dari kota hanya mencapai 48% dari total responden. Ini disebabkan oleh lebih banyaknya jumlah kabupaten dibandingkan dengan kota-kota yang ada di Indonesia. Menurut Badan Pusat Statistik (BPS), jumlah kabupaten di Indonesia adalah 416 kabupaten, sedangkan jumlah kota di Indonesia adalah 98 kota[13]. Dari segi pulau, mayoritas responden berasal dari Pulau Jawa dengan jumlah 286 orang atau telah mencapai sekitar 72,3%. Sejumlah 110 orang lainnya berasal dari berbagai macam pulau di luar Jawa seperti Sumatera, Kalimantan, Nusa Tenggara, Papua, dan lain sebagainya.

Dari segi pendidikan, 87,1% survei ini lebih didominasi oleh masyarakat okedengan pendidikan terakhir di jenjang pendidikan dasar sampai menengah akhir, atau bisa disebut pelajar yang belum lulus kuliah dibandingkan yang sudah menamatkan studi di perguruan tinggi. Ini berkaitan dengan usia sebelumnya yang mayoritas pengguna *smartphone* di Indonesia yaitu pada rentang usia sekitar 20 sampai 24 tahun, pada usia tersebut rata-rata pengguna sedang menempuh jenjang perkuliahan dan tamat perkuliahan. Dari segi penghasilan bulanan kurang dari Rp. 1.000.000 yang dikarenakan tingginya angka pelajar dan mahasiswa yang menjadi responden dalam penelitian ini.

Selanjutnya, dilakukan perhitungan skor kesadaran keamanan di kalangan pengguna *smartphone* android di Indonesia yang hasilnya dapat dilihat pada Gambar 1. Untuk keseluruhan pengguna *smartphone* android di Indonesia, didapatkan skor 80 yang dalam penelitian ini dikategorikan ke dalam nilai Rata-Rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge*, *attitude*, maupun *behavior*, juga memiliki nilai Rata-Rata di rentang 78 hingga 84. Dari kelima area fokus yang ada, hanya area fokus *permission* yang mendapatkan kategori baik dengan rentang nilai 86 hingga 91. Dengan kata lain, kesadaran keamanan terkait isu *permission* dirasa sudah baik dan perlu dipertahankan pada level tersebut, sedangkan untuk area fokus *Android OS* memiliki nilai rata-rata di rentang 77 hingga 84. Dengan kata lain, kesadaran keamanan terkait isu *Android OS* dirasa cukup baik, namun masih terbuka peluang ditingkatkan. Untuk area fokus *Backdoor* memiliki nilai rata-rata rentang 68 hingga 84. Dengan kata lain untuk nilai pada titik terendah yaitu 68, sehingga perlu perhatian khusus untuk upaya peningkatan. Dan terakhir untuk area fokus *Hardware* memiliki nilai rata-rata di rentang 68 pada dimensi *Knowledge*, 73 pada dimensi *Attittude*, hingga 80 pada dimensi *Behavior*. Dengan kata lain, kesadaran keamanan terkait isu *Behavior* memiliki titik terendah pada angka 68 pada dimensi *Knowledge*, diikuti nilai 73 pada dimensi *Attitude*, dan terakhir nilai 80 pada dimensi *Behavior*, sehingga perlu perhatian khusus untuk upaya peningkatan pada area fokus *Hardware*.



Gambar 1. Tingkat Kesadaran Keamanan Informasi *Smartphone* Android di Indonesia

Selanjutnya, hasil analisis regresi linear berganda yang bertujuan untuk mencari seberapa besar faktor-faktor yang

ditentukan dari demografis apakah berpengaruh pada perbedaan tingkat kesadaran keamanan *smartphone* android di Indonesia disajikan pada Tabel 6. Dari hasil diagnosis pada iterasi awal, ditemukan lima buah *outliers* dan *influential cases* yang tidak disertakan pada iterasi berikutnya sehingga tersisa 396 responden yang menjadi model akhir di analisis regresi ini. Faktor yang memiliki pengaruh paling besar yaitu jenis kelamin.

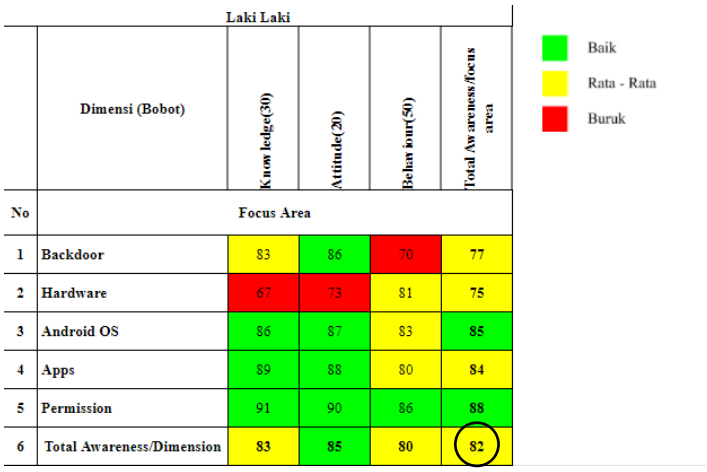
Tabel 6. Hasil Regresi Linear Berganda atas Skor Kesadaran Keamanan Pengguna *Smartphone* android di Indonesia

Jenis Kelamin *Perempuan*	**-3.396** **-0.134** **(0.055)**	*
Usia	**0.495** **0.108** **(0.061)**	.
Asal Daerah *Kota*	**-0.374** **-0.015** **(0.056)**	
Pulau *Jawa*	**-2.056** **-0.073** **(0.057)**	
Pendidikan *Sudah lulus kuliah*	**-0.818** **-0.021** **(0.061)**	
Penghasilan Bulanan *Kurang dari 1 juta rupiah*	**1.481** **0.017** **(0.056)**	
Constant/Intercept	**71.627** **-0.011** **(0.055)**	***
R^2 **Highest VIF** **Mean VIF** **Ramsey RESET Test** **Observation**	**0.032** **1.308** **1.109** **0.232** **391**	

Catatan: Angka pada baris pertama adalah unstandardized estimate, baris kedua adalah standardized estimate (beta), dan baris ketiga adalah robust standard error; '***' p < 0.001, '**' p<0.01, '*' p<0.05, '.' p<0.1, ' ' p<1.

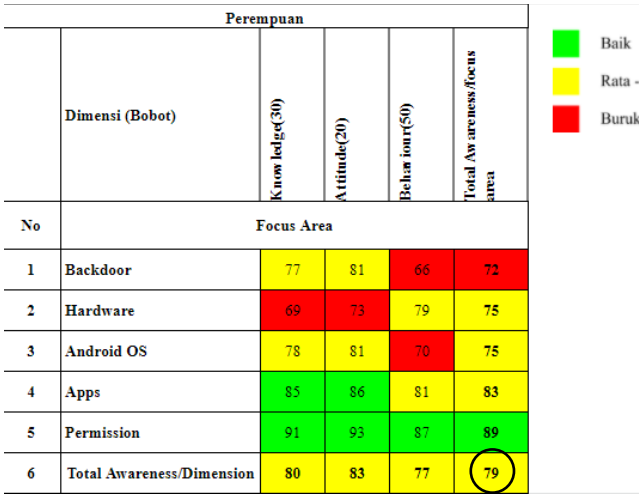
Hasil regresi linear berganda atas skor dari kesadaran keamanan pengguna *smartphone* Android menunjukkan perbedaan signifikan pada tingkat kesadaran hanya terdapat pada faktor jenis kelamin, di mana perempuan memiliki nilai 3,4 poin lebih rendah dari laki-laki jika semua faktor lain dianggap konstan.

Untuk mengetahui perbandingan dari perhitungan skor kesadaran keamanan pada kategori demografi jenis kelamin yang hasilnya dapat dilihat pada Gambar 2. dan Gambar 3. Untuk kategori jenis kelamin laki-laki didapatkan skor total *awareness* 82 lebih tinggi dari total skor *awareness* perempuan. Dalam penelitian ini skor *awareness* laki-laki dikategorikan kedalam nilai Rata-Rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude*, maupun *behavior*, juga memiliki nilai Rata-Rata di rentang 80 hingga 85. Dari kelima area fokus yang ada, pada area fokus *permission* yang mendapatkan kategori baik dengan rentang nilai 86 hingga 91. Dengan kata lain, kesadaran keamanan terkait isu *permission* dirasa sudah sudah baik dan perlu dipertahankan pada level tersebut. Dan area fokus *Android OS* yang mendapatkan kategori baik dengan rentang nilai 83 hingga 87. Untuk area fokus lainya, seperti *Backdoor, Hardware, Apps* memiliki nilai rata-rata, sehingga dirasa cukup baik, namun masih terbuka peluang untuk upaya peningkatan.



Gambar 2. Tingkat kesadaran Keamanan Informasi Jenis Kelamin Laki – Laki

Kemudian, dibandingkan dengan perhitungan skor keamanan pada kategori demografis jenis kelamin laki-laki. Jenis kelamin perempuan memiliki skor *awareness* yang lebih rendah dengan laki-laki. Menurut Farooq, Isoaho, dan Virtanen, bahwa perempuan memiliki tingkat kesadaran yang lebih rendah dibandingkan laki-laki karena perempuan sering kali tidak mengetahui dan tidak menyadari apa yang mereka lakukan di dunia maya[14]. Dalam penelitian ini skor *awareness* perempuan dikategorikan ke dalam nilai Rata-Rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude*, maupun *behavior*, juga memiliki nilai Rata-Rata di rentang 77 hingga 83. Dari kelima area fokus yang ada, hanya pada area fokus *permission* yang mendapatkan kategori baik dengan rentang nilai 87 hingga 93. Dengan kata lain, kesadaran keamanan terkait isu *permission* dirasa sudah sudah baik dan perlu dipertahankan pada level tersebut. Namun pada area fokus *backdoor* mendapatkan kategori buruk dengan total skor *awareness* 72, sehingga perlu perhatian khusus untuk upaya peningkatan. Untuk area fokus lainya, seperti *Hardware, Android OS, Apps* memiliki nilai rata-rata, sehingga dirasa cukup baik, namun masih terbuka peluang untuk upaya peningkatan.



Gambar 3. Tingkat Kesadaran Keamanan Informasi Jenis Kelaminf Perempuan

V. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan ini, telah didapat hasil tingkatan kesadaran keamanan atau *security awareness* pengguna *smartphone* android di Indonesia yaitu berada pada tingkatan rata-rata. Hasil ini berdasarkan nilai kesadaran total yang ada pada Gambar 1 sebelumnya yaitu 80 dari nilai maksimal keseluruhan 100. Dengan begitu hasilnya berada pada tingkatan kategori rata-rata, maka masih dapat ditingkatkan kembali di beberapa bagian, terutama pada area fokus *Backdoor*, *Hardware* dan *Android OS* yang cukup tertinggal jika dibandingkan dengan area fokus *Permission*, *Apps*. Pada ketiga area tersebut, perlu dilakukan upaya-upaya khusus dalam bentuk edukasi pengguna untuk meningkatkan kesadaran keamanan dalam menggunakan *smartphone* android untuk menghindari dari serangan berbasis *backdoor* yang dapat mengakses *smartphone* android dengan mudah, dan mencegah terjadinya kehilangan data dan pencurian informasi.

Selain itu, penelitian ini juga menemukan hasil yang signifikan dalam menganalisis tingkatan kesadaran keamanan pengguna *smartphone* android di Indonesia berdasarkan faktor-faktor demografis responden, terutama pada kategori Jenis Kelamin. Pengguna *smartphone* android dengan jenis kelamin Perempuan memiliki tingkat kesadaran keamanan yang lebih rendah, dibanding pengguna *smartphone* android dengan jenis kelamin laki-laki. Adapun terkait faktor lain seperti, usia, pendidikan, lokasi, tidak ditemukan perbedaan yang signifikan antara kelompok pengguna *smartphone* android yang berbeda dalam penelitian ini.

Hasil dari penelitian ini diharapkan dapat berguna untuk menjadi sebuah acuan untuk melakukan penelitian serupa dengan area fokus yang berbeda ke depannya. Selain itu, masih terdapat beberapa kesalahan yang ada pada penelitian ini, seperti pertanyaan yang digunakan untuk meningkatkan skor kesadaran keamanan masih perlu ditingkatkan lebih baik lagi dari segi kuantitas dan kualitas sebuah pertanyaan, juga pertanyaan yang mudah dimengerti dan dipahami oleh responden. Kemudian karakteristik responden dalam pengisian cenderung bersifat homogen, baik dari sisi usia maupun lokasi dapat berpotensi menyebabkan nilai kesadaran pengguna yang perlu kehati-hatian lebih jika akan dilakukan proses generalisasi ke seluruh pengguna *smartphone* Android di Indonesia.

REFERENSI

[1] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," *J. Sist. Inf. Bisnis*, vol. 8, no. 2, p. 115, 2018.

[2] M. Universitas, B. Darma, D. Universitas, B. Darma, J. A. Yani, and N. Plaju, "Analisis Pendeteksian dan Pencegahan Serangan Backdoor Pada Layanan Server," no. 12, pp. 1–10.

[3] H. D. Kartika, *Pengukuran Tingkat Kesaranan Keamanan Infomrasi: Studi Kasus PT MNC SKY VISION Tbk.*, vol. 1, no. 4. 2019.

[4] M. Amin, "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda)," *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, pp. 15–24, 2014.

[5] H. Chan and S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector," *Int. J. Comput. Appl.*, vol. 60, no. 10, pp. 23–31, 2012, doi: 10.5120/9729-4202.

[6] M. E. Whitman and H. J. Mattord, "Principles of Information Security Fourth Edition," *Learning*, pp. 269, 289, 2011.

[7] M. Alexander, "Protect, Detect and Correct Methodology to Mitigate Incidents: Insider Threats," *Isaca J.*, vol. 3, pp. 1–7, 2018.

[8] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[9] T. S. E. G. Tan, "Isu Keselamatan Peranti Mudah Alih Dalam Dunia Digital untuk Institusi Pengajian Tinggi," no. November 2019, pp. 119–129, 2020.

[10] P. Faruki *et al.*, "Android security: A survey of issues, malware penetration, and defenses," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 998–1022, 2015, doi: 10.1109/COMST.2014.2386139.

[11] N. T. Puspita Kencana Sari, Candiwan, "Information Security Awareness Measurement with Confirmatory Factor Analysis," *SAGE Encycl. Educ. Res. Meas. Eval.*, no. Istmet 2014, pp. 218–223, 2018.

[12] P. Kencana Sari and Candiwan, "Measuring information security awareness of Indonesian smartphone users," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 12, no. 2, pp. 493–500, 2014.

[13] Badan Pusat Statistik, "Statistik Indonesia 2019," *BPS, 2019 (Indonesian Stat.*, p. Jakarta: Badan Pusat Statistik, 2019.

[14] A. Farooq, "Information Security Awareness in Educational Institution : An Analysis of Students ' Individual Factors," no. December, 2015, doi: 10.13140/RG.2.1.4128.5205.