ANALISIS KESADARAN KEAMANAN DI KALANGAN PENGGUNA *SMARTPHONE* ANDROID ATAS SERANGAN BERBASIS *BACKDOOR*

Disusun Oleh:

N a m a : Muhammad Raffi Akhyari

NIM : 17523207

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2020

HALAMAN PENGESAHAN DOSEN PEMBIMBING

ANALISIS KESADARAN KEAMANAN DI KALANGAN PENGGUNA *SMARTPHONE* ANDROID ATAS SERANGAN BERBASIS *BACKDOOR*

TUGAS AKHIR

Disusun Oleh:

N a m a : Muhammad Raffi Akhyari

NIM : 17523207

Yogyakarta, 14 Desember 2020

Pembimbing,

(Ahmad M. Raf'ie Pratama, S.T., M.I.T., Ph.D.)

HALAMAN PENGESAHAN DOSEN PENGUJI

ANALISIS KESADARAN KEAMANAN DI KALANGAN PENGGUNA *SMARTPHONE* ANDROID ATAS SERANGAN BERBASIS *BACKDOOR*

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 13 Januari 2021

Tim Penguji

Ahmad M. Raf'ie Pratama, ST., M.I.T., Ph.D. _____

Anggota 1

Andhik Budi Cahyono, S.T., M.T. _____

Anggota 2

Moh. Idris, S.Kom., M.Kom. _____

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Muhammad Raffi Akhyari

NIM : 17523207

Tugas akhir dengan judul:

ANALISIS KESADARAN KEAMANAN DI KALANGAN PENGGUNA *SMARTPHONE* ANDROID ATAS SERANGAN BERBASIS *BACKDOOR*

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 14 Desember 2020

(Muhammad Raffi Akhyari)

HALAMAN PERSEMBAHAN

Alhamdulillahirobbil'alamin, puji syukur kepada Allah SWT atas izin dan karunia-Nya telah diberikan kelancaran, kemudahan, dan kebarokahan selama proses pembuatan hingga penyelesaian Laporan Tugas Akhir tepat pada waktunya.

Terima kasih yang tak terhingga untuk orang tua ku tercinta Mama Rahmawati, Etah Farudi, dan Mama Septina Kristianingrum yang sudah banyak sekali memberikan doa, dukungan, tenaga, usaha, pikiran, nasehat dan hal-hal lain yang tidak bisa disebutkan satu per satu. Terima kasih banyak Mama dan Etah yang selalu mendampingi Raffi sejak kecil hingga dewasa ini. Mohon maaf jika Raffi belum bisa memberikan sesuatu yang dapat menggantikan rasa kasih sayang yang sudah Mama dan Etah berikan selama ini.
Terima kasih juga untuk adik-adik saya tercinta, Sella Ratna Septiani, Muhammad Ilhan Manzis, Muhammad Reyhan Dzakwan, Aulia Maritza Elvina, Adinda Fitriana Agustine, dan Muhammad Fatih Haidar yang selalu memberikan semangat untuk Raffi, mendoakan Raffi.
Terima kasih sudah mau terus berjuang dan mau belajar bersama
hingga saat ini.

Terima kasih untuk Bapak Ahmad Munasir Raf'ie Pratama, ST., M.I.T., Ph.D., selaku pembimbing, Ketua Program Studi Informatika dan Para Dosen Informatika yang selalu membimbing dan mengajarkan ilmu-ilmu pengetahuan hingga pelajaran hidup yang sangat berharga untuk bekal kehidupan
yang akan mendatang.

Terimakasih untuk seluruh keluarga besar atas doa, nasehat, dan bantuan yang telah diberikan kepada Raffi selama ini, dan telah mengajarkan tentang rasa kebersamaan dan kekuatan dari dukungan sebuah keluarga.

Semoga Allah mengganti kebaikan-kebaikan yang kalian berikan dengan kebaikan yang lebih lagi. Semoga diberikan kelancaran, kemudahan, kebarokahan, kesehatan dan kebahagiaan untuk kita semua. Aamiin.

HALAMAN MOTO

لَا يُكَلِّفُ اللّٰهُ نَفْسًا اِلَّا وُسْعَهَا

"Allah tidak membebani seseorang hambanya melainkan sesuai dengan kesanggupannya"

Q.S Al Baqarah: 286

"Alih-alih menetapkan tujuan, carilah momen yang menentukan. Itu adalah ujian yang sebenarnya, karena Anda harus rela gagal dalam situasi tekanan di depan orang lain."

Huge Jackman

"Menjadi orang baik itu lelah, tetapi rasa lelah itu disembuhkan dengan kebahagiaan orang lain atas kebaikan yang kita perbuat"

Muhammad Raffi Akhyari

KATA PENGANTAR

Puji dan syukur tak terhingga kepada Allah *SWT* yang Maha Agung dan Maha Pengasih atas nikmat dan rahmat-Nya, serta segala kekuatan, kemudahan dan kelancaran sehingga karya ini dapat terselesaikan dengan baik. Shalawat serta salam senantiasa tercurah kepada Nabi kita Nabi Muhammad *SAW,* keluarga sahabat dan para pengikutnya. Berkat rahmat dan pertolongan Allah *SWT* penulis dapat menyelesaikan Laporan Tugas Akhir tentang Kesadaran Keamanan di Kalangan Pengguna *Smartphone* Android atas Serangan Berbasis *Backdoor*.

Penulis menyadari bahwa dalam penyelesaian skripsi banyak pihak yang telah memberikan bantuan, bimbingan, dan dukungan. Oleh karena itu, dalam kesempatan ini perkenankan penulis mengucapkan rasa syukur dan terima kasih yang tak terhingga kepada:

1. Orang tua tercinta (Bapak Farudi, Mama Rahmawati, Mama Septiani Kristianingrum) dan Adik-adikku (Sella Ratna Septiani, Muhammad Ilhan Manzis, Muhammad Reyhan Dzakwan, Aulia Maritza Elvina, Adinda Fitriana Agustine, dan Muhammad Fatih Haidar) yang tiada hentinya telah memberikan doa, cinta, kasih sayang, nasehat, dukungan, motivasi, serta pengorbanan yang tak terhingga selama ini hingga skripsi dan masa perkuliahan ini dapat diselesaikan dengan baik.
2. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc. selaku Ketua Program Studi Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Bapak Ahmad Munasir Raf'ie Pratama, ST., M.I.T., Ph.D. selaku Dosen Pembimbing Skripsi, atas segala bimbingan, waktu, dan pemikiran yang selalu diberikan sejak sebelum skripsi ini dibuat, dengan waktu
4. Seluruh dosen Program Studi Informatika Fakultas Teknologi Industri Universitas Islam Indonesia yang banyak memberikan ilmu, pelajaran, pengalaman, serta nasihat yang tak dapat terhitung jumlahnya. Semoga kebaikan Bapak/Ibu dosen Allah berikan balasan yang bermanfaat dan barokah.
5. Kepada sahabat dan teman hidup dunia akhirat ku (Mafhirota Afifah, Abdul Aziz Barunda, Difka Sabila Rasyad, Yahya Maulana Ibrahim, Agil Albertini, Royan Zahara Putri, Qonita Alimatu, Novianna Wulandari) *Alhamdulillah JazaKumullahu Khoiro* terima kasih atas nasihat, motivasi, dan kebersamaan serta rasa persaudaraan yang telah tercipta selama di Jogja. Dukungan yang tiada habisnya kalian berikan, memberikan kontribusi terhadap penelitian ini. Semoga kekeluargaan kita tetap terjalin dengan baik tidak hanya di dunia, namun akhirat juga.

6. Teman-teman Harapan Bangsa (Arap, Teguh, Ardhy, Alip, Nopal, Axel, Zaki, Akbar) dan yang lainnya tak bisa penulis sebutkan satu per satu, terima kasih atas dukungan dan waktu kebersamaanya selama masa perkuliahan yang kemudian menjadikan Jogja semakin dirindu-rindukan. Semoga kesuksesan selalu mengiringi kalian semua.
7. Teman-teman seperjuangan Expo Informatika (Faza, Rio, Syamil, Rizaldi, Ivan) dan yang lainnya tak bisa penulis sebutkan satu per satu, terima kasih atas dukungan dan ilmu yang telah kalian berikan selama masa perkuliahan menempuh Expo Informatika ini. Semoga kesuksesan selalu mengiringi kalian semua.
8. Teman-teman Informatika UII angkatan 2017, atas segala bantuan dan kebersamaan selama masa perkuliahan. Semoga silaturahmi kita bisa tetap terjalin dengan baik.
9. Teman-teman seperjuangan SBMPTN (Ayu, Vega) terima kasih telah mengajarkan bentuk sebuah keikhlasan, bahwa semua itu dapat diraih dengan belajar dan usaha. Semoga kalian diberikan kelancaran dalam menjalankan tugas akhir dan penelitian kalian, semoga sukses mengiringi kalian.
10. Semua pihak yang telah membantu penulis dengan penuh keikhlasan, yang tidak dapat disebutkan satu persatu, terima kasih atas segala bantuan yang telah diberikan kepada penulis.

Pada akhirnya, penulis mengharapkan semoga skripsi ini dapat bermanfaat bagi penulis dan semua pihak yang berkenan menelaah di kemudian hari. Semoga Allah SWT memberikan limpahan rahmat, karunia dan balasan yang lebih baik atas kebaikan semua pihak yang secara langsung maupun tidak langsung membantu terwujudnya skripsi ini, Aamiin ya Rabbal alamin.

Yogyakarta, 14 Desember 2020

(Muhammad Raffi Akhyari)

SARI

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 dan Usia. 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.

Kata kunci: *Smartphone*, Kesadaran Keamanan, *Backdoor*, Android, Literasi Digital

GLOSARIUM

Backdoor	*Backdoor* adalah suatu teknik *hacker* atau peretas yang dapat memungkinkan mereka peretas mengakses ke suatu sistem tanpa melalui autentifikasi normal (login).
OLS	Metode statistik analisis untuk memperkirakan atau menghitung hubungan antara satu atau lebih variabel independen dan variabel dependen
RStudio	IDE untuk pemrograman Bahasa R yang digunakan untuk komputasi statistik dan grafik
Security Awareness	Kesadaran keamanan yang dimiliki oleh setiap orang untuk melindungi segala informasi yang dimilikinya.
Outliers	titik data yang sangat berbeda dengan titik data lainnya dalam suatu kumpulan data.
Influential Cases	Kasus apa pun yang secara signifikan mengubah nilai koefisien regresi setiap kali nilai tersebut dihapus dari analisis.
Android	Android merupakan sistem operasi dengan perangkat mobile berbasis linux yang dapat mencakup sistem operasi, middleware, dan aplikasi.
Literasi Digital	Pengetahuan dan kecakapan dalam menggunakan media digital, alat-alat komunikasi, dan dapat memanfaatkanya secara sehat, bijak, cerdas, cermat, tepat, dan patuh hukum
Cyber Crime	Tindak kejahatan melalui komputer dan jaringan internet
AHP	Sebuah metode untuk memeringkat alternatif keputusan dan memilih yang terbaik dengan beberapa kriteria.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

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 (Akraman et al., 2018).

Seiring berjalannya waktu, *smartphone* sering mengalami permasalahan pada sistem operasi. 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* (Kurniawan et al., 2017).

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 (Kartika, 2019). Rogers (2003) mengatakan, bahwa keputusan mengadopsi suatu inovasi, termasuk teknologi informasi dipengaruhi oleh tiga jenis pengetahuan: (1) pengetahuan kesadaran bahwa teknologi informasi itu ada, (2) pengetahuan prosedural tentang bagaimana menggunakan teknologi informasi, dan (3) pengetahuan prinsip atau pemahama tentang teknologi informasi (Glanz et al., 2002).

Dalam penelitian ini, pertanyaan yang akan dijawab adalah seberapa besar pengetahuan tentang kesadaran keamanan akan informasi 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. Karena banyaknya permasalahan dan kejahatan yang dilakukan para peretas Penelitian ini diharapkan dapat berkontribusi untuk memberikan gambaran tingkat kesadaran keamanan di kalangan pengguna *smartphone* Android di Indonesia.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

a. Seberapa besar pengetahuan tentang kesadaran keamanan akan informasi di kalangan pengguna *smartphone* Android di Indonesia?
b. Bagaimana tingkat kesadaran keamanan di kalangan pengguna *smartphone* Android di Indonesia?
c. Bagaimana dampak pengetahuan akan *security awareness* pengguna *smartphone* Android terkait serangan berbasis *backdoor*?
d. Apakah ada perbedaan tingkat pengetahuan dan kesadaran akan keamanan, serta kebiasaan penggunaan *smartphone* Android berdasarkan faktor demografis seperti jenis kelamin, usia, lokasi seperti kabupaten/kota maupun asal pulau, pendidikan terakhir, adopsi teknologi informasi dan penghasilan bulanan di Indonesia.

1.3 Batasan Masalah

Batasan penelitian yang diberikan agar lebih terarah dan sesuai dengan yang dimaksudkan adalah sebagai berikut:

a. Pengambilan data yang dilakukan survey secara daring via Google Form dan akan disebar luaskan kepada seluruh pengguna *smartphone* Android se-Indonesia.
b. Kriteria responden penelitian ini yaitu pengguna *smartphone* Android se-Indonesia.

1.4 Tujuan Penelitian

Menganalisis kesadaran keamanan terhadap serangan *backdoor*, kepada para pengguna *smartphone* Android se-Indonesia, dan menganalisis literasi digital setiap

pengguna *smartphone* Android guna mengetahui tingkatan kesadaran keamanan terkait penggunaan *smartphone* Android.

1.5 Manfaat Penelitian

Penelitian ini diharapkan untuk mengetahui seberapa pentingnya kesadaran keamanan bagi pengguna *smartphone* terkait serangan berbasis *backdoor* dan mengetahui bentuk pemahaman literasi digital yang dapat ditanamkan kepada pengguna *smartphone* Android sehingga pengguna dapat mengetahui dan mengantisipasi dari pencurian data, dan pembocoran informasi pribadi akibat dari serangan berbasis *Backdoor*.

BAB II
LANDASAN TEORI

2.1 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 (Amin, 2014). Menurut Von Solms dan Cervone (1998, 2005), dalam meminimalisir risiko pada pelanggaran terhadap keamanan informasi, sangat penting bagi setiap organisasi terutama pengguna untuk menerapkan rencana atau strategi keamanan informasi. Namjoo (2008) mengatakan, pencegahan yang dilakukan setelah terjadinya suatu pelanggaran keamanan informasi, bisa menjadi sangat terlambat (Chan & Mubarak, 2012). Whitman dan Mattord (2011) 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 (Whitman & Mattord, 2011). Adapun Harris dan Maymi (2016) 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 (Alexander, 2018).

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 (Kruger & Kearney, 2006). Untuk mengetahui tingkat kesadaran keamanan informasi pengguna, Kruger dan Kearney (2006) 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 (*behavior*). 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 (Kruger & Kearney, 2006).

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 (Tan, 2020). Sejak awal, sistem operasi dirancang untuk dianggap sebagai *platform* seluler yang tidak hanya kaya fitur, kuat dan seluler, tetapi juga open source (Faruki et al., 2015). 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* (Sari & Candiwan, 2014).

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 (Kurniawan et al., 2017). 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 dilakukan 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.

2.2 Landasan Teori

2.2.1 *Security Awareness*

Program kesadaran keamanan sering kali dilembagakan untuk meningkatkan tingkat kesadaran peserta tentang faktor risiko di area risiko tertentu. Sayangnya, pemahaman yang lebih baik tentang risiko yang terkait dengan area tertentu tidak menjamin hasil yang spesifik. Kruger dan Kearney (2006) menjelaskan faktor-faktor berikut yang harus dihasilkan dari menangani tingkat kesadaran dalam suatu organisasi, yaitu *Knowledege* (apa yang orang tahu atau pengetahuan seseorang), *Attitude* (apa yang orang pikirkan), *Behaviour* (apa yang orang tersebut lakukan). Kesadaran keamanan informasi *smartphone* menentukan tingkat pengetahuan yang dimiliki karyawan dan manajer organisasi terkait dengan keamanan seluler dari informasi yang terdapat pada perangkat tersebut. Selanjutnya, definisi ini mendefinisikan sikap yang ditanggapi oleh kelompok-kelompok ini terhadap pengetahuan yang mereka miliki, dan perilaku spesifik apa yang mereka ambil sebagai tanggapan atas gabungan sikap dan pengetahuan mereka. Tingkat kesadaran mencakup faktor-faktor ini karena tidak hanya terkait dengan perangkat dan kemampuannya, tetapi juga konteks yang berubah di mana perangkat digunakan sebagai perjalanan pengguna seluler sepanjang hari. Upaya penyadaran saat ini berfokus pada pelatihan sekali dengan pemantauan yang sangat sedikit terhadap perilaku organisasi dalam jangka panjang (Allam et al., 2014). Peneliti membuat sebuah pertanyaan dari kesadaran keamanan untuk menguji sisi *attitude*, *knowledge*, dan *behavior* dalam perspektif penggunaan *smartphone* Android. Beberapa pertanyaan dijawab dalam skala 3 poin yaitu setuju, tidak tahu dan tidak setuju (dimensi *attitude* dan *knowledge*), sementara yang lain hanya membutuhkan jawaban yang setuju atau tidak setuju (dimensi *behavior*) (Sari & Candiwan, 2014). Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu pengetahuan (apa yang mereka ketahui tentang keamanan dan privasi), Sikap (bagaimana perasaan mereka tentang keamanan dan privasi), dan perilaku (apa yang mereka lakukan terhadap keamanan dan privasi) (Kartika, 2019). Tujuan utama dari program kesadaran keamanan adalah untuk meningkatkan kesadaran keamanan informasi karyawan dalam sebuah organisasi. Seperti program lainnya, keberhasilan program kesadaran keamanan informasi akan sangat bergantung pada bagaimana informasi kesadaran tersebut disampaikan. Ada banyak model penyampaian kesadaran keamanan informasi. Model ini mampu meningkatkan kesadaran karyawan tentang beragam masalah keamanan dunia maya yang berkisar dari *spam* dan *phishing* hingga serangan

yang terorganisir dengan baik yang dimaksudkan untuk merusak atau menonaktifkan sistem. Pada bagian ini, akan ditinjau berbagai metode penyampaian kesadaran keamanan informasi yang biasa digunakan untuk memberikan konteks untuk diskusi berikutnya tentang pekerjaan kami (Abawajy, 2014).

2.2.2 Model Kruger dan Kearney

Metodologi ini digunakan untuk mengembangkan alat ukur yang didasarkan pada teknik yang dipinjam dari bidang psikologi sosial yang mengusulkan bahwa kecenderungan yang dipelajari untuk merespons dengan cara yang menguntungkan atau tidak menguntungkan untuk objek tertentu memiliki tiga komponen yaitu pengaruh, perilaku dan kognisi (Kruger & Kearney, 2006). Ketiga komponen ini digunakan sebagai dasar dan model yang dikembangkan pada tiga dimensi ekuivalen yaitu apa yang diketahui seseorang (pengetahuan), bagaimana perasaan mereka tentang topik (sikap), dan apa yang mereka lakukan (perilaku) (Kruger & Kearney, 2006).

Sebagai bentuk klasifikasi pertama dari apa yang harus diukur, itu diputuskan untuk mengukur tiga dimensi yaitu *knowledge* (apa yang anda ketahui), *attitude* (apa yang anda pikirkan) dan *behavior* (apa yang anda lakukan) (Kruger & Kearney, 2006). Masing-masing dari dimensi tersebut kemudian dibagi menjadi enam area fokus seperti yang dibahas dan menjadi dasar program kesadaran (Kruger & Kearney, 2006). Untuk mendapatkan nilai *knowledge*, *attitude*, dan *behavior*, maka dilakukan dengan memberi sejumlah pertanyaan kepada responden melalui sebuah kuesioner. Beberapa pertanyaan yang dijawab di skala dengan 3 poin benar, tidak tahu, dan salah (dimensi *attitude* dan *knowledge*), sementara yang lain hanya memerlukan respon benar dan salah saja (dimensi *behavior*) (Sari & Candiwan, 2014).

Selanjutnya, perlu dilakukan pembobotan pada dimensi dan area fokus. Pembobotan kesadaran ditentukan menggunakan *Analytical Hierarchy Process* (AHP) (Sari & Candiwan, 2014). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi subyektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen (Akraman et al., 2018). Setiap dimensi akan memiliki bobot masing-masing yang digunakan dalam perhitungan kesadaran atau *awareness* nantinya.

2.2.3 Android OS

Android adalah sebuah *platform open-source* yang tersusun secara komprehensif dan dirancang untuk *smartphone.* Dikatakan komprehensif karena Android menyediakan semua *tools* dan *frameworks* yang lengkap agar dapat menyimpan sebuah informasi penting yang akan diperlukan tetap tersimpan meskipun *smartphone* dimatikan. Penyimpanan data yang diterapkan oleh sistem operasi Android yaitu menggunakan *SQLite* yang merupakan suatu *open source database* yang cukup stabil dan telah banyak digunakan pada banyak *smartphone* berukuran kecil (Silvia et al., 2014).

a. Sejarah Android

Android merupakan sistem operasi dengan perangkat mobile berbasis linux yang dapat mencakup sistem operasi, *middleware,* dan aplikasi. Android menyediakan *platform* terbuka atau *open source* bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan bermacam *smartphone*. Pada awalnya, perusahaan Google Inc. membeli Android Inc. yang merupakan sebuah pendatang baru yang dapat membuat *software* untuk *smartphone*. Kemudian Android dikembangkan dengan dibentuknya *Open Handset Alliance,* dan konsorsium dari 34 perusahaan *hardware, software* dan telekomunikasi, termasuk Google, Intel, HTC, Qualcomm, Motorola, T-Mobile, dan Nvidia (Andi, 2015). Pada saat perilisan perdana Android, pada tahun 5 November 2007, Android bersama *Open Handset Alliance* menyatakan untuk mendukung semua pengembang *open source* pada perangkat mobile. Di lain pihak, Google akan merilis kode-kode Android di bawah license *Apache,* sebuah lisensi *software* dan *open platform* pada sebuah perangkat seluler, yaitu *smartphone.*

b. Versi Android

Dari sejarah dan perkembangan Android yang sangat cepat ini, diketahui bahwa proses adalah hal yang terpenting. *Google* dalam memberikan nama untuk versi Androidnya sangat menarik. Dari mulai Android akan dirilis untuk komersial selalu diberikan nama yang berkaitan dengan makanan manis dan sesuai urutan abjad, hanya saja untuk veri Android yang terbaru dinamai Android 10 untuk memperingati bahwa Android telah berjalan 1 dekade (Ramadhani, 2019). Berikut penjelasan terkait versi Android:

- Android 1

  Versi Android 1.0 dirilis pertama kali dengan sebutan Android 1.0 Alpha. Android 1.0 Alpha diluncurkan dan diperkenalkan pada September 2008 dan tidak digunakan untuk kebutuhan komersial. Walaupun belum dirilis secara komersial, versi Android

ini dilengkapi dengan fitur-fitur dukungan seperti akses web *browser*, *streaming* youtube, pemutar media, *Google Maps*, dan sinkronisasi dengan aplikasi *Google* lainnya.

Selang beberapa bulan versi Android 1.0 *Alpha* rilis, versi Android 1.1 *Beta* diluncurkan pada tanggal 9 Februari 2009. Sama seperti Android *Alpha*, versi Android ini belum dirilis secara komersial, hanya diperuntukan untuk satu perangkat saja. Pembaruan yang dilakukan yait memperbaiki *bugs* dan meningkatkan performa beberapa fitur seperti rincian lokasi pada aplikasi *maps* serta fitur untuk menyembunyikan dan mnampilkan tombol panggilan.

Pada tanggal 30 April 2009 diluncurkan kembali versi Android 1.5 Cupcake yang akan diperkenalkan secara komersial. Versi Cupcake merupakan generasi pertama yang telah dirilis secara komersial, dan berawal dari versi Android 1.5 Cupcake mulai menggunakan nama makanan manis kepada setiap versi Android yang dirilisnya. Fitur yang ditawarkan pada versi Android 1.5 Cupcake ini yaitu seperti dukungan akan rotasi layar otomatis, *widget*, dan *keyboard* virtual. Pada tanggal 15 September 2009 Android kembali mengembangkan versi terbarunya yaitu Android 1.6 Donut. Pada versi ini Android menambahkan beberapa fitur seperti persentase daya baterai, dukungan gestur, fasilitas pencarian di Android market atau yang sekarang kita kenal dengan *Play Store*

- Android 2.0

Selang sebulan setelah melakukan pembaruan pada versi Android sebelumnya, Android kembali merilis versi terbarunya yaitu Android 2.0 Eclair, dirilis dan diluncurkan tepat pada tanggal 26 Oktober 2009 sebulan setelah Android merilis Android 1.6 *Donut*. Pembaruan yang diberi nama *Éclair* dan pada versi ini terdapat beberapa fitur tambahan baru seperti *multi touch, live wallpaper*, perubahan tampilan antarmuka dan dukungan *browser* untuk HTML5.

Kemudian pada tanggal 20 mei 2010 Android kembali meluncurkan versi terbarunya yaitu versi 2.2 *Froyo*. Pada versi Froyo ini sudah mulai dikenal luas oleh vendor atau pabrikan produksi ponsel. Pembaruan yang ditawarkan oleh Android 2.2 ini membawa beberapa fitur unggulan seperti memperbesar gambar pada galeri dengan gestur, peningkatanan fitur USB *tethering* dan *Hotspot Wifi* serta dukungan animasi GIF pada *Website Browser.*

Tanggal 6 Desember 2010 Android kembali merilis versi terbarunya yaitu Android 2.3 Gingerbread, pada versi ini tidak bisa diragukan lagi karena Android telah menjadi sistem operasi *mobile* yang populer. Kerjasama antar pabrikan Samsung dalam membuat produk *smartphone* Samsung *Galaxy Series* semakin menambah kepopuleran Android. Versi 2.3 ini didukung dengan fitur seperti NFC, fitur *copy* atau *paste* dengan memilih kata melalui layar yang ditekan serta dukungan beberapa sensor lainnya.

- Android 3.0 *Honeycomb*

Versi Android berikutnya yang telah dirilis oleh Android yaitu, Android 3.0 *Honeycomb* yang dirilis dan diperkenalkan pada tanggal 22 Februari 2011. Versi ini dikhususkan untuk menjadi sebuah perangkat tablet PC, dengan fitur yang ditujukan untuk komputasi bisnis pada tablet. Fitur yang dimiliki Android *Honeycomb* memiliki dukungan prosesor *multi core,* dukungan obrolan video dengan *Google Talk* dan percepatan saat berpindah aplikasi yang sedang berjalan dengan fitur *multitasking recent apps.*

- Android 4.0

Tepat pada tanggal 19 Oktober 2011 Android kembali menunjukkan pembaruan terbarunya terhadap versi Android dari sebelum-sebelumnya. Android 4.0 diluncurkan dengan versi terbarunya yaitu Android 4.0 *Ice Cream Sandwich*. Versi ini menunjukan fitur-fitur yang dimiliki oleh Honeycomb sebelumnya untuk bisa berjalan pada *smartphone* yang sebelumnya hanya ditujukan untuk tablet PC. Selain itu fitur tambahan seperti perbaikan antarmuka dan kustomisasi *widget.*

Android 4.1 *Jelly Bean* diluncurkan pada tanggal 27 Juni 2012. Versi pengembangan yang difokuskan pada *Jelly Bean* yaitu peningkatan performa tampilan antarmuka. Fitur terbaru yang telah disematkan pada versi Jelly Bean adalah *keyboard* yang bisa dikostumisasi oleh pnegguna dan dukungan gestur pada *keyboard*, *user interface* yang lebih *smooth*, dukungan tampilan nirkabel, *widget* yang bisa diatur dan disesuaikan ukurannya.

Setelah setahun perilisan Android 4.1 *Jelly Bean*, Android kembali meluncurkan versi pembaruan yaitu versi 4.4 yang telah diresmikan pada tanggal 31 Oktober 2013. Pada versi ini Android meningkatkan optimalisasi dengan memberikan fitur-fitur yang lebih baik. Dengan beberapa fitur yang dibawa Android 4.4 KitKat seperi

WebViews yang berbasiskan *Chromium,* pengoptimalan kinerja terhadap perangkat dengan spesifikasi rendah, dukungan sensor *batching* dan *step detector*.

- Android 5.0 *Lollipop*

  Versi Android selanjutnya adalah versi 5.0 *Lollipop* yang diperkenalkan oleh Android pada tanggal 25 Juni 2014. Pada versi ini Android bertujuan tidak hanya menjadikan Android sebagai sistem operasi pada perangkat *smartphone,* namun juga telah berjalan pada perangkat *mobile* lainnya seperti *Android TV* dan juga *Google Fit.* Beberapa fitur tersebut ditambahkan pada versi ini seperti *user interface* yang mengikuti desain *Google* yaitu *material design* dan fitur *factory reset protection* untuk menjaga *smartphone* agar tidak di reset apabila hilang.

- Android 6.0 *Marshmallow*

  Android 6.0 *Marshmallow* di perkenalkan pada tanggal 5 Mei 2015. Fitur yang dibawa oleh versi Android *Marshmallow* adalah dukungan sensor sidik jari untuk mengakses *smartphone*, fasilitas menjalankan beberapa aplikasi pada tata letak layar dengan dukungan *multi window,* dukungan *platform virtual reality,* dan kemampuan dalam mengurangi pemakaian *bandwidth* pada mode *data saver.*

- Android 7.0 *Nougat*

  Android 7.0 *Nougat* diluncurkan dan diperkenalkan pada tanggal 19 Oktober 2016. Sejak diluncurkan Android 7.0 Nougat berfokus pada peningkatan performa *user interface* sehingga lebih intuitif dan penggunaan aplikasi bisa secara bersamaan dan lebih *multi-tasking* dengan ditambahkanya fitur *multi window*. Selain peningkatan fitur tersebut, Android *Nougat* juga menambahkan beberapa fitur lain seperti dukungan cahaya malam atau *night mode, keyboard default* yang dapat mengirim animasi GIF secara langsung dan dukungan panggilan *multi-endpoint.*

- Android 8.0 *Oreo*

  Android 8.0 *Oreo* diluncurkan pada bulan Agustus 2017. Nama oreo dipilih sendiri secara langsung oleh Android untuk digunakan pada versi Android 8.0 sejak perilisannya. *User interface* yang dikembangkan pada Android *Oreo* lebih simpel agar memudahkan dalam mengakses aplikasi. Pembaruan yang dibawa oleh Android 8.0 *Oreo* ini yaitu, beberapa fitur seperti fitur *Autofill* yang memberikan kemudahan dalam mengisi formulir, dengan dukungan gambar dalam gambar dan pengoptimalan *booting* agar lebih cepat.

- Android 9.0 *Pie*

Android 9.0 *Pie* merupakan versi Android terbaru dengan dirilis pada bulan Agustus 2018. Fitur unggulan yang dipamerkan oleh Android 9.0 *Pie* ini adalah kemampuan AI atau kecerdasan buatan. Fitur AI *smartphone* akan mudah menganalisa dan mempelajari pola pemakaian sesuai penggunanya menggunakan *smartphone* secara otomatis. Selain itu fitur lainya yang diusung yaitu, *Adaptive Brightness* yang akan menyesuaikan kecerahan layar secara otomatis dan dukungan pada ponsel *bezel less.*

- Android 10

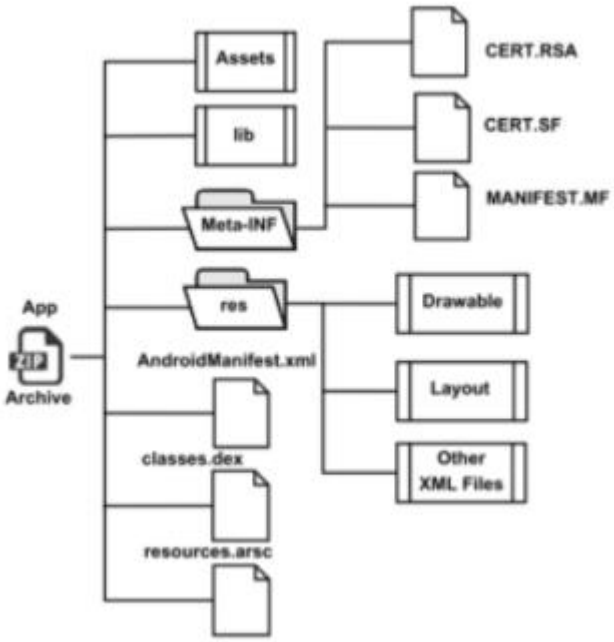
  Versi Android ini merupakan versi Android terbaru. Versi Android 10 lebih berfokus pada penyempurnaan *dark mode* dan *light mode* serta peningkatan fitur *sound amplifier* untuk mengatur kualitas audio. Kemudian versi ini ditambahkan fitur *smart reply* untuk pengguna agar tinggal mengklik pada sebuah notifikasi pesan masuk dan dapat meresponnya tanpa harus membuka aplikasi lain. Selanjutnya, Android 10 memperbaharui navigasi gestur sehingga perpindahan dari satu aplikasi ke aplikasi lainnya menjadi lebih mudah dan interaktif.

2.2.4 *Backdoor*

Backdoor adalah suatu teknik *hacker* atau peretas yang dapat memungkinkan mereka peretas mengakses ke suatu sistem tanpa melalui autentifikasi normal (*login*) terlebih dahulu dan tidak terdeteksi oleh sistem (Adenansi & Novarina, 2017). Dengan melewati prosedur-prosedur keamanan, *backdoor* juga digunakan untuk memfasilitasi pemasangan aplikasi dengan sistem berbahaya yang telah ditanam. *Backdoor* umumnya menggunakan jenis eksploitasi tingkat root untuk mendapatkan hak superuser (*root*), sehingga *backdoor* dapat menyembunyikan dirinya dari sebuah aplikasi keamanan lain, bahkan *backdoor* dapat memperburuk lagi dengan cara menonaktifkannya juga. Jumlah eksploitasi *backdoor* berada pada level *root* dan telah dimanfaatkan seperi *rage against the cage* dan *gingerbreak* untuk mendapatkan kendali penuh atas perangkat. *Basebridge, KMin, Obad* adalah contoh aplikasi *backdoor* terkenal (Faruki et al., 2015).

Backdoor dapat dikemas menggunakan aplikasi Android dengan ekstension file .apk, secara teknis bisa merupakan arsip zip, yang terdiri dari beberapa file dan folder seperti yang ditunjukkan pada Gambar 2.1 secara khusus, file AndroidManifest.xml berisi meta-data tentang aplikasi, seperti nama paket, izin yang diperlukan, definisi satu atau lebih komponen seperti aktivitas, layanan, penerima siaran atau penyedia konten, versi *platform* minimum dan

maksimum yang didukung, pustaka yang akan ditautkan, dan sebagainya. Folder res terdiri dari ikon, gambar, *string*, numerik, konstanta warna, *layout* UI, menu, animasi, dll, yang disusun ke dalam format biner. Folder assets berisi sumber daya yang tidak dikompilasi dan struktur direktori dipertahankan. Class.dex berisi *byte code* Dalvik yang dapat dieksekusi untuk dijalankan di bawah "Mesin Virtual Dalvik". Folder META-INF berisi tanda tangan digital aplikasi, serta sertifikat pengembang yang masing-masing digunakan untuk verifikasi dan identifikasi (Faruki et al., 2015).



Gambar 2.1 Apk Struktur

Android telah dirancang dengan mempertimbangkan keamanan sejak awal dengan tujuan untuk melindungi data pengguna, aplikasi, perangkat, dan jaringan. Namun, keamanan keseluruhan bergantung pada kemauan dan kemampuan pengembang untuk menerapkan praktik terbaik. Selain itu, pengguna harus menyadari pengaruh beberapa aplikasi setelah penginstalan, pada data dan keamanan perangkatnya. Solusi *anti-malware* di Android tidak dapat menangani *malware* secara agresif karena model keamanan yang diterapkan pada aplikasi. Misalnya, aplikasi *anti malware* memiliki kemampuan pemindaian atau pemantauan terbatas untuk aplikasi atau sistem file lain di perangkat. Pada bagian ini, kami merevisi fitur keamanan yang disediakan oleh *platform* Android.

2.2.5 *Android Permissions*

Inti dari sebuah model keamanan Android adalah sistem berbasis hak perizinan atau *permission* yang secara *default* dapat menolak akses ke fitur atau fungsionalitas yang dapat menimbulkan dampak negatif pada pengalaman pengguna, sistem atau aplikasi lain ketika di-*install* pada sebuah perangkat. Untuk memanfaatkan fungsionalitas terbatas yang berpotensi terjadinya bahaya jika digunakan dengan menggabungkan fitur lain, atau dengan cara yang berbeda dari yang dimaksud oleh perancang OS Android, Android mengharuskan pengembang aplikasi untuk bisa menanyakan kepada pengguna untuk bisa menggunakan fitur terbatas dari hak akses perizinan atau *permission* yang dapat digunakan.

Kesalahan dalam menggunakan hak akses perizinan dapat mengakibatkan sebuah panggilan terhadap sistem yang terkait dengan fitur terbatas yang diberi hak akses perizinan, karena fungsionalitas tersebut diidentifikasi membutuhkan izin eksplisit agar Android dapat memberikan hak akses perizinan atau *permission* (Saragih, 2013). Karena kesalahan tersebut dapat mengontrol akses ke fungsi jaringan dan GPS, informasi pribadi, perangkat keras dan beberapa pengaturan sistem, dan banyak fitur perangkat lainnya. Namun, Android dirancang sedemikian rupa agar aplikasi pihak ketiga dapat menentukan fungsionalitas baru (misalnya melalui API) dan membuat fungsionalitas yang spesifik dan tersedia untuk aplikasi lain berdasarkan hak akses perizinan yang telah ditentukan pengembang (Barrera et al., 2010).

2.2.6 *Analytical Hierarchy Process*

Analytical Hierachy Process merupakan suatu model dalam pendukung keputusan yang ditelah dikembangkan oleh Thomas L. Saaty. Model pendukung keputusan ini dapat menguraikan sebuah masalah kompleks seperti multi kriteria atau multi faktor yang telah menjadi suatu hierarki, menurut Saaty, hierarki didefinisikan sebagai representasi dari sebuah permasalahan kompleks disetiap struktur multi level dimana level pertama adalah tujuan, yang telah diikuti level faktor, kriteria, sub kriteria, dan seterusnya ke bawah hingga level terakhir dari alternatif. Suatu masalah yang kompleks dapat diuraikan secara langsung dengan hierarki, dan diatur sesuai ke dalam kelompok-kelompoknya yang kemudian dapat diatur menjadi suatu bentuk hirarki sehingga suatu permasalahan bisa tampak lebih terstruktur dan sistematis. *Analytical Hierarchy Process* (AHP) sering digunakan sebagai metode pemecahan suatu masalah dibanding dengan metode yang lain karena beberapa alasan sebagai berikut:

- Struktur yang berhierarki, sebagai konsekuensi dari kriteria yang dipilih, sampai pada sub kriteria yang paling dalam.

- Dapat memperhitungan validitas sampai dengan batas toleransi inkonsistensi berbagai kriteria dan alternatif yang dipilih oleh pengambilan keputusan.

2.2.7 *Multiple Regression Linear*

Teknik analisis data *Multiple Linear Regression* adalah alat perhitungan statistik atau metode untuk perhitungan statistik yang digunakan untuk mengetahui seberapa besar pengaruh antara satu atau beberapa variabel terhadap satu buah variabel. Terdapat dua jenis variable pada metode ini, yakni varabel bebas (*independent*) dan variabel terikat (*dependent*). Variabel bebas merupakan variabel yang memengaruhi, sedangkan variabel terikat merupakan variabel yang dipengaruhi (Aptaguna & Pitaloka, 2016).

Menurut Sugiyono (2006) dalam Yulianti (2010) analisis regresi ganda digunakan untuk meramalkan bagaimana kondisi dari keadaan (naik turun) variabel dependen, jika dua atau lebih variabel independen sebagai faktor prediktor dimanipulasi (dinaikturunkan nilainya). Model analisis ini dipilih karena sebagian penelitian dirancang untuk meneliti variabel bebas yang berpengaruh atau signifikan terhadap variabel tidak bebas (Manufaktur, 2013). Metode analisis regresi berganda ini memiliki rumus sebagai berikut:

$$Y_i = \beta_0 + \beta_1 X_{1i} + \beta_2 X_{2i} + \ldots + \beta_k X_{ki} + \varepsilon_i$$

Gambar 2.2 Model untuk Regresi Linear Berganda
Sumber (Harlan, 2018)

β , 1 β , 2 β , . . . , k β adalah nilai-nilai parameter yang akan diestimasi dengan perintah Stata tersebut. Sebagai keluaran akan diperoleh hasil estimasi persamaan garis regresi linear ganda

$$\hat{Y}_i = b_0 + b_1 X_{1i} + b_2 X_{2i} + \ldots + b_k X_{ki} \quad ; \quad i = 1, 2, \ldots, n$$

Gambar 2.3 Model Keluaran Estimasi Persamaan Regresi Linear Ganda
Sumber (Harlan, 2018)

2.2.8 Bahasa R dan IDE Rstudio

Bahasa R merupakan sebuah bahasa pemrograman statistika yang dapat digunakan untuk menganalissi dan memanipulasi data statistika seperti pemodelan statistika, dan grafik (Gio & Effendie, 2018). Bahasa R diciptakan oleh Ross Ihaka dan Robert Gentleman dari departemen statistika, di Universitas Auckland, New Zealand (Gio & Effendie, 2018). Untuk membantu pemrograman menggunakan bahasa R dapat dibantu melalui fasilitas atau *package* yang disediakan Rstudio. Rstudio adalah *Integrated Development Environment* (IDE) yang tersedia dari server CRAN (*Comprehensive R Archive Network*) untuk memudahkan analisis dan manipulasi data serta grafik dari data yang akan diolah. Rstudio telah menyediakan hampir semua fitur yang diinginkan untuk sebuah IDE dengan cara yang baru, membuatnya lebih mudah dan lebih produktif untuk menggunakan Bahasa R (Gio & Effendie, 2018). RStudio menyediakan banyak kenyamanan dan kemudahan dalam menggunakannya untuk mengatur *packages, workspaces, files*, dan lainnya. Rstudio merupakan *open source project* dengan pengembangan alat yang luar biasa supaya dapat membantu praktik dan teknik yang dibutuhkan dalam menciptakan analisis yang berkualitas (Gio & Effendie, 2018).

2.2.9 *Diffusion of Innovation*

Perkembangan studi difusi telah muncur dari berbagai bentuk konseptual dan penelitian selama lima puluh tahun terakhir. Rogers (2003) mengindentifikasi sembilan tradisi dari penelitian difusi utama, telah memperkirakan bahwa empat di antaranya mencakup hampir 2 pertiga dari semua publikasi difusi: sosiologi pedesaan, pemasaran dan manajemen, komunikasi, dan kesehatan masyarakat.

Rogers (1995, 2003) telah menggambar sebuah proses adopsi sebuah inovasi oleh setiap individu sebagai distribusi normal berbentuk lonceng, dengan lima kategori *adopter*: *innovators*, *early adopters*, *early majority*, *late majority*, dan *laggards.* Rogers (1995, 2003) mencirikan pengadopsi pada setiap mayoritas awal dan akhir sebagai dalam satu standar deviasi di kedua sisi mean atau titik tengah sebuah kurva, *adopter* dan *laggards* sebagai dua deviasi standar, dan *inovator* sebagai tiga standar deviasi di sisi positif dari mean. Roger (1995, 2003) mengusulkan kaitannya bahwa dengan mengindenftifikasi kategori dari setiap pengadopsi dapat memberikan dasar yang kuat untuk merancang dan menerapkan strategi intervensi yang telah ditujukan pada sebuah kelompok individu tertentu (Glanz et al., 2002).

Seperti pada awalnya yang telah diusulkan, kategori adopter ini akan digunakan untuk tujuan deskriptif dan perencanaan. Namun, ada kecenderungan untuk menggunakan kategori ini sebagai variabel penjelas atau prediktor, meskipun masi sedikit empiris untuk pendekatan ini (Glanz et al., 2002). Proses pengambilan keputusan pada calon pengadopsi akan dipengaruhi oleh banyak faktor lain dalam konteks, yang terdiri antara lingkungan atau sistem di mana proses tersebut berlangsung, beberapa di antaranya telah didukung oleh beberapa bukti empiris.

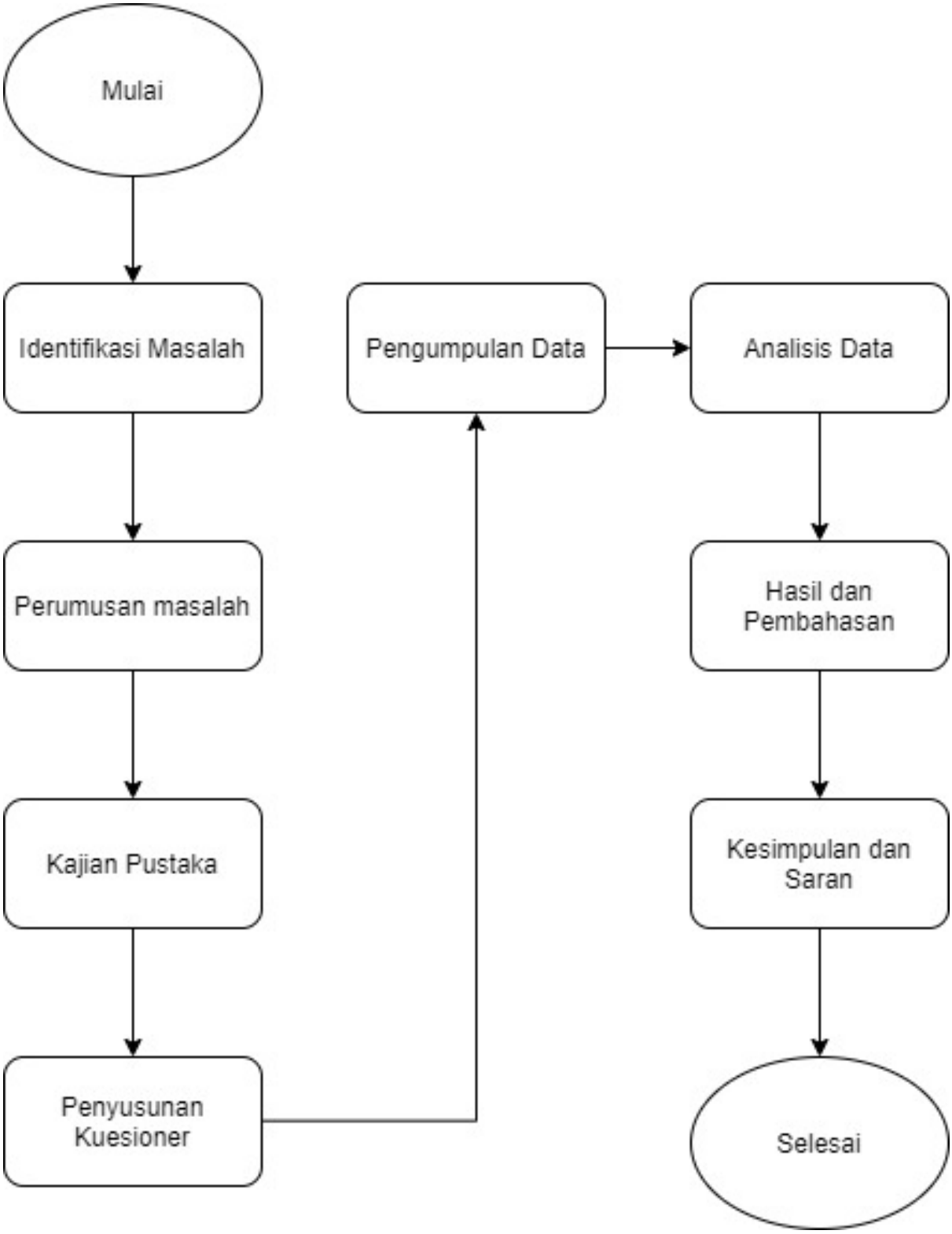
BAB III
METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Penelitian ini dilakukan dengan menggunakan jenis penelitian desktriptif dengan metode pendekatan kuantitatif. Menurut Sugiyono (2015), sebuah penelitian deskriptif adalah penelitian yang dilakukan untuk mengetahui garis besar hubungan antar dua variabel atau lebih. Pada penelitian deskriptif ini digunakan untuk menjelaskan tentang kesadaran keamanan pada pengguna *smartphone* Android dan demografi terhadap kesadaran keamanan di kalangan pengguna *smartphone* Android dari serangan berbasis *backdoor* di Indonesia.

Pendekatan metode kuantitatif ini digunakan untuk mendapatkan informasi dari populasi atau sampel tertentu dengan melakukan analisis data menggunakan alat statistik dan instrumen penelitian sebagai alat pengumpulan data, dengan tujuan agar untuk dapat melakukan pengujian terhadap hipotesis yang telah ditentukan (Sugiyono, 2015). Data yang digunakan merupakan kumpulan hasil dari responden yang menjawab melalui kuesioner yang disebar di beberapa *platform* sosial media seperti *WhatsApp, Telegram, Instagram, Twitter, Line* dan *Facebook*. Kemudian dilanjutkan kepada proses analisis statitstik dari data yang telah dikumpulkan untuk mendapatkan hasil skor kesadaran keamanan pengguna *smartphone* yang ada di Indonesia.

Dalam penelitian ini, ada beberapa tahapan yang dilakukan mulai dari identifikasi masalah, perumusan masalah, kajian pustaka, penyusunan kuesioner, pengumpulan data, analisis data, hasil dan pembahasan, dan yang terakhir kesimpulan dan saran. Lalu adapun sampel yang digunakan merupakan bagian kecil dari populasi penelitian yang dilakukan dikarenakan populasi yang begitu luas yang mencakup seluruh Indonesia. Alur penelitian yang dilakukan dapat dilihat pada Gambar 3.1.



Gambar 3.1 Diagram Alur Penelitian

3.2 Pengumpulan Data

Untuk melakukan sebuah penelitian, perlu dilakukan terlebih dahulu sebuah analisis dari berbagai aspek-aspek seperti pengumpulan data. Di dalam pengumpulan data tersebut terbagi menjadi beberapa bagian penting yaitu cara pengumpulan data, waktu pengumpulan data, populasi, dan sampel. Kemudian, teknik *sampling* yang digunakan untuk pengumpulan data penelitian ini merupakan sebuah gabungan dari teknik *purposive sampling* dan *snowball sampling.*

Teknik *purposive sampling* juga disebut *judgement sampling*, adalah pilihan yang disengaja dari partisipan karena kualitas yang dimiliki partisipan (Etikan, 2016). Teknik *purposive sampling* bisa diartikan pula sebagai teknik pengambilan data sesuai dengan kriteria dan kebutuhan pada suatu penelitian. Pada penelitian ini, karena tujuannya adalah mencari nilai kesadaran keamanan pengguna *smartphone* Android di Indonesia, maka pengumpulan datanya pun disesuaikan dengan kriteria responden yang dibutuhkan yaitu kalangan pengguna *smartphone* Android di Indonesia.

Snowball sampling atau *chain referral sampling* dari populasi yang tersembunyi dimulai dengan *convenience sample* dari subjek awal. Jika sampel acak dapat diambil, populasi tidak akan dibatasi sebagai tersembunyi. Subjek awal ini berfungsi sebagai "benih" di mana subjek gelombang 1 direkrut, kemudian subjek gelombang 1 secara bergantian merekrut subjek gelombang 2 dan sampel sebagai konsekuensinya mengembang gelombang demi gelombang seperti bola salju yang membesar saat berguling menuruni bukit (Douglas D. Heckathorn, 2010). Salah satu bentuk pengambilan sampel non-probabilitas yang paling terkenal adalah metode *snowball sampling*, yang sangat cocok jika populasi yang dibutuhkan sulit dijangkau dan sulit untuk disusun daftar populasinya oleh peneliti (Etikan, 2016). Teknik *snowball sampling* bisa didefinisikan sebagai sebuah teknik pengambilan sampel data yang bersifat berantai, misal kuesioner disebar ke orang A kemudian dari orang A disebar lagi ke orang B dan C lalu disebar lagi ke orang D, E, F, dan seterusnya.

3.2.1 Cara Pengumpulan Data

Sumber data yang digunakan pada penelitian ini menggunakan data primer yang telah diperoleh secara langsung oleh peneliti dengan cara menyebarkan kuesioner. Kuesioner merupakan teknik pengumpulan yakni untuk memberikan daftar pertanyaan atau pernyataan kepada setiap responden yang mengisi kuesioner untuk dijawabnya secara langsung (Sugiyono, 2015). Kuesioner dirancang agar bisa menjawab kesadaran keamanan pada pengguna

smartphone Android dari serangan *backdoor* dengan tipe atau pernyataan positif, sehingga responden tinggal memilih jawaban yang telah diberikan. Data yang telah dikumpukan untuk penelitian ini akan dianalisis dengan analisis kuantitatif.

Dalam penelitian ini, pertanyaan pada kuesioner dirancang dan dibedakan ke tiga dimensi yang berbeda, Menurut Kruger dan Kearney, dengan melalui teori psikologi sosial akan dibagi menjadi tiga komponen untuk mengukur objek yaitu, *cognition, affection,* dan *behavior (*sitasi kruger). Komponen tersebut digunakan untuk mengembangkan tiga dimensi tersebut. yaitu dimensi *knowledge* (pengetahuan seseorang), dimensi *attitude* (sikap seseorang), dan dimensi *behavior* (perilaku seseorang). Untuk pilihan jawaban yang diajukan menggunakan skala guttman dengan model *cross sectional*. Menurut Sugiyono (2015) skala guttman digunakan untuk mengukur pendekatan kuantitatif dengan menggunakan beberapa sebutan atau istilah, seperti mendekati kesesuaian dalam bentuk angka, persentase. Berikut skala guttman yang digunakan pada penelitian ini:

Tabel 3.1 Skala Guttman berdasarkan Hasil Kuesioner

No	Keterangan	Skor
1	Benar	10
2	Salah	0
3	Tidak Tahu	5

3.2.2 Waktu Pengumpulan Data

Dalam pengumpulan data ini memiliki dua metode pendekatan yaitu *Longitudinal* dan *Cross Section.* Pendekatan *Longitudinal* atau (pendekatan bujur) adalah penelitian yang meneliti perkembangan sesuatu aspek pada suatu hal dalam seluruh periode waktu, atau sebuah tahapan perkembangan yang cukup panjang (เพ็ชราภรณ์, 2557). Sedangkan pendekatan *Cross Section* adalah pendekatan penelitiaan dalam satu tahapan atau satu periode waktu, hanya meneliti perkembangan dalam sebuah tahapan tertentu saja (เพ็ชราภรณ์, 2557). Berdasarkan waktu pengumpulan, data ini akan termasuk ke dalam *Cross Section/Insidental* yaitu data akan dikumpulkan dalam suatu rentang waktu tertentu. Dalam penelitian ini waktu yang diperlukan untuk mengumpulkan data dari responden adalah 14 hari kalender, dimulai dari tanggal 25 September 2020 sampai 7 Oktober 2020.

3.2.3 Populasi

Menurut Sugiyono (2015) populasi adalah objek atau subjek pada wilayah secara umum yang memiliki kualitas dan karakteristik tertentu yang akan dipelajari oleh peneliti untuk menarik kesimpulan. Pada penelitian ini populasinya adalah pengguna *smartphone* Android di Indonesia (Sugiyono, 2015).

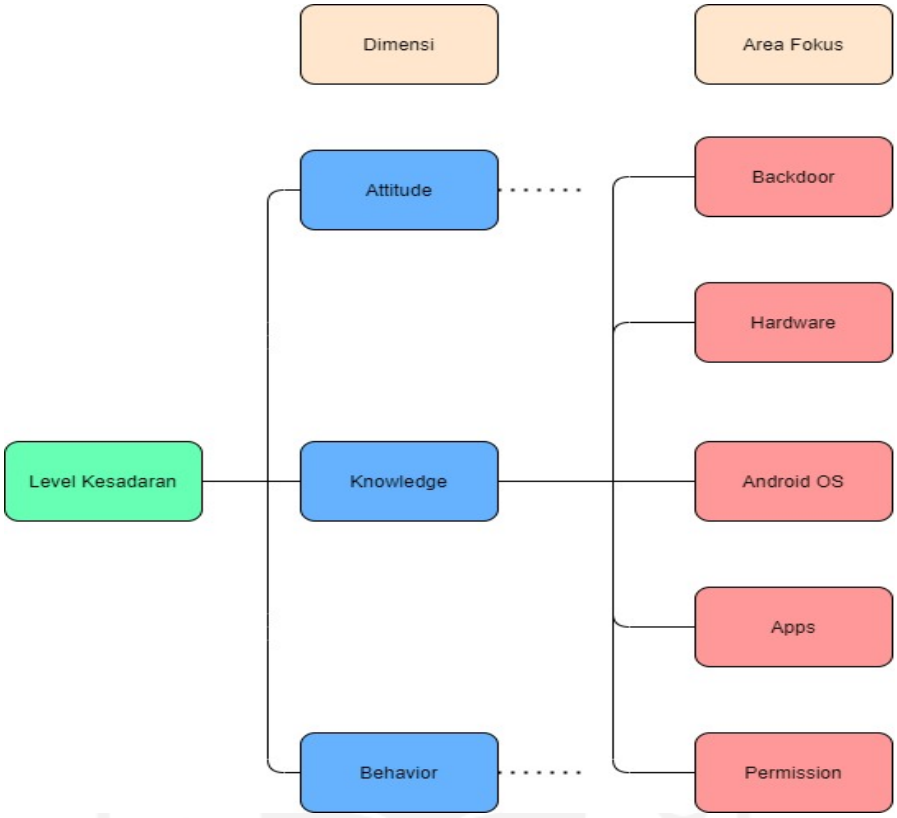
3.2.4 Sampel

Sampel adalah bagian dari jumlah dan karakteristik yang dimiliki oleh suatu populasi (Sugiyono, 2015). Jika jumlah populasi besar dan tidak memungkinkan untuk mempelajari semua anggota populasi, baik karena keterbatasan dana, waktu, atau tenaga, maka penelitian dapat menggunakan sampel yang telah diambil dari populasi itu. Apapun yang telah dipelajari dari sampel tersebut kesimpulannya dapat diaplikasikan pada populasi tersebut. Karena sampel yang dipakai untuk penelitian harus representatif.

Sampel yang digunakan dalam pengumpulan data penelitian ini yaitu masyarakat atau kalangan pengguna *smartphone* yang mengisi kuesioner via *Google Forms* yang disebarkan di beberapa *platform* media sosial seperti *WhatsApp, Telegram, Instagram, Twitter, Line, dan Facebook.*

3.3 Hasil Uji Instrumen Penelitian

Data kuesioner yang dimiliki peneliti terlebih dahulu dilakukan pengujian untuk melihat seberapa akurat dan ketepatan dari data penelitian yang dimiliki sebelum melakukan suatu analisis. Dalam penelitian ini instrumen yang digunakan itu melalui kuesioner yang telah dijawab secara langsung oleh responden berupa *Google Forms* yang telah disebar. Dalam kuesioner tersebut terdapat pertanyaan yang telah disusun sedemikan rupa yang akan dijawab oleh responden sesuai dengan apa yang mereka ketahui atau lakukan. Pertanyaan tersebut dibuat berdasarkan Model Kruger dan Kearney dengan variabel yang diteliti yaitu *knowledge, attitude,* dan *behavior*. Pengukuran kesadaran keamanan yang dikembangkan dengan mengikuti model Kruger dan Kearney berlandaskan teori psikologi sosial yang membagi tiga komponen untuk mengukur objek yaitu *Cognition, Affection,* dan *Behavior* (Kruger & Kearney, 2006).



Gambar 3.2 Kerangka Pengukuran Kesadaran Keamanan Informasi

Gambar 3.2 di atas, merupakan kerangka untuk melakukan pengukuran kesadaran keamanan pada kalangan pengguna *smartphone* Android di Indonesia berdasarkan Model Kruger dan Kearney dengan variabel yang diteliti yaitu *knowledge, attitude,* dan *behavior*. Pada setiap dimensi akan terdapat lima area fokus yang sama yaitu, *backdoor*, *hardware, Android OS, apps,* dan *permission*. Ada beberapa *point* penting yang harus diingat ketika menggunakan *smartphone* Android yaitu jangan meng-*install* sebuah aplikasi secara sembarangan, hindari mengunduh sebuah aplikasi yang bukan repositori resmi milik aplikasi, menjaga *smartphone* Android dari penggunaan orang lain, karena kesadaran keamanan paling riskan terletak kepada manusia itu sendiri, selalu memperhatikan hak perizinan atas sebuah aplikasi disaat ketika meng-*install* sesuai kebutuhan pribadi pengguna. Dari poin penting tersebut dan hasil perumusan pertanyaan yang dibuat untuk kuesioner yang dikelompokkan bersama dosen pembimbing didapatkan ke lima area fokus tersebut.

Contoh pertanyaan untuk uji *knowledge*
Smartphone berbasis Android berpotensi mendapatkan serangan berbasis *backdoor* yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna.
1. Benar 2. Salah 3. Tidak Tahu

Contoh pertanyaan untuk uji *attitude*
Saya sadar bahwa *smartphone* berbasis Android berpotensi mendapatkan serangan berbasis *backdoor* yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna.
1. Benar 2. Salah 3. Tidak Tahu

Contoh pertanyaan untuk uji *behaviour*
Saya terbiasa untuk melakukan langkah-langkah pencegahan atas serangan berbasis *backdoor* di *smartphone* Android saya.
1. Benar 2. Salah

Gambar 3.3 Contoh Pertanyaan Kuesioner

Berdasarkan model Kruger dan Kearney, dibuatlah contoh pertanyaan untuk penelitian ini yang disesuaikan dengan model tersebut dan topik dari penelitian ini yaitu *smartphone* Android. Pada dimensi *knowledge* dan *attitude,* diberikan tiga buah opsi jawaban yaitu benar, salah, dan tidak tahu. Sedangkan pada dimensi *behavior* berkaitan dengan kebiasaan pengguna sehari-hari yang jika dipikirkan setiap pengguna seharusnya tahu dengan apa saja kebiasaan yang sering mereka lakukan ketika menggunakan *smartphone* Android baik itu ketika memasang sebuah aplikasi, mengunduh langsung dari repositori, dan mengetahui bahwa *smartphone* yang digunakan telah lulus "*Build Test Suite*" dan mempunyai sertifikasi OEM (*Original Equipment Manufacture*), dan lain sebagainya.

3.4 Analisis Data

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* (Kruger & Kearney, 2006). Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *knowledge* (pengetahuan seseorang), *attitude* (sikap seseorang), dan *behavior* (perilaku seseorang) (Akraman et al., 2018). Dari 36 pertanyaan tersebut dibagi menjadi masing-masing 12 pertanyaan setiap dimensinya, dimulai dari *knowledge*, *attitude*, dan *behavior*. 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 3.2.

Tabel 3.2 Daftar 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. 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.	• Benar • Salah

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. Peneliaian berdasarkan skala ordinal yang merupakan skala pengukuran yang menyatakan peringkat antar tingkatan di mana jarak atau interval antar tingkatan juga tidak harus sama (Janna, 2020). 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) (Sari & Candiwan, 2014). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi secara subjektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen (Akraman et al., 2018). 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 3.3 dan Tabel 3.4

Tabel 3.3 Pembagian Bobot Dimensi

Dimensi	**Bobot**
Knowledge	30%
Attitude	20%
Behaviour	50%

Sumber: Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers and Security, 25(4), 289–296.

Tabel 3.4 Pembagian Pertanyaan untuk Tiap 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 3.4 yang merupakan hasil penyesuaian dari model Kruger dan Kearney khusus untuk penelitian ini. Setelah pembersihan data, maka dilakukan perhitungan tingkat kesadaran keamanan dari data yang telah dikumpulkan sebelumnya. Perhitungan dibagi menjadi 5 tahap yaitu penjumlahan nilai pertanyaan yang dijawab responden untuk masing-masing area fokus pada setiap dimensi, perhitungan nilai kesadaran untuk masing-masing area fokus pada setiap dimensi, perhitungan nilai total kesadaran fokus area, perhitungan nilai total kesadaran dimensi dan perhitungan nilai kesadaran secara keseluruhan. Tahap pertama yaitu penjumlahan nilai pertanyaan yang dijawab responden untuk masing-masing area fokus pada setiap dimensi melalui persamaan (3.1).

$$JN = J_1 + J_2 + J_3 + \ldots + J_n \tag{3.1}$$

Keterangan:

JN = jumlah nilai jawaban responden

$J =$ nilai jawaban responden

$n =$ pembagian pertanyaan untuk setiap area fokus

Lalu, tahap kedua yaitu perhitungan nilai kesadaran untuk masing-masing area fokus pada setiap dimensi melalui persamaan (3.2) dan (3.3). Perhitungan dilakukan pada setiap dimensi untuk memudahkan analisis data agar tidak terlalu banyak atau tertumpuk pada *sheets* yang sama.

$$\sum JN = \left(\frac{JN_1}{JP_i}/10\right) + \left(\frac{JN_2}{JP_i}/10\right) + \left(\frac{JN_3}{JP_i}/10\right) + \ldots + \left(\frac{JN_n}{JP_i}/10\right) \tag{3.2}$$

$$NA = \frac{\sum JN}{JR} x\ 100 \tag{3.3}$$

Keterangan:

$\sum$JN =jumlah nilai jawaban dari seluruh responden

NAF = nilai kesadaran area fokus pada masing-masing dimensi

JN_n = jumlah nilai jawaban responden ke-n

$JP_i =$ jumlah bobot pertanyaan area fokus ke-i

JR = jumlah responden

Selanjutnya, tahap ketiga yaitu perhitungan nilai total kesadaran untuk masing-masing fokus area melalui persamaan (3.4). Nilai total kesadaran berkisar antara 0% – 100%.

$$\sum NAF = (NAF_1 x0{,}3) + (NAF_2 x0{,}2) + (NAF_3 x0{,}5) \quad (3.4)$$

Keterangan:

$\sum NAF$ = total nilai kesadaran untuk masing-masing area fokus

NAF_1 = nilai kesadaran area fokus pada dimensi 1 (*Knowledge*)

NAF_2 = nilai kesadaran area fokus pada dimensi 2 (*Attitude*)

NAF_3 = nilai kesadaran area fokus pada dimensi 3 (*Behavior*)

Kemudian, tahap keempat yaitu perhitungan nilai total kesadaran untuk masing-masing dimensi melalui persamaan (3.5). Nilai total kesadaran berkisar antara 0% – 100%.

$$\sum NKD = (NKD_1 + NKD_2 + NKD_3 + NKD_4 + NKD_5)/5 \quad (3.5)$$

Keterangan:

$\sum NKD$: total nilai kesadaran untuk masing-masing dimensi

$NKD1$: nilai kesadaran area fokus 1 (*Backdoor*)

$NKD2$: nilai kesadaran area fokus 2 (*Hardware*)

$NKD3$: nilai kesadaran area fokus 3 (*Android OS*)

$NKD4$: nilai kesadaran area fokus 4 (*Apps*)

$NKD5$: nilai kesadaran area fokus 5 (*Permission*)

Terakhir, tahap ke lima yaitu perhitungan nilai kesadaran secara keseluruhan sebagai hasil akhir nilai kesadaran keamanan pengguna *smartphone* Android di Indonesia melalui persamaan (3.6), (3.7), dan (3.8). Nilai total kesadaran berkisar antara 0% – 100%.

$$RTNAF = (\sum NAF_1 + \sum NAF_2 + \sum NAF_3 + \sum NAF_4 + \sum NAF_5)/5 \quad (3.6)$$

$$RTNKD = (\sum NKD_1 x0{,}3) + (\sum NKD_2 x0{,}2) + (\sum NKD_3 x0{,}5) \quad (3.7)$$

$$\sum KS = \frac{RTNAF + RTNKD}{2} \quad (3.8)$$

Keterangan:

∑KS: nilai kesadaran keseluruhan

RTNAF: rata total nilai kesadaran untuk masing-masing area fokus

RTNKD: rata total nilai kesadaran untuk masing-masing dimensi

$\sum NAF1$: total nilai kesadaran area fokus 1 (*Backdoor*)

$\sum NAF2$: total nilai kesadaran area fokus 2 (*Hardware*)

$\sum NAF3$: total nilai kesadaran area fokus 3 (*Android OS*)

$\sum NAF4$: total nilai kesadaran area fokus 4 (*Apps*)

$\sum NAF4$: total nilai kesadaran area fokus 5 (*Permission*)

$\sum NKD1$: total nilai kesadaran area fokus pada dimensi 1 (*Knowledge*)

$\sum NKD2$: total nilai kesadaran area fokus pada dimensi 2 (*Attitude*)

$\sum NKD3$: total nilai kesadaran area fokus pada dimensi 3 (*Behavior*)

Dari hasil perhitungan tingkat kesadaran yang didapatkan, maka akan didapatkan nilai yang dapat merepresentasikan tingkat kesadaran pengguna *smartphone*, baik secara keseluruhan responden penelitan, individu, maupun kelompok individu yang akan dievaluasi sesuai kriteria yang tertera pada Tabel 3.5 yang merupakan hasil penyesuaian dari model Kruger dan Kearney khusus untuk penelitian ini.

Tabel 3.5 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

Sumber: Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers and Security, 25(4), 289–296.

Selanjutnya, untuk mengukur perbedaan tingkat kesadaran keamanan antar kelompok demografi yang berbeda sekaligus menginvestigasi pengaruh perbedaan faktor demografis tersebut, akan dilakukan analisis lanjutan berupa regresi linear berganda (*multiple linear regression*) menggunakan metode OLS (*ordinary least squares*) dengan nilai atau skor kesadaran keamanan sebagai *dependent variable* dan berbagai faktor demografi responden sebagai *independent variables*.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Karakteristik Responden

Tabel 4.1 di bawah ini berisikan informasi karakteristik dari keseluruhan responden yang telah mengisi dan telah melaui proses pembersihan data, dengan total responden 396 orang. Informasi tersebut akan disajikan dalam sebuah tabel dengan berbagai kategori sesuai informasi demografi.

Tabel 4.1 Tabel Karakteristik Operasional Variabel Demografi

	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	72,2%
Non Jawa	110	27,8%
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%

Sampel merupakan data pengisi kuesioner yang terdiri dari 396 responden pengguna *smartphone* Android di Indonesia, serta variabel demografi yang berjumlah tujuh, yaitu jenis kelamin, usia, asal daerah, pulau, pendidikan, penghasilan bulanan, dan adopsi teknologi informasi. Dapat dilihat dari tabel di atas, pada variabel jenis kelamin terlihat bahwa jumlah

sampel perempuan lebih sedikit daripada laki-laki yaitu sebanyak 187 responden dengan persentase 47,2% sedangkan laki-laki sebanyak 209 responden dengan persentase 52,8%. Dari segi usia responden, survei ini didominasi oleh responden dengan usia 20 sampai 24 tahun sebanyakan 297 responden yang mencapai 75% dari total responden. Hal ini dapat diperkirakan bahwa pengguna *smartphone* Android mayoritas rata-rata pada usia 20 sampai 24 adalah pelajar atau mahasiswa yang sedang menempuh pendidikan pada tahun 2020 yang biasanya identik dengan disebut kaum *millennial*, karena kaum *millennial* sering disebut sebagai kaum yang sangat cepat beradaptasi dengan teknologi baru yang bermunculan, sama halnya dengan teknologi *smartphone* berbasis Android (Khadijah, 2019).

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 (Badan Pusat Statistik, 2019). Dari segi pulau, mayoritas responden berasal dari Pulau Jawa dengan jumlah 286 orang atau telah mencapai sekitar 72,3%. Sedangkan 110 orang lainnya berasal dari berbagai macam pulau di luar Jawa seperti Sumatera, Kalimantan, Nusa Tenggara, Papua, dan lain sebagainya.

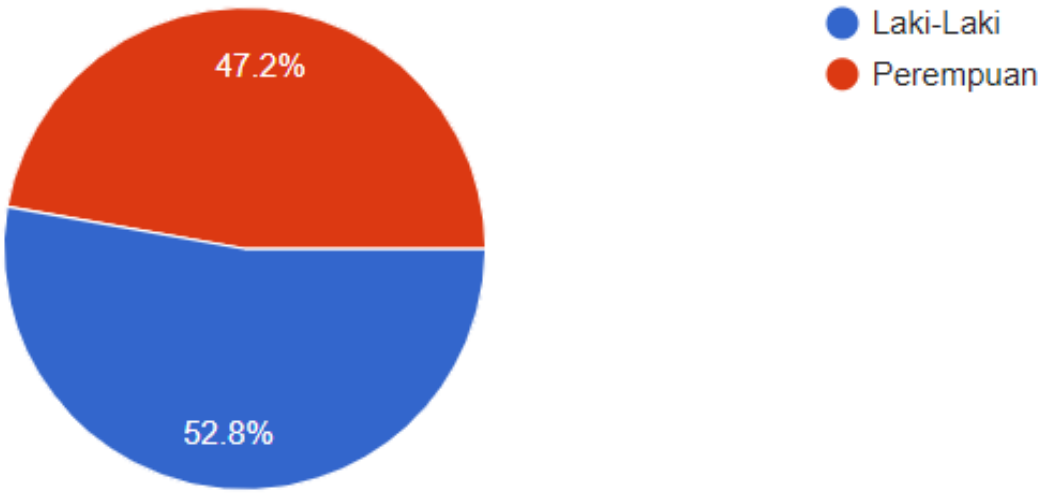
Dari segi pendidikan, 87,1% lebih didominasi oleh responden yang dengan pendidikan terakhir di jenjang pendidikan dasar sampai menengah akhir, atau bisa disebut pelajar yang belum lulus kuliah dibandingkan yang sudah menamatkan studi di perguruan tinggi. Hal ini berkaitan dengan usia sebelumnya yang mayoritas pengguna *smartphone* di Indonesia yaitu pada jenjang usia sekitar 20 sampai 24. Pada usia tersebut rata-rata pengguna sedang menempuh jenjang perkuliahan dan tamat perkuliahan. Dari segi penghasilan bulanan kurang dari Rp1.000.000,00 yang dikarenakan tingginya angka pelajar dan mahasiswa yang menjadi responden dalam penelitian ini.

Terakhir, dari segi adopsi teknologi informasi, 59,3% lebih didominasi oleh responden dengan tingkat "*Majority*" bahwa responden dominan mengikuti kebanyakan orang lain, menunggu beberapa saat sebelum memutuskan untuk menggunakan teknologi-teknologi terbaru. Lalu 22,7% diikuti dengan tingkatan "*Early Adopter*" dalam artian bahwa responden berusaha selalu mengikuti perkembangan terbaru dan seringkali termasuk yang pertama kali menggunakan teknologi yang diluncurkan di pasaran. Kemudian 17,9% diikuti dengan

tingkatan "*Laggard*" dalam artian bahwa responden tidak mengikuti perkembangan teknologi terbaru dan tidak menggunakannya sampai semua orang lain disekitarnya menggunakan.

4.1.1 Jenis Kelamin Responden

Berikut persentase jenis kelamin responden dapat dilihat pada gambar sebagai berikut:

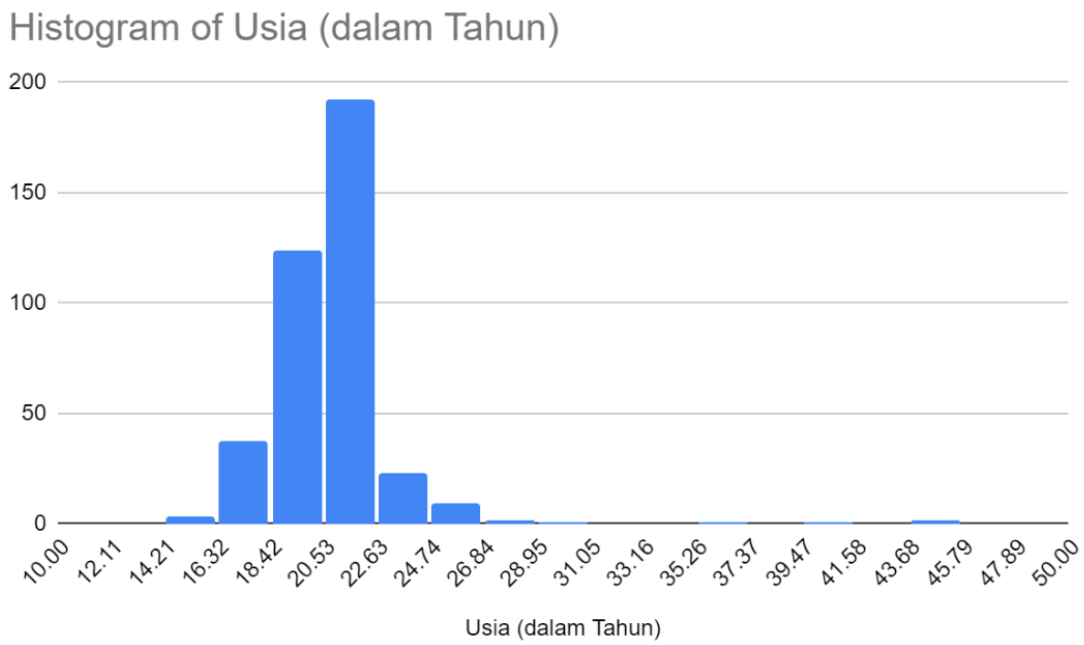


Gambar 4.1 Jumlah Responden Menurut Jenis Kelamin

Berdasarkan Gambar 4.1 menunjukan bahwa responden dalam penelitian ini dominan laki-laki dengan jumlah responden 209 orang atau memiliki persentase sebesar 52,8 persen, sedangkan responden perempuan dalam penelitian ini berjumlah 187 orang atau memiliki persentase sebesar 47,2 persen.

4.1.2 Usia Responden

Berikut persentase responden menurut usia dapat dilihat pada gambar sebagai berikut:

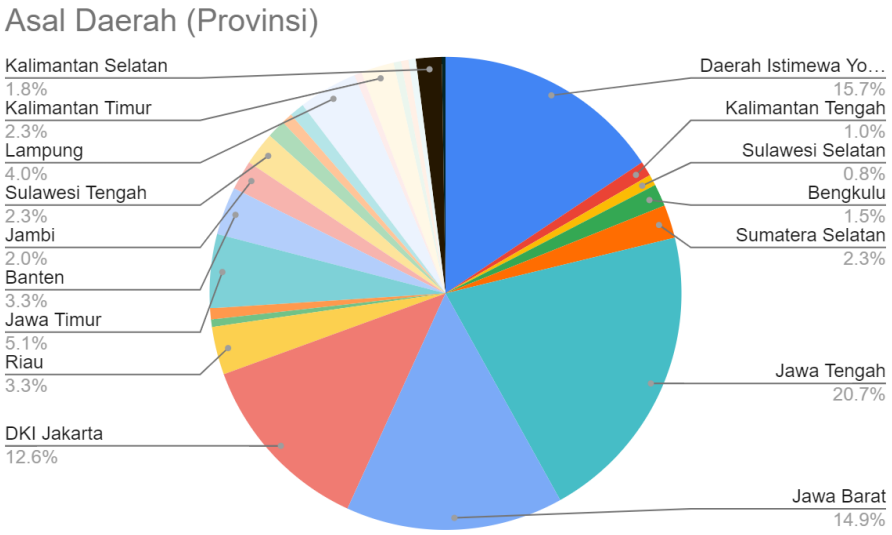


Gambar 4.2 Jumlah Responden menurut usia responden

Pada Gambar 4.2 dapat dilihat Sebagian besar usia responden dalam penelitian ini adalah 20-24 tahun dengan jumlah responden 297 orang atau memiliki persentase sebesar 75 persen, sedangkan responden di bawah 20 tahun berjumlah 83 orang atau memiliki persentase sebesar 20,9 persen, Sebagian kecil responden berusia 25 tahun hingga lebih berjumlah 16 orang atau memiliki persentase 4,04 persen.

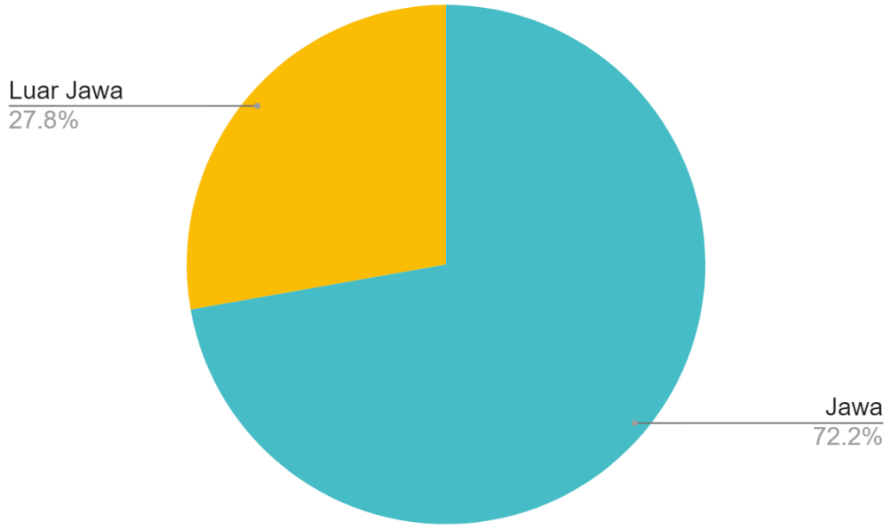
4.1.3 Asal Daerah Responden

Berikut persentase domisili dan daerah asal responden dapat dilihat pada gambar sebagai berikut:



Gambar 4.3 Jumlah Responden Menurut Asal Daerah Responden

Setelah melakukan penyebaran kuesioner berdasarkan Gambar 4.3 didapatkan total provinsi dari 396 responden yaitu 16 provinsi dengan mayoritas responden berdomisili Jawa Tengah, Daerah Istimewa Yogyakarta, Jawa Barat, dan DKI Jakarta dengan total mayoritas 63,9 persen. Karena keberagaman itu, peneliti melakukan kategorisasi menjadi Jawa dan luar Jawa (Sumatera, Kalimantan, Sulawesi, dan lainya). Berikut hasil kategorisasi domisili berdasarkan daerah asal dapat dilihat pada gambar berikut:

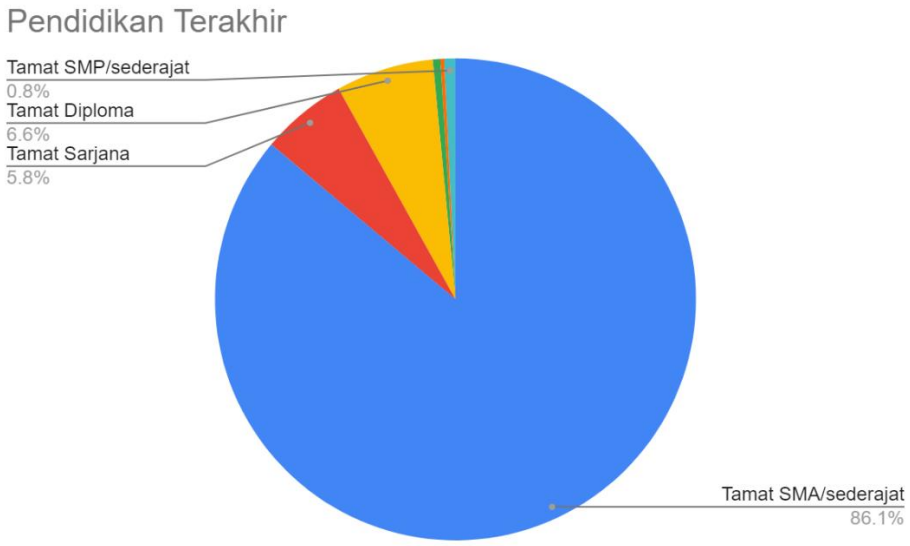


Gambar 4.4 Jumlah Responden Menurut Asal Domisili Responden

Berdasarkan Gambar 4.4 menunjukan bahwa Sebagian besar responden dalam penelitian ini adalah berdomisili di Jawa dengan jumlah responden 286 orang atau memiliki persentase sebesar 72,2 persen, selanjutnya responden dengan domisili luar Jawa berjumlah 110 orang atau 27,8 persen.

4.1.4 Pendidikan Responden

Berikut persentase pendidikan terakhir responden dapat dilihat pada gambar sebagai berikut:

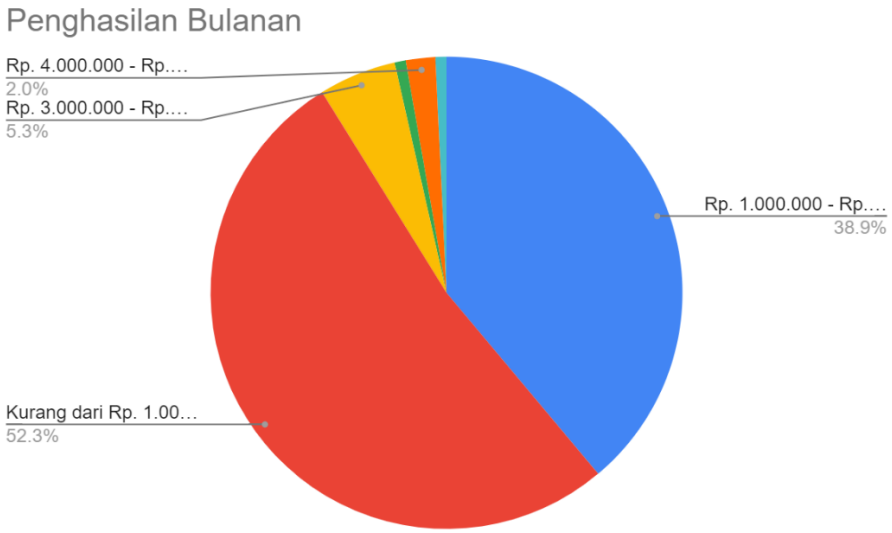


Gambar 4.5 Jumlah Responden Menurut Pendidikan Terakhir Responden

Pada Gambar 4.5 bisa dilihat dalam penelitian ini dominan pada jenjang Tamat SMA/sederajat dengan jumlah 341 orang atau memiliki persentase 86,1 persen. Sedangkan responden pada jenjang Tamat Kuliah dengan jumlah 51 orang atau memiliki persentase 12,9 persen, dan sebagian kecil baru saja Tamat SD/SMP sederajat dengan jumlah 4 orang atau memiliki persentase 1,1 persen.

4.1.5 Penghasilan Bulanan Responden

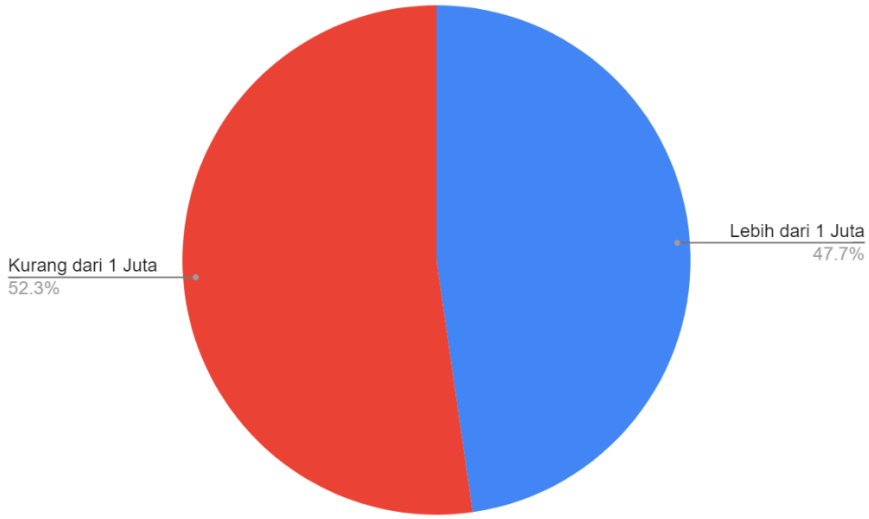
Berikut persentase penghasilan bulanan responden dapat dilihat pada gambar sebagai berikut:



Gambar 4.6 Jumlah Responden Menurut Penghasilan Bulanan Responden

Berdasarkan Gambar 4.6 menunjukkan bahwa sebagian besar penghasilan bulanan responden dalam penelitian ini adalah di bawah 1 juta dengan jumlah 207 orang atau memiliki persentase 52,3 persen, selanjutnya responden dengan penghasilan bulanan 1-2,9 juta dengan jumlah 154 orang atau memiliki persentase 38,9 persen. Selanjutnya responden dengan penghasilan 3-4,9 juta dengan jumlah 21 orang atau memiliki persentase 5,3 persen. Diikuti dengan responden penghasilan bulanan 4-9,9 juta dengan jumlah 8 orang atau memiliki persentase 2,0 persen. Kemudian sebagian kecil responden yang memiliki penghasilan bulanan di atas 10 juta dengan jumlah 6 orang atau memiliki persentase 1,6 persen.

Karena keberagaman itu, peneliti melakukan kategorisasi menjadi penghasilan di bawah 1 juta, dan penghasilan di atas 1 juta. Berikut hasil kategorisasi domisili berdasarkan kategorisasi pembagian penghasilan responden dapat dilihat pada gambar berikut:

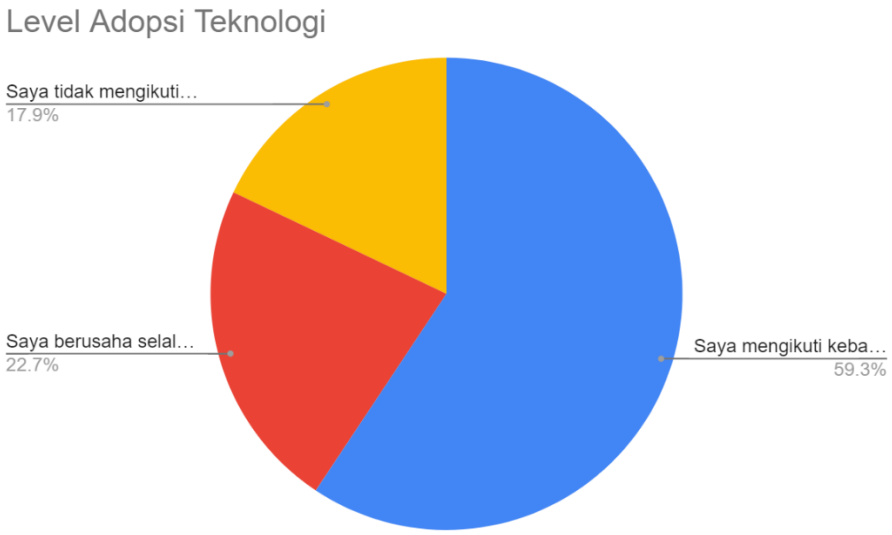


Gambar 4.7 Kategorisasi Penghasilan Bulanan Responden

Berdasarkan Gambar 4.7 menunjukan bahwa Sebagian besar responden dalam penelitian ini adalah berpenghasilan kurang dari 1 juta dengan jumlah responden 207 orang atau memiliki persentase sebesar 52,3 persen, selanjutnya responden dengan berpenghasilan lebih dari 1 juta berjumlah 189 orang atau 47,7 persen.

4.1.6 Adopsi Teknologi Informasi Responden

Berikut persentase pendapatan bulanan responden dapat dilihat pada gambar sebagai berikut:



Gambar 4.8 Jumlah Responden Menurut Level Adopsi Teknologi Informasi Responden

Berdasarkan Gambar 4.8 menunjukkan bahwa sebagian besar adopsi teknologi informasi responden dalam penelitian ini adalah "*Majority*" atau responden yang mengikuti kebanyakan orang lain, menunggu beberapa saat sebelummemutuskan untuk menggunakanteknologi-teknologi terbaru memiliki persentase sebesar 59,3 persen. Selanjutnya diikuti dengan responden "*Early Adopter*" atau responden yang berusaha selalu mengikuti perkembangan terbaru dan seringkali termasuk yang pertama kali menggunakan teknologi yang diluncurkan di pasaran dengan skor total persentase 22,7 persen. Terakhir diikuti dengan responden "*Laggard*" atau responden yang tidak mengikuti perkembangan teknologi terbaru dan tidak menggunakannya sampai semua orang lain di sekitarnya menggunakan, responden tersebut memiliki persentase sebesar 17,9 persen.

4.2 Analisis Skor Kesadaran Keamanan

Selanjutnya, dilakukan perhitungan skor kesadaran keamanan di kalangan pengguna *smartphone* Android di Indonesia yang hasilnya dapat dilihat pada Gambar 4.9 Skor kesadaran keamanan ini meliputi skor dari masing-masing dimensi dan area fokus yang kemudian menghasilkan skor akhir kesadaran keamanan secara keseluruhan.

		Awareness			
		Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
No	Focus Area				
1	**Backdoor**	80	84	68	**75**
2	**Hardware**	68	73	80	**75**
3	**Android OS**	82	84	77	**80**
4	**Apps**	87	87	80	**84**
5	**Permission**	91	91	86	**89**
6	**Total Awareness/Dimension**	**82**	**84**	**78**	**80**

Baik
Rata - Rata
Buruk

Gambar 4.9 Skor Total Keamanan Informasi Pengguna *Smartphone* Android

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 ke lima 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. Sedangkan 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 ratarata di rentang 68 pada dimensi *Knowledge*, 73 pada dimensi *Attitude*, 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*.

4.2.1 Skor Kesadaran Menurut Jenis Kelamin

Laki Laki

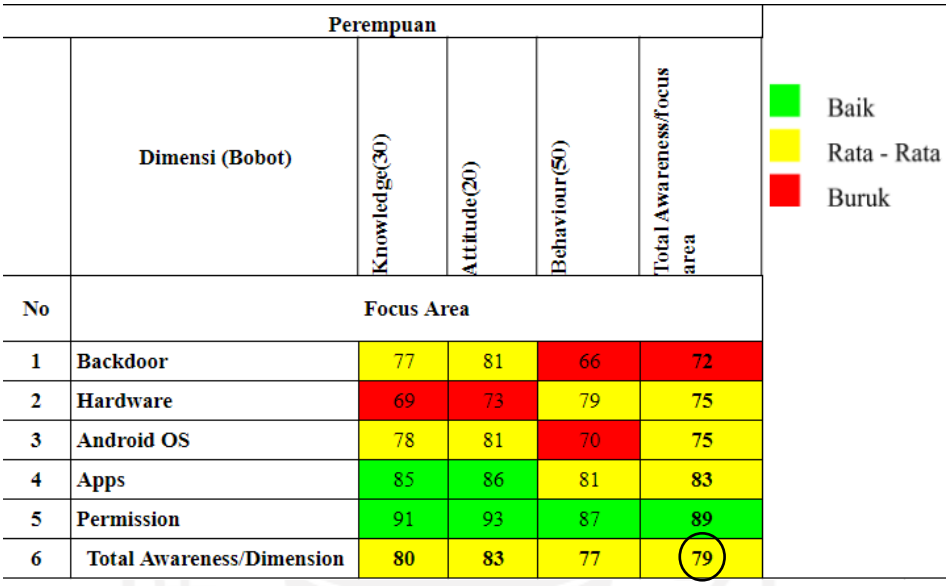
No	Dimensi (Bobot) / Focus Area	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
1	Backdoor	83	86	70	77
2	Hardware	67	73	81	75
3	Android OS	86	87	83	85
4	Apps	89	88	80	84
5	Permission	91	90	86	88
6	Total Awareness/Dimension	83	85	80	82

Baik
Rata - Rata
Buruk

Gambar 4.10 Skor Kesadaran Jenis Kelamin Laki-Laki

Pada Gambar 4.10 dari segi laki-laki, didapatkan skor 82 yang dalam penelitian ini masuk dalam kategori dengan 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 ke lima area fokus yang ada, area fokus *Android OS* dan *Permission* mendapatkan kategori

baik dengan nilai 85 dan 88. Dengan kata lain, kesadaran keamanan terkait isu *Android OS* dan *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti *Backdoor, Hardware,* dan *Apps* walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.



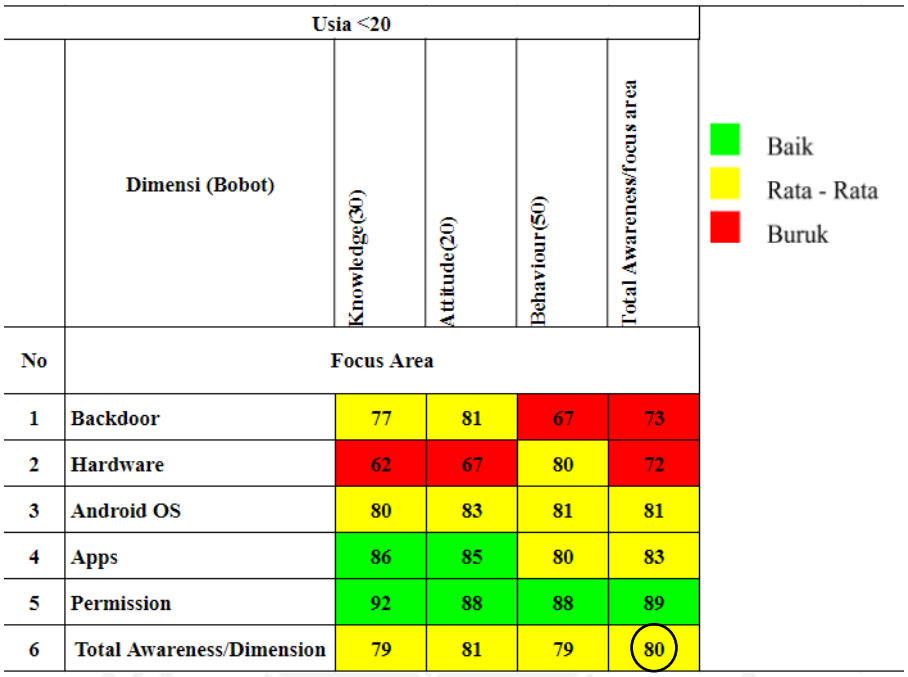
Perempuan						
	Dimensi (Bobot)	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/Focus area	Baik Rata - Rata Buruk
No	Focus Area					
1	Backdoor	77	81	66	72	
2	Hardware	69	73	79	75	
3	Android OS	78	81	70	75	
4	Apps	85	86	81	83	
5	Permission	91	93	87	89	
6	Total Awareness/Dimension	80	83	77	79	

Gambar 4.11 Skor Kesadaran Jenis Kelamin Perempuan

Lalu berdasarkan Gambar 4.11 dari segi perempuan, didapatkan skor 79 yang dalam penelitian ini masuk dalam kategori dengan 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 area fokus *Permission* mendapatkan kategori baik dengan rentang nilai 87 hingga 93 dengan rata-rata nilai 89. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut, ketiga area fokus lainnya seperti *Hardware, Android OS* dan *Apps* walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut. Namun pada area fokus terkait isu *Backdoor* mendapatkan kategori buruk dengan rentang nilai 66 hingga 81, dengan rata-rata nilai 72, sehingga perlu perhatian khusus untuk upaya peningkatan.

Diantara laki-laki dan perempuan, secara skor keseluruhan memiliki perbedaan yang signifikan antara keduanya. Dari seluruh total keseluruhan berdasarkan area fokus *Backdoor, Hardware, Android OS, Apps, dan Permission* laki-laki lebih dominan namun hanya pada area fokus *permission*, nilai perempuan lebih tinggi dibandingkan laki-laki.

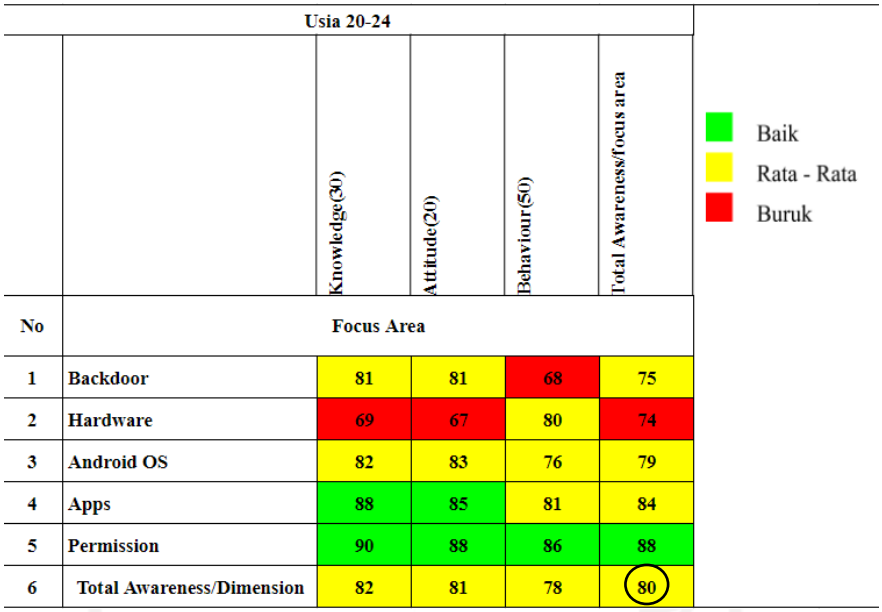
4.2.2 Skor Kesadaran Menurut Usia



Usia <20					
	Dimensi (Bobot)	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
No	Focus Area				
1	Backdoor	77	81	67	73
2	Hardware	62	67	80	72
3	Android OS	80	83	81	81
4	Apps	86	85	80	83
5	Permission	92	88	88	89
6	Total Awareness/Dimension	79	81	79	80

Gambar 4.12 Skor Kesadaran Usia Di bawah 20 Tahun

Berdasarkan Gambar 4.12 dari segi usia di bawah 20 tahun, didapatkan skor 80 yang dalam penelitian ini masuk dalam kategori dengan nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge*, *attitude*, maupun *behavior* juga memiliki nilai rata-rata di rentang 79 hingga 81. Dari kelima area fokus yang ada, hanya area fokus *Permission* mendapatkan kategori baik dengan rentang nilai 88 hingga 92 dengan rata-rata nilai 89. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut, kedua area fokus lainnya seperti *Android OS* dan *Apps* walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut. Namun pada area fokus terkait isu *Backdoor dan Hardware* mendapatkan kategori buruk sehingga perlu perhatian khusus untuk upaya peningkatan.



No	Focus Area				
1	Backdoor	81	81	68	75
2	Hardware	69	67	80	74
3	Android OS	82	83	76	79
4	Apps	88	85	81	84
5	Permission	90	88	86	88
6	Total Awareness/Dimension	82	81	78	80

Gambar 4.13 Skor Kesadaran Usia 20 Sampai 24 Tahun

Lalu berdasarkan Gambar 4.13 dari segi usia rentang 20 hingga 24 tahun, didapatkan skor 80 yang dalam penelitian ini masuk dalam kategori dengan 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 area fokus *Permission* mendapatkan kategori baik dengan rentang nilai 87 hingga 93 dengan rata-rata nilai 89. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut, ketiga area fokus lainnya seperti *Hardware, Android OS* dan *Apps* walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut. Namun pada area fokus terkait isu *Backdoor* mendapatkan kategori buruk dengan rentang nilai 66 hingga 81 dengan rata-rata nilai 72, sehingga perlu perhatian khusus untuk upaya peningkatan.

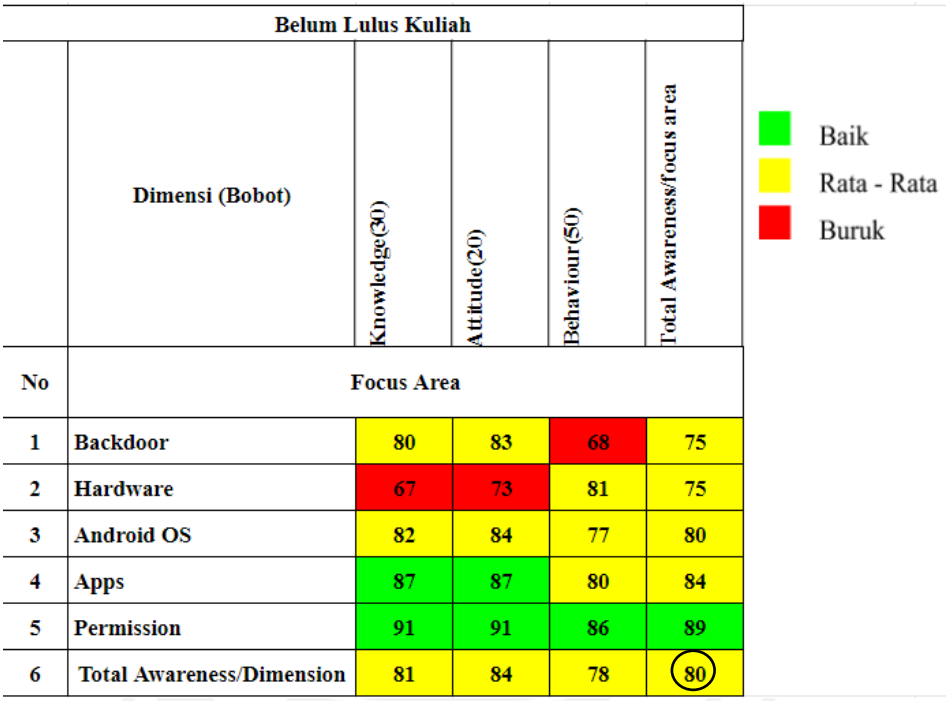
Usia 25+						
	Dimensi Bobot	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area	Baik Rata - Rata Buruk
No	Focus Area					
1	Backdoor	84	90	66	76	
2	Hardware	74	80	81	79	
3	Android OS	81	88	77	80	
4	Apps	84	88	77	81	
5	Permission	91	92	83	87	
6	Total Awareness/Dimension	83	88	77	81	

Gambar 4.14 Skor Kesadaran Usia Di atas 25 Tahun

Lalu berdasarkan Gambar 4.14 dari segi usia rentang 20 hingga 24 tahun, didapatkan skor 81 yang dalam penelitian ini masuk dalam kategori dengan 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 88. Dari kelima area fokus yang ada, hanya area fokus *Permission* mendapatkan kategori baik dengan rentang nilai 83 hingga 92 dengan rata-rata nilai 87. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut. Keempat area fokus lainnya seperti *Backdoor, Hardware, Android OS* dan *Apps* walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Diantaran 3 pembagian di atas, secara skor keseluruhan terdapat sedikit perbedaan yang terlihat dari skor kesadaran keamanan usia 25 tahun lebih dengan tinggi skor 1 dibandingkan usia di bawah 25 tahun. Hal ini disebabkan usia 25 tahun dan seterusnya sudah matang dari segi pemikiran dan masih muda yang lebih paham dengan apa yang harus dilakukan ketika menggunakan *smartphone* dengan baik dan tepat (Common & Curricula, 2012).

4.2.3 Skor Kesadaran Menurut Pendidikan



Belum Lulus Kuliah					
	Dimensi (Bobot)	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
No	Focus Area				
1	Backdoor	80	83	68	75
2	Hardware	67	73	81	75
3	Android OS	82	84	77	80
4	Apps	87	87	80	84
5	Permission	91	91	86	89
6	Total Awareness/Dimension	81	84	78	80

Gambar 4.15 Skor Kesadaran Belum Lulus Kuliah

Berdasarkan Gambar 4.15 dari segi responden yang masih menempuh pendidikan dan belum lulus kuliah, didapatkan skor 80 yang dalam penelitian ini masuk dalam kategori dengan 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* mendapatkan kategori baik dengan rentang nilai 86 hingga 91 dengan rata-rata nilai 89. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut. Keempat area fokus lainnya seperti *Backdoor*, *Hardware*, *Android OS* dan *Apps* walaupun sudah cukup baik, masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Sudah Lulus Kuliah					
	Dimensi (Bobot)	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
No	Focus Area				
1	Backdoor	81	88	64	74
2	Hardware	71	75	77	75
3	Android OS	84	89	77	82
4	Apps	87	88	81	84
5	Permission	88	92	87	88
6	Total Awareness/Dimension	82	86	77	81

Baik
Rata - Rata
Buruk

Gambar 4.16 Skor Kesadaran Sudah Lulus Kuliah

Lalu berdasarkan Gambar 4.16 dari segi responden yang masih menempuh pendidikan dan belum lulus kuliah, didapatkan skor 81 yang dalam penelitian ini masuk dalam kategori dengan 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 86. Dari kelima area fokus yang ada, hanya area fokus *Permission* mendapatkan kategori baik dengan rentang nilai 87 hingga 92 dengan rata-rata nilai 88. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut. Keempat area fokus lainnya seperti *Backdoor*, *Hardware, Android OS* dan *Apps* walaupun sudah cukup baik, masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut. Namun pada area fokus terkait isu *Backdoor* mendapatkan kategori buruk dengan rentang nilai 64 hingga 88, dengan rata-rata nilai 74, sehingga perlu perhatian khusus untuk upaya peningkatan.

4.2.4 Skor Kesadaran Menurut Adopsi Teknologi Informasi

Early Adopter					
	Dimensi (Bobot)	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
No	Focus Area				
1	Backdoor	83	87	75	80
2	Hardware	69	75	84	78
3	Android OS	85	88	81	84
4	Apps	87	90	84	86
5	Permission	92	94	94	93
6	Total Awareness/Dimension	83	87	84	84

Baik
Rata - Rata
Buruk

Gambar 4.17 Skor Keamanan Early Adopter

Pada Gambar 4.17 dari *Early Adopter*, didapatkan skor 84 yang dalam penelitian ini masuk dalam kategori dengan nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai rata-rata di rentang 83 hingga 87. Dari kelima area fokus yang ada, area fokus *Apps* dan *Permission* mendapatkan kategori baik dengan nilai 86 dan 93. Dengan kata lain, kesadaran keamanan terkait isu *Apps* dan *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut. Sedangkan ketiga area fokus lainnya seperti *Backdoor, Hardware,* dan *Android OS* walaupun sudah cukup baik, masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Majority

No	Dimensi (Bobot) / Focus Area	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
1	Backdoor	80	83	68	75
2	Hardware	67	73	80	75
3	Android OS	82	84	78	80
4	Apps	87	86	79	83
5	Permission	90	91	87	89
6	Total Awareness/Dimension	81	83	78	80

Baik
Rata - Rata
Buruk

Gambar 4.18 Skor Keamanan Majority

Berdasarkan Gambar 4.18 dari segi *Majority*, didapatkan skor 80 yang dalam penelitian ini masuk dalam kategori dengan 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 83. Dari kelima area fokus yang ada, hanya area fokus *Permission* mendapatkan kategori baik dengan rentang nilai 87 hingga 91 dengan rata-rata nilai 89. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut. Keempat area fokus lainnya seperti *Backdoor*, *Hardware*, *Android OS* dan *Apps* walaupun sudah cukup baik, masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

	Laggard				
	Dimensi (Bobot)	Knowledge(30)	Attitude(20)	Behaviour(50)	Total Awareness/focus area
No	Focus Area				
1	Backdoor	79	82	59	70
2	Hardware	68	72	74	72
3	Android OS	80	81	69	75
4	Apps	86	86	79	83
5	Permission	89	90	77	83
6	Total Awareness/Dimension	80	82	72	76

Baik
Rata - Rata
Buruk

Gambar 4.19 Skor Keamanan Laggard

Berdasarkan Gambar 4.12 dari segi usia di bawah 20 tahun, didapatkan skor 80 yang dalam penelitian ini masuk dalam kategori dengan nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge*, *attitude*, maupun *behavior* juga memiliki nilai rata-rata di rentang 79 hingga 81. Dari kelima area fokus yang ada, hanya area fokus *Permission* mendapatkan kategori baik dengan rentang nilai 88 hingga 92 dengan rata-rata nilai 89. Dengan kata lain, kesadaran keamanan terkait isu *Permission* dirasa sudah baik dan perlu dipertahankan di level tersebut. Kedua area fokus lainnya seperti *Android OS* dan *Apps* walaupun sudah cukup baik, masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut. Namun pada area fokus terkait isu *Backdoor dan Hardware* mendapatkan kategori buruk sehingga perlu perhatian khusus untuk upaya peningkatan.

4.3 Analisis *Multiple Linear Regression*

Melalui *multiple linear regression* yang dihitung menggunakan RStudio dengan Bahasa Pemrograman R akan memudahkan proses pencarian faktor-faktor yang berpengaruh pada perbedaan tingkat kesadaran keamanan pengguna *smartphone* Android di Indonesia. Regresi linear merupakan sebuah model sederhana. Model sederhana ini membentuk model dengan pendekatan garis linear dengan prinsip meminimalkan jumlah kuadrat residual pada sebuah data.

Tabel 4.2 Kode Program untuk Memanggil *File Google Sheets*

```
#___data prep Smartphone Android___#
library(gsheet)
dewal <-
gsheet2tbl("https://docs.google.com/spreadsheets/d/19YKsj2aMyAEZqyTC1BJjO
ewniKPvYss-nqa_owrbbq0/edit#gid=0")
View(dewal)
summary(dewal)
str(dewal)
```

Pada Tabel 4.2 merupakan kode program untuk mengunduh terlebih dahulu *Google Sheets* sebagai tabel dari link yang dapat disebarkan melalui *library gsheet* menggunakan fungsi *gsheet2tbl.* Kemudian, menampilkan sebuah data dari *Google Sheets* sebelumnya ke dalam Rstudio dengan memanggil data dewal menggunakan fungsi *view*. Fungsi *summary* digunakan untuk menghasilkan ringkasan dari berbagai fungsi *model fitting* dan fungsi *str* digunakan untuk menghasilkan secara ringkas struktur internal objek R, fungsi diagnostik dan alternatif untuk ringkasan.

Tabel 4.3 Kode Program Deskripsi Variabel Kesadaran Keamanan

```
#___variable desc smartphone Android#
# id        no unik responden
# na        nilai total awareness per orang
# jk        jenis kelamin (perempuan = 1)
# us        usia/umur
# pd        pendidikan terakhir (sudah lulus kuliah = 1)
# ti        adopsi teknologi informasi (Earlyadopt= 1, majority= 2,
laggard= 3)
# inc       income/pemasukan dalam sebulan (< 1 jt = 1)
# pl        pulau (jawa = 1)
# ad        asal daerah kabupaten/kota (kota = 1)
# m2        multiple linear regression
```

Berdasarkan deskripsi variabel kesadaran keamanan pengguna *smartphone* Android, Tabel 4.3 berikut merupakan deskripsi dari variabel kesadaran keamanan pengguna *smartphone* Android.

Tabel 4.4 Kode Program untuk Analisis Linear berganda

```
#____multiple linear regression smartphone Android___#
m2 <- lm(na ~  jk + us + pd + ad + pl + ti + inc , data = dewal)
print(m2)
summary(m2)

#__Standardized__#
m2.sd <- lm(scale(na) ~ scale(jk) + scale(us) + scale(pd) +
            scale(ad) + scale(pl)+ scale(ti) + scale(inc), data = dewal)
print(m2.sd)
summary(m2.sd)
```

Pada Tabel 4.4 merupakan kode program untuk melakukan proses analisis regresi linear berganda. Pada bagian pertama merupakan sebuah kode untuk analisis regresi linear berganda yang belum di standarisasi nilai DV (*Dependent Variable*) dan IV (*Independent Variable*) yang akan menjelaskan seberapa banyak perubahan dalam *dependent variable* (Y) yang diprediksi terjadi per unit perubahan dalam *independent variable* (X). Lalu, kode program yang kedua merupakan sebuah kode untuk menganalisis regresi linear berganda yang sudah di standarisasi nilai DV (*Dependent Variable*) dan IV (*Independent Variable*) dengan standar deviasi yang memberi tahu seberapa banyak perubahan dalam *dependent variable* (Y) yang diprediksi terjadi per unit perubahan dalam *independent variable* (X).

Ketika kode program tersebut dijalankan pada Rstudio akan menyajikan beragam informasi seperti nilai koefisien dan tingkat signifikan pada suatu variabel. Melalui kode program ini didapatkan nilai estimasi, nilai standar eror, tingkat pengaruh variabel yang mempengaruhi skor kesadaran keamanannya, dan lain sebagainya. Selain itu terdapat fungsi *print* yang digunakan untuk menampilkan hasil analisis regresi linear berganda dan fungsi *summary* yang digunakan menghasilkan hasil ringkasan dari berbagai fungsi *model fitting*. hasil *output* dapat dilihat pada Gambar 4.20 dan Gambar 4.21 di bawah ini.

```
> summary(m2)

Call:
lm(formula = na ~ jk + us + pd + ad + pl + ti + inc, data = dewal)

Residuals:
    Min      1Q  Median      3Q     Max
-46.563  -8.040   1.558   9.355  21.307

Coefficients:
            Estimate Std. Error t value Pr(>|t|)
(Intercept)  71.6273     6.0747  11.791   <2e-16 ***
jk           -3.3959     1.3951  -2.434   0.0154 *
us            0.4948     0.2780   1.780   0.0760 .
pd           -0.8001     2.3108  -0.346   0.7294
ad           -0.3736     1.4017  -0.267   0.7900
pl           -2.0555     1.6187  -1.270   0.2050
ti            0.4987     1.0844   0.460   0.6459
inc           1.4812     1.4176   1.045   0.2968
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 12.78 on 337 degrees of freedom
  (51 observations deleted due to missingness)
Multiple R-squared:  0.032,     Adjusted R-squared:  0.01189
F-statistic: 1.591 on 7 and 337 DF,  p-value: 0.1368
```

Gambar 4.20 Hasil Formula *Unstandardized*

```
> summary(m2.sd)

Call:
lm(formula = scale(na) ~ scale(jk) + scale(us) + scale(pd) +
    scale(ad) + scale(pl) + scale(ti) + scale(inc), data = dewal)

Residuals:
    Min      1Q  Median      3Q     Max
-3.6880 -0.6368  0.1234  0.7409  1.6876

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept) -0.008858   0.054620  -0.162   0.8713
scale(jk)   -0.134446   0.055231  -2.434   0.0154 *
scale(us)    0.107794   0.060565   1.780   0.0760 .
scale(pd)   -0.021252   0.061383  -0.346   0.7294
scale(ad)   -0.014807   0.055554  -0.267   0.7900
scale(pl)   -0.073012   0.057498  -1.270   0.2050
scale(ti)    0.025407   0.055244   0.460   0.6459
scale(inc)   0.058670   0.056151   1.045   0.2968
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 1.012 on 337 degrees of freedom
  (51 observations deleted due to missingness)
Multiple R-squared:  0.032,     Adjusted R-squared:  0.01189
F-statistic: 1.591 on 7 and 337 DF,  p-value: 0.1368
```

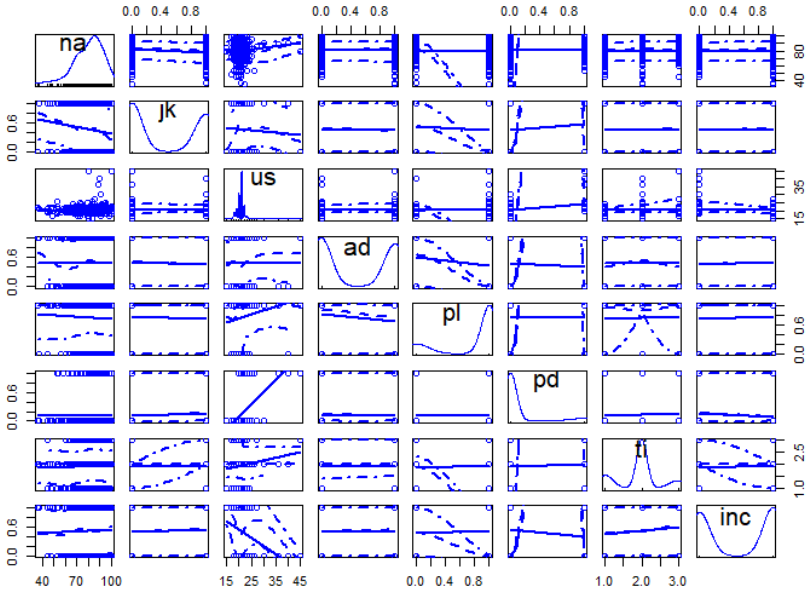
Gambar 4.21 Hasil Formula *Standardized*

Tabel 4.5 Kode Program untuk Diagnosis *Outliers*

```
#___diagnostic smartphone Android#

#install.packages("car")
library(car)
scatterplotMatrix(~ na + jk + us + ad + pl + pd + ti + inc, data = dewal)

#studentized residuals
res.std <- rstandard(m2)
plot(res.std, ylab="Standardized Residual", ylim=c(-3.5,3.5))
abline(h =c(-3,0,3), lty = 2)
index <- which(res.std > 3 | res.std < -3)
text(index-20, res.std[index], labels = dewal$id[index])
print(index)
print(dewal$id[index])

plot(res.std, ylab="Standardized Residual", ylim=c(-3.5,3.5))
abline(h =c(-2.5,0,2.5), lty = 2)
index <- which(res.std > 2.5 | res.std < -2.5)
text(index-20, res.std[index], labels = dewal$id[index])
print(index)
print(dewal$id[index])

#Bonferroni p-values for testing outliner
outlierTest(m2)

#detecting points with high leverage
#install.packages("faraway")
library(faraway)
h <- influence(m2)$hat
halfnorm(influence(m2)$hat, ylab = "leverage")

#the cut of value for cook's distance
cutoff <- 4/((nrow(dewal)-length(m2$coefficients)-2))
plot(m2, which = 4, cook.levels = cutoff)

#cook's distance, studentized residuals, and leverage in the same plot
influencePlot(m2, main="Influence Plot", sub="Circle size is proportional
to Cook's Distance" )

#4 diagnostic plots to identify influential points
infIndexPlot(m2)

#residual vs. fitted value plot for Homoscedasticity
plot(m2$resid ~ m2$fitted.values)
abline(h = 0, lty = 2)

#residual vs. fitted value and all predictors plus test for curvature
residualPlots(m2)
```

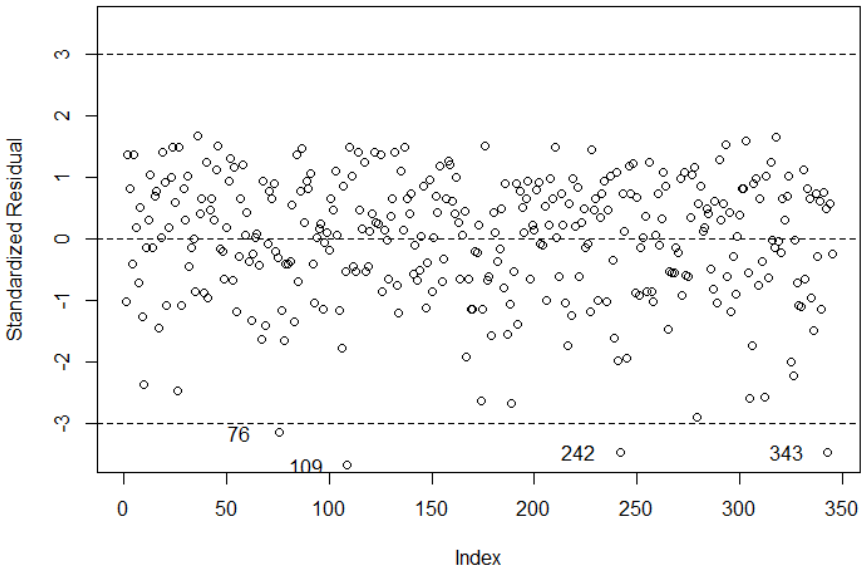
Pada Tabel 4.20 merupakan kode program untuk menguji *outlier* pada data yang ingin digunakan. *Outliers* adalah observasi atau data dengan karakteristik yang unik dan terlihat sangat berbeda jauh dengan observasi-observasi lainnya dan muncul dalam bentuk nilai ekstrim baik untuk variabel tunggal atau variabel kombinasi (Ghozali, 2009). Pada kode program *scatterplotMatrix* berfungsi untuk membuat sebuah *plot* matriks sebar yang ditingkatkan,

termasuk tampilan univariat pada sebuah diagonal dan berbagai garis yang dipasang dapat dilihat pada Gambar 4.22.

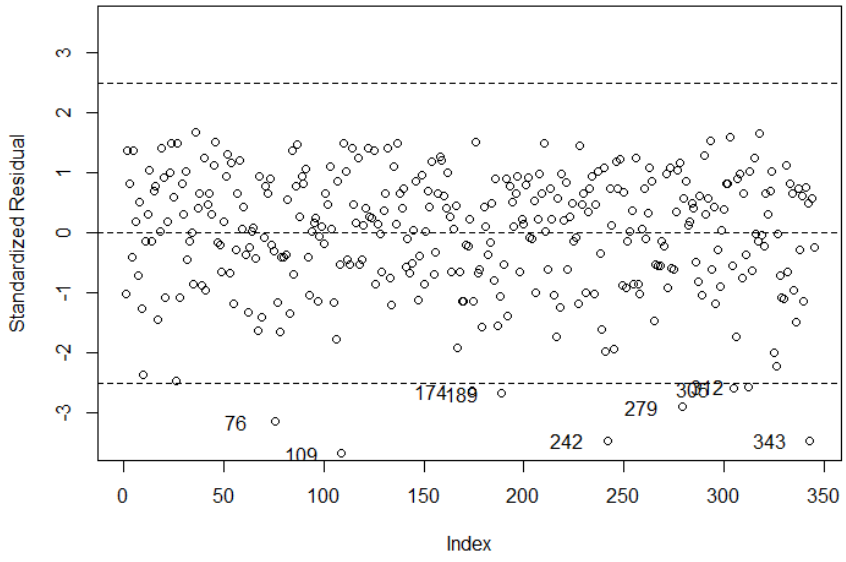


Gambar 4.22 *Plot scatterplot Matrix*

Lalu, kode program *studentized residuals range* yang dicoba pada *range* pertama (-3, 0, 3) dan (-2.5, 0, 2.5) digunakan untuk menghasilkan nilai dari sisa bagi dengan standar deviasi yang pada kedua *range* tersebut. Dari kode tersebut akan menghasilkan data yang kemungkinan *outlier*, untuk hasil *outlier's* yang memiliki kemungkinan signifikan dapat dilihat pada Gambar 4.23 dan Gambar 4.24.



Gambar 4.23 *Studentized Residuals Range* (-3,0,3)



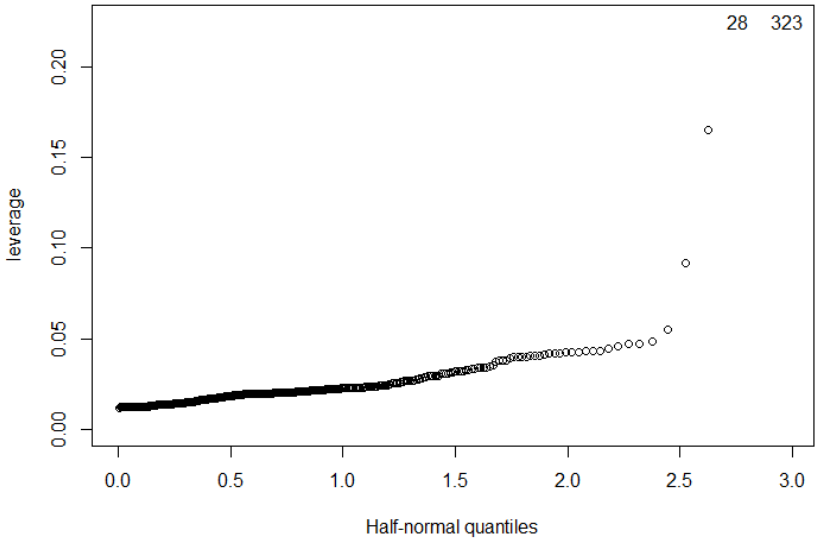
Gambar 4.24 *Studentized Residuals Range* (-2.5,0,2,5)

Selanjutnya kode untuk melihat *outlierTest* dari analisi linear berganda dengan *Bonferroni p-values for testing outlier, high leverage, Cook's distance.* Pada hasil dari kode program *Bonferroni p-values for testing outlier* yaitu data 109 merupakan data yang signifikan dapat dilihat pada Gambar 4.25 di bawah ini.

```
> #Bonferroni p-values for testing outliner
> outlierTest(m2)
No Studentized residuals with Bonferroni p < 0.05
Largest |rstudent|:
     rstudent unadjusted p-value Bonferroni p
109 -3.737604         0.00021828     0.075306
```

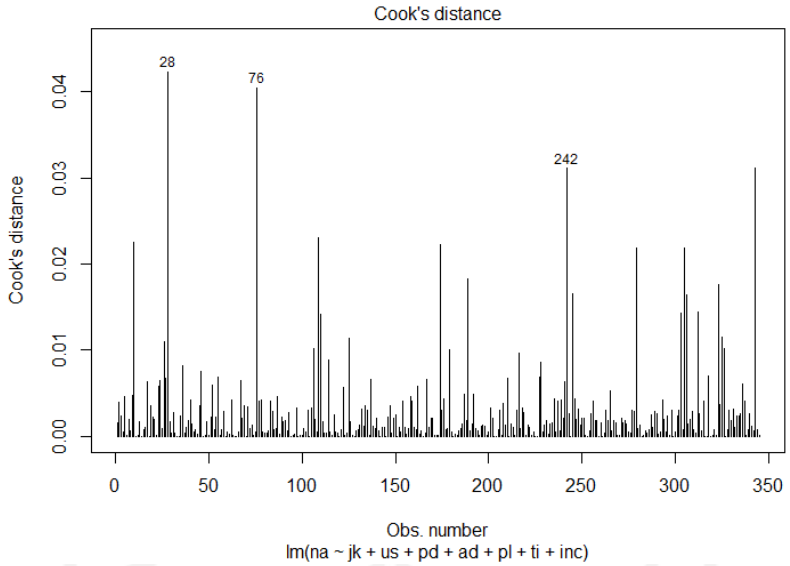
Gambar 4.25 Hasil *Bonferroni p-values for testing outlier*

Lalu pada hasil *high leverage*, dapat dilihat data yang memungkinkan signifikan didapatkan yaitu, pada data 28 dan 323 kemudian data tersebut dapat divisualisai menggunakan fungsi *Half-Normal Quantiles* dapat dilihat pada Gambar 4.26 di bawah ini.



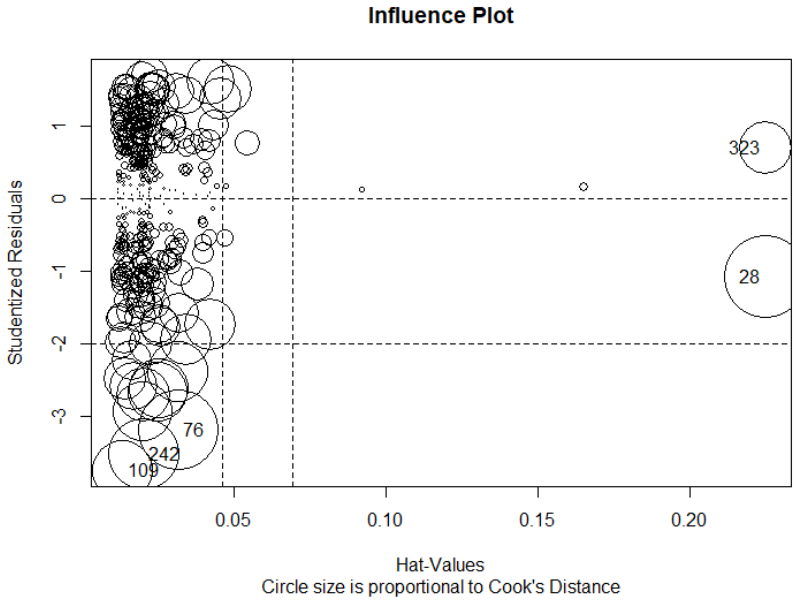
Gambar 4.26 Hasil *high leverage*

Kemudian pada hasil *Cook's distance*, dapat dilihat dapat yang memungkinkan signifikan didapatkan yaitu, pada data 28, 76, dan 242 kemudian data tersebut dapat divisualisasi menggunakan fungsi *plot* pada *cook's distance* dapat dilihat pada Gambar 4.27 di bawah ini.



Gambar 4.27 Hasil *Cook's distance*

Lalu, tiga kode *cook's distance, standardized residuals, and leverage* dimasukkan dalam satu *plot* yang berfungsi untuk membuat *plot* "gelembung" dari *studentized residuals versus hat values* dengan area lingkaran yang mewakili pengamatan yang sebanding dengan nilai *Cook's distance*. Dari *plot* ini, dapat dihasilkan *outlier* akhir dengan membandingkan 3 cara yang berbeda untuk mencari *outlier* tersebut agar mendapatkan hasil yang akurat dapat dilihat pada Gambar 4.28 di bawah ini.



Gambar 4.28 Hasil Visualisasi *Influence Plot*

Kemudian, kode selanjutnya berfungsi untuk memberikan pengaruh dari indeks *plot* dan diagnostik terkait untuk mode regresi. Terakhir, kode residual yang akan dicoba dengan *plot homoscedasticity* berfungsi untuk membandingkan residual dengan *fitted values* untuk menguji *homoskedastisitas*. Terdapat lima buah *outlier* yang ditemukan yaitu data ke 28, 76, 109, 242, 323 yang memungkinkan paling signifikan. *Outlier* tersebut tidak akan dimasukkan ke dalam perhitungan analisis regresi linear berganda untuk menghindari perubahan nilai yang jauh dikarenakan *outlier* tersebut dan menambah keakuratan pada hasil analisis linear berganda.

Tabel 4.6 Kode Program untuk Analisis Regresi Linear BergandaTanpa *Outlier*

```
#___hasil regresi setelah diagnostic tanpa outlier__#
library(car)
m2 <- lm(na ~ jk + us + ad + pl + pd + ti + inc, data = dewal[-c(28, 76,
109, 239, 318),])
print(m2)
summary(m2)
vif(m2)

m2.sd <- lm(scale(na) ~ scale(jk) + scale(us) + scale(ad) +
            scale(pl) + scale(pd) + scale(ti) + scale(inc),
            data = dewal[-c(28, 76, 109, 239, 318),])
print(m2.sd)
summary(m2.sd)
vif(m2)
```

Pada Tabel 4.6 sebuah kode program untuk analisis linear berganda tanpa *outlier* yang belum distandarisasi dan yang sudah distandarisasi nilai *dependent variable* dan *independent variable* tanpa *outlier* tersebut sudah didapatkan melalui proses *diagnostic*. Selain itu, terdapat fungsi tambahan yaitu fungsi vif yang digunakan untuk mendapat nilai VIF (*Variance Inflation Factor)* untuk setiap *independent variable,* kemudian hasil dari kode program analisis regresi setelah melalui proses *diagnostic* dapat dilihat pada Gambar 4.29 dan Gambar 4.30 di bawah ini.

```
> summary(m2)

Call:
lm(formula = na ~ jk + us + ad + pl + pd + ti + inc, data = dewal[-c(28,
    76, 109, 242, 323), ])

Residuals:
    Min      1Q  Median      3Q     Max
-45.366  -7.895   1.502   9.109  21.797

Coefficients:
            Estimate Std. Error t value Pr(>|t|)
(Intercept)  67.5696     7.3789   9.157  < 2e-16 ***
jk           -3.6709     1.3342  -2.751  0.00626 **
us            0.6944     0.3421   2.030  0.04318 *
ad           -0.1582     1.3438  -0.118  0.90638
pl           -2.9783     1.5557  -1.914  0.05643 .
pd           -1.5071     2.2126  -0.681  0.49626
ti            0.8587     1.0381   0.827  0.40875
inc           2.3251     1.3554   1.715  0.08720 .
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 12.15 on 332 degrees of freedom
  (51 observations deleted due to missingness)
Multiple R-squared:  0.04649,   Adjusted R-squared:  0.02639
F-statistic: 2.313 on 7 and 332 DF,  p-value: 0.02582
```

Gambar 4.29 Hasil Formula *Unstandardized*

Setelah *Diagnostic*

```
> summary(m2.sd)

Call:
lm(formula = scale(na) ~ scale(jk) + scale(us) + scale(ad) +
    scale(pl) + scale(pd) + scale(ti) + scale(inc), data = dewal[-c(28,
    76, 109, 242, 323), ])

Residuals:
    Min      1Q  Median      3Q     Max
-3.7381 -0.6505  0.1237  0.7506  1.7960

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept) -0.002262   0.054429  -0.042  0.96688
scale(jk)   -0.151253   0.054975  -2.751  0.00626 **
scale(us)    0.123432   0.060812   2.030  0.04318 *
scale(ad)   -0.006519   0.055395  -0.118  0.90638
scale(pl)   -0.109867   0.057390  -1.914  0.05643 .
scale(pd)   -0.041166   0.060437  -0.681  0.49626
scale(ti)    0.045283   0.054747   0.827  0.40875
scale(inc)   0.095826   0.055862   1.715  0.08720 .
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 1.001 on 332 degrees of freedom
  (51 observations deleted due to missingness)
Multiple R-squared:  0.04649,   Adjusted R-squared:  0.02639
F-statistic: 2.313 on 7 and 332 DF,  p-value: 0.02582
```

Gambar 4.30 Hasil Formula *Standardized*

Setelah *Diagnostic*

Tabel 4.7 Kode Program untuk Mencari Rata-Rata Nilai VIFdan Nilai Ramsey

```
#mean VIF
meanvif <- (1.019427+
1.260169+1.037292+1.053731+1.221221+1.014130+1.056964)/7
print(meanvif)

#ramsey reset test
library(lmtest)
resettest(m2.sd, power = 2:3, type = c("fitted", "regressor",
                                       "princomp"), data = dewal[-c(28,
76, 109, 242, 323),])
```

Pada Tabel 4.7 dilakukan proses untuk menghitung rata-rata nilai VIF (*Variance Inflation Factor*) dari keseluruhan *independent variable* pada analisis regresi linear berganda. Kemudian dilanjutkan proses untuk mencari nilai *Ramsey RESET Test*. *Ramsey RESET Test* merupakan sebuah uji spesifikasi umum untuk model regresi linear yang telah dikembangkan oleh James B. Ramsey. Kata *RESET* pada *Ramsey RESET Test* merupakan singkatan dari *Regression Equation Specification Error Test* atau sebuah Uji Kesalahan Spesifikasi Persamaan Regresi.

Tabel 4.8 Kode Program Visualisasi Faktor-Faktor Berpengaruh

```
#___visualisasi faktor___#
library(jtools)
library(ggplot2)
effect_plot(m2, pred = jk, interval = TRUE, y.label = "Skor Kesadaran
Keamanan", x.label = "Perempuan") + ylim(75,88)
effect_plot(m2, pred = us, interval = TRUE, y.label = "Skor Kesadaran
Keamanan", x.label = "Usia") + ylim(70,115)
effect_plot(m2, pred = ad, interval = TRUE, y.label = "Skor Kesadaran
Keamanan", x.label = "asal daerah") + ylim(77,85)
effect_plot(m2, pred = pl, interval = TRUE, y.label = "Skor Kesadaran
Keamanan", x.label = "pulau jawa") + ylim(77,87)
effect_plot(m2, pred = pd, interval = TRUE, y.label = "Skor Kesadaran
Keamanan", x.label = "pendidikan") + ylim(74,88)
effect_plot(m2, pred = ti, interval = TRUE, y.label = "Skor Kesadaran
Keamanan", x.label = "adopsi teknologi informasi") + ylim(77,87)
effect_plot(m2, pred = inc, interval= TRUE, y.label = "Skor Kesadaran
Keamanan", x.label = "penghasilan") + ylim(75,85)
```

Pada Tabel 4.8 merupakan kode program untuk memvisualisasikan skor kesadaran keamanan terhadap sebuah faktor-faktor yang mempengaruhinya pada penelitian ini yaitu jenis kelamin, usia, asal daerah, Pulau Jawa dan luar Jawa, pendidikan terakhir, adopsi teknologi informasi, dan penghasilan bulanan dari pengguna *smartphone* Android di Indonesia. Terdapat 2 *library* yang biasa digunakan untuk memvisualisasi skor kesadaran keamanan tersebut, yaitu *Library jtools* dan *ggplot2. Library jtools* adalah kumpulan alat agar lebih efisien dalam memahami dan berbagi hasil terutama dalam menganalisis sebuah regresi yang di dalamnya

terdapat sejumlah fungsi untuk keperluan statistik dan pemrograman, sedangkan *library ggplot2* adalah sebuah alat untuk membuat grafik dengan kita yang memberikan sebuah data, memberi tahu *ggplot2* cara memetakan variabel ke primitif grafis apa yang digunakan, dan menangani detail pada visualisasi *plot*. Lalu fungsi *effect plot* yang digunakan untuk membuat visualisasi dalam bentuk *plot* yang fungsinya terdapat dalam *library jtools* untuk memudahkan penjelasan terkait pengaruh sebuah faktor-faktor demografis yang sudah disebutkan terhadap skor kesadaran keamanan pengguna *smartphone* Android di Indonesia. Kemudian di dalam fungsi *effect plot* terdapat fungsi lain yaitu *ylim* yang digunakan untuk membatasi skala skor kesadaran keamanan yang divisualisasikan yang terdapat dalam *library ggplot2.*

4.4 Hasil Regresi Linear Berganda

Dari hasil analisis regresi linear berganda yang bertujuan untuk mencari faktor-faktor demografis yang berpengaruh pada perbedaan tingkat kesadaran keamanan pengguna *smartphone* Android di Indonesia disajikan pada Tabel 4.9.

Tabel 4.9 Hasil Regresi Linear Berganda

Skor Kesadaran Keamanan Pengguna *Smartphone* Android di Indonesia

Jenis Kelamin	**-3.671**	****
Perempuan	**-0.151**	
	(0.055)	
Usia	**0.694**	*****
	0.123	
	(0.061)	
Asal Daerah	**-0.158**	
Kota	**-0.007**	
	(0.055)	
Pulau	**-2.978**	**.**
Jawa	**-0.110**	
	(0.057)	
Pendidikan	**-1.507**	
Sudah lulus kuliah	**-0.041**	
	(0.060)	
Adopsi Teknologi Informasi	**0.859**	
	0.045	
	(0.055)	
Penghasilan Bulanan	**2.325**	**.**
Kurang dari 1 juta rupiah	**0.096**	
	(0.056)	
Constant/Intercept	**67.570**	*****
	-0.002	
	(0.054)	
R^2	**0.046**	
Highest VIF	**1.260**	
Mean VIF	**1.095**	
Ramsey RESET Test	**0.603**	
Observation	**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.

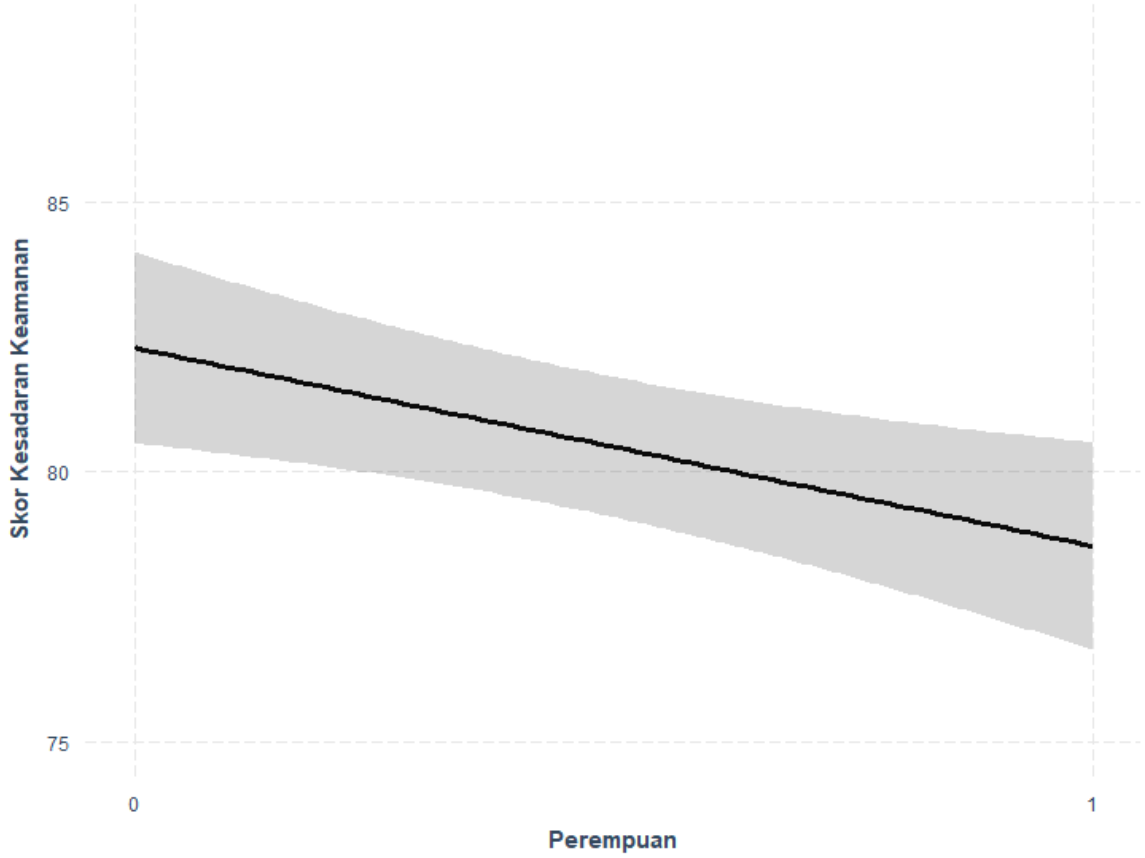
Dari hasil diagnosis pada iterasi awal, ditemukan lima buah *outliers* dan *influential cases* yang tidak disertakan pada iterasi berikutnya sehingga tersisa 391 responden yang menjadi model akhir di analisis regresi ini. Faktor yang memiliki pengaruh paling besar yaitu jenis

kelamin dan diikuti oleh usia. Apabila semua faktor lain bernilai sama, maka pengguna *smartphone* Android yang memiliki jenis kelamin perempuan akan memiliki skor 3,7 poin lebih rendah dibandingkan jenis kelamin laki-laki. Begitu pula dengan usia, pengguna *smartphone* Android yang usia memiliki skor sekitar 0,7 poin lebih tinggi jika semua faktor dianggap konstan.

Sementara itu, dari sisi faktor lain seperti asal daerah, Pulau Jawa, pendidikan, adopsi teknologi informasi, dan penghasilan bulanan ini tidak ditemukan perbedaan signifikan dari sisi skor kesadaran keamanannya. Pada faktor asal daerah, pengguna yang tinggal di kota memiliki skor 0.6 poin lebih rendah dibandingkan yang tinggal di kabupaten. Kemudian, pada faktor pulau pengguna yang tinggal di Pulau Jawa memiliki skor 3,0 poin lebih rendah dibandingkan pengguna yang tinggal di luar Pulau Jawa meliputi Sumatera, Kalimantan, Sulawesi, dan lainnya. Pada faktor penghasilan bulanan pengguna *smartphone* Android yang memiliki penghasilan bulanan kurang dari 1 juta rupiah akan memiliki skor 2,3 poin lebih rendah dibandingkan yang berpenghasilan 1 juta ke atas per bulannya. Begitu pula dengan pendidikan terakhir, pengguna *smartphone* Android yang memiliki pendidikan tinggi yang sudah lulus kuliah memiliki skor sekitar 1,5 poin lebih tinggi dibandingkan dengan yang tidak mengenyam atau belum lulus dari perguruan tinggi jika semua faktor dianggap konstan. Kemudian pada faktor adopsi teknologi informasi semakin tidak mengikuti perkembangan teknologi terbaru dan tidak menggunakannya pengguna *smartphone* Android tersebut maka akan turun skor kesadaran keamanannnya sebanyak 0,9 poin. Sebaliknya, semakin berusaha selalu mengikuti perkembangan terbaru dan sering kali termasuk yang pertama kali menggunakan *smartphone* Android tersebut maka akan naik skor kesadaran keamanannya sebanyak 0,9 poin.

4.4.1 Visualisasi Efek Faktor Jenis Kelamin

Dari hasil analisis regresi linear berganda faktor jenis kelamin, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.31.

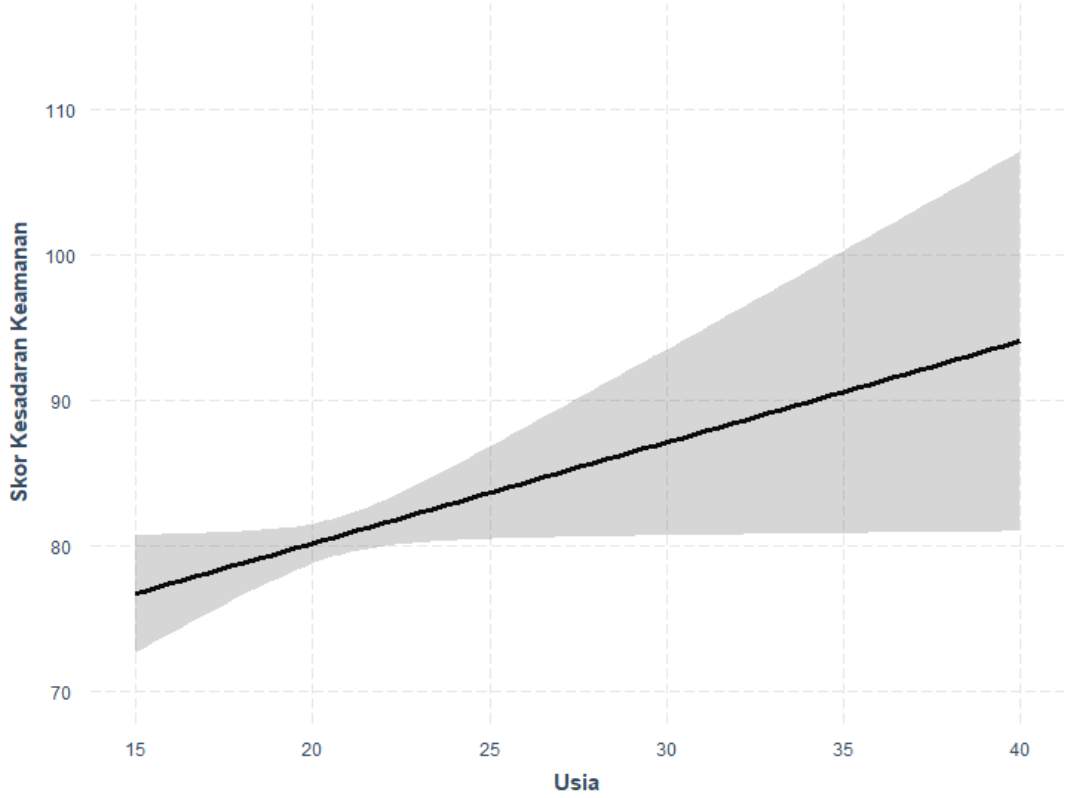


Gambar 4.31 Pengaruh Faktor Jenis Kelamin

Dari Gambar 4.31, pengaruh dari faktor jenis kelamin terlihat cukup signifikan sesuai dengan Tabel 4.9 sebelumnya. Untuk setiap pengguna *smartphone* Android dengan jenis kelamin perempuan akan memiliki skor 3,7 poin lebih rendah dibandingkan pengguna jenis kelamin laki-laki.

4.4.2 Visualisasi Efek Faktor Usia

Dari hasil analisis regresi linear berganda faktor usia, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.32.

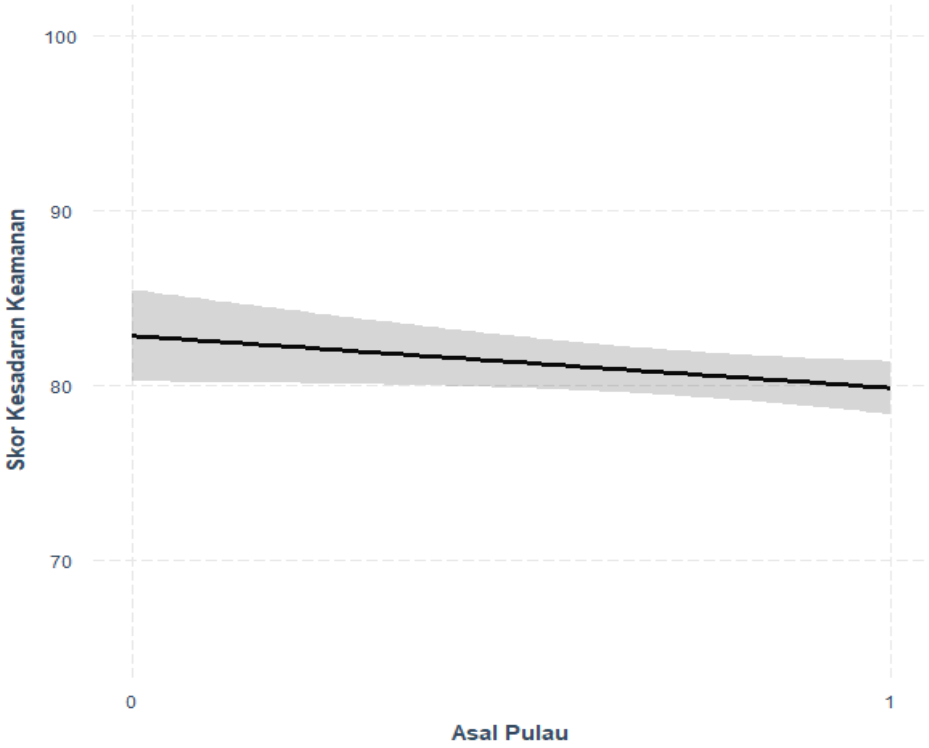


Gambar 4.32 Pengaruh Faktor Usia

Dari Gambar 4.32, pengaruh dari faktor usia terlihat ada perbedaan untuk setiap skor kesadaran keamanan terlihat cukup signifikan sesuai dengan Tabel 4.9. Semakin tua usia pengguna *smartphone* Android tersebut maka akan turun skor kesadaran keamananya sebanyak 0,7 poin setiap 1 tahun lebih tua. Sebaliknya, semakin muda usia pengguna *smartphone* Android tersebut maka skor kesadaran keamanannya akan naik sebanyak 0,7 poin setiap 1 tahun lebih muda.

4.4.3 Visualisasi Efek Faktor Pulau

Dari hasil analisis regresi linear berganda faktor asal daerah yaitu Pulau Jawa dan luar Pulau Jawa, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.33.

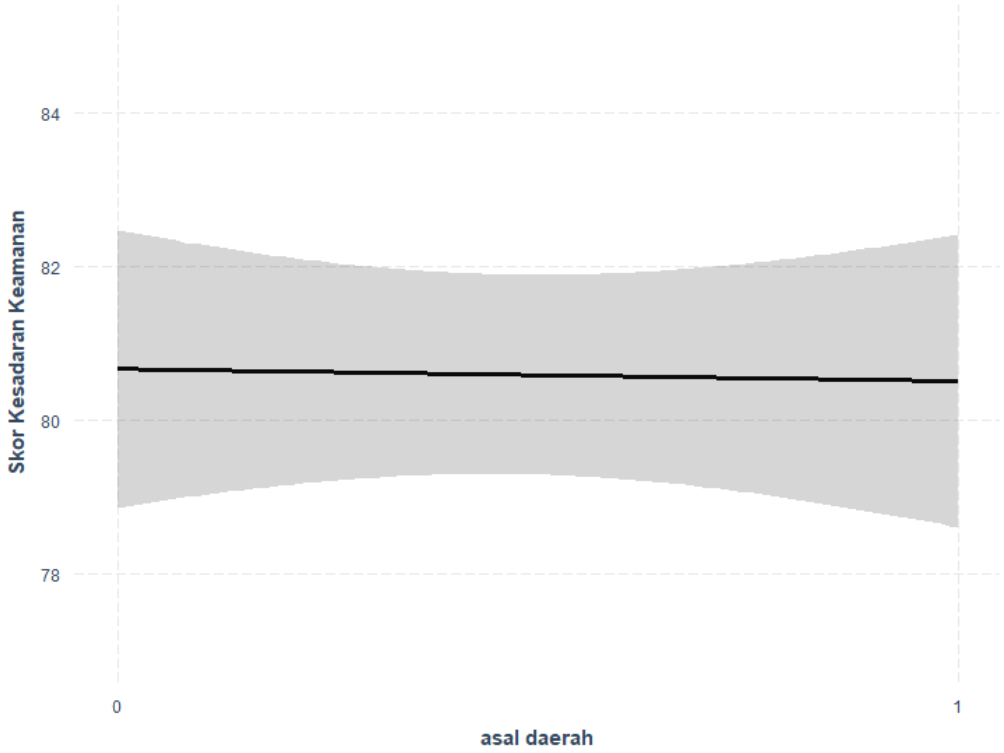


Gambar 4.33 Pengaruh Faktor Pulau

Dari Gambar 4.33, pengaruh dari faktor pulau cukup terlihat ada perbedaan untuk setiap skor kesadaran keamanan walaupun tidak signifikan sesuai dari hasil analisis pada Tabel 4.9. Untuk setiap pengguna *smartphone* Android yang tinggal di Pulau Jawa akan memiliki skor 3,0 poin lebih rendah dibandingkan pengguna yang tinggal di daerah luar Pulau Jawa. Sebaliknya, setiap pengguna *smartphone* Android yang tinggal di daerah luar Pulau Jawa akan memiliki skor 3,0 poin lebih tinggi dibandingkan dengan pengguna yang tinggal di Pulau Jawa.

4.4.4 Visualisasi Efek Faktor Asal Daerah

Dari hasil analisis regresi linear berganda faktor asal daerah yaitu kabupaten dan kota, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.34.

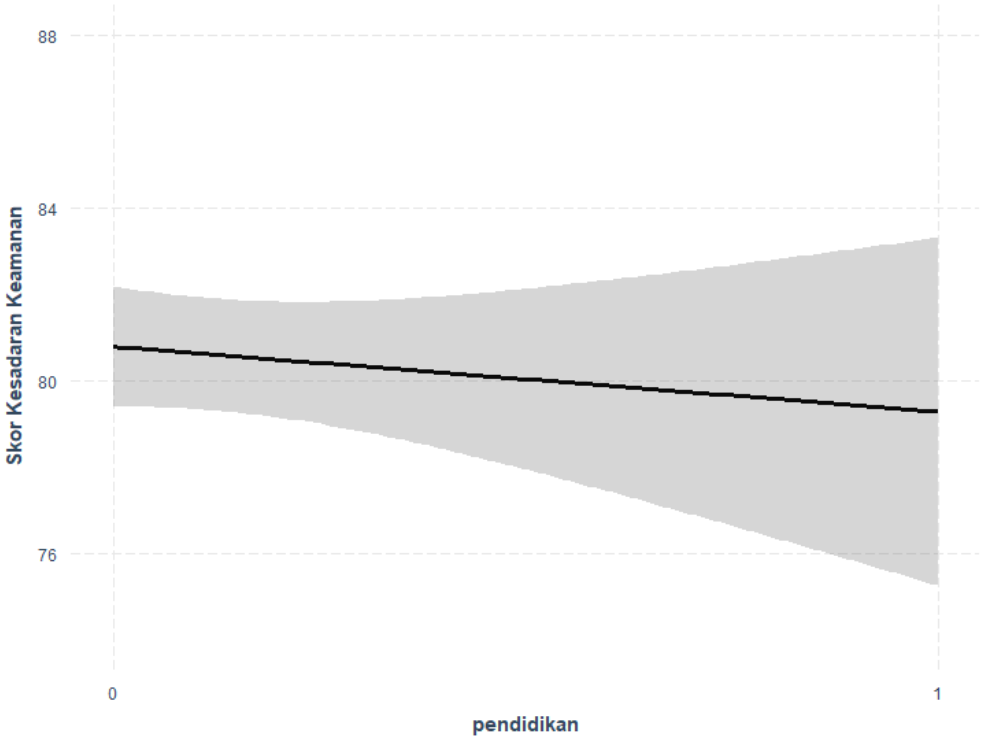


Gambar 4.34 Pengaruh Faktor Asal Daerah

Dari Gambar 4.26, pengaruh dari faktor asal daerah terlihat ada perbedaan untuk setiap skor kesadaran keamanan walaupun tidak signifikan sesuai dengan Tabel 4.9. Untuk setiap pengguna *smartphone* Android yang tinggal di daerah kota akan memiliki skor 0,16 poin lebih rendah dibandingkan pengguna yang tinggal di daerah kabupaten. Sebaliknya, setiap pengguna *smartphone* Android yang tinggal di daerah kabupaten akan memiliki skor 0,16 poin lebih tinggi dibandingkan dengan pengguna yang tinggal di daerah kota.

4.4.5 Visualisasi Efek Faktor Pendidikan

Dari hasil analisis regresi linear berganda faktor pendidikan yaitu belum lulus kuliah dan yang sudah lulus kuliah, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.34.

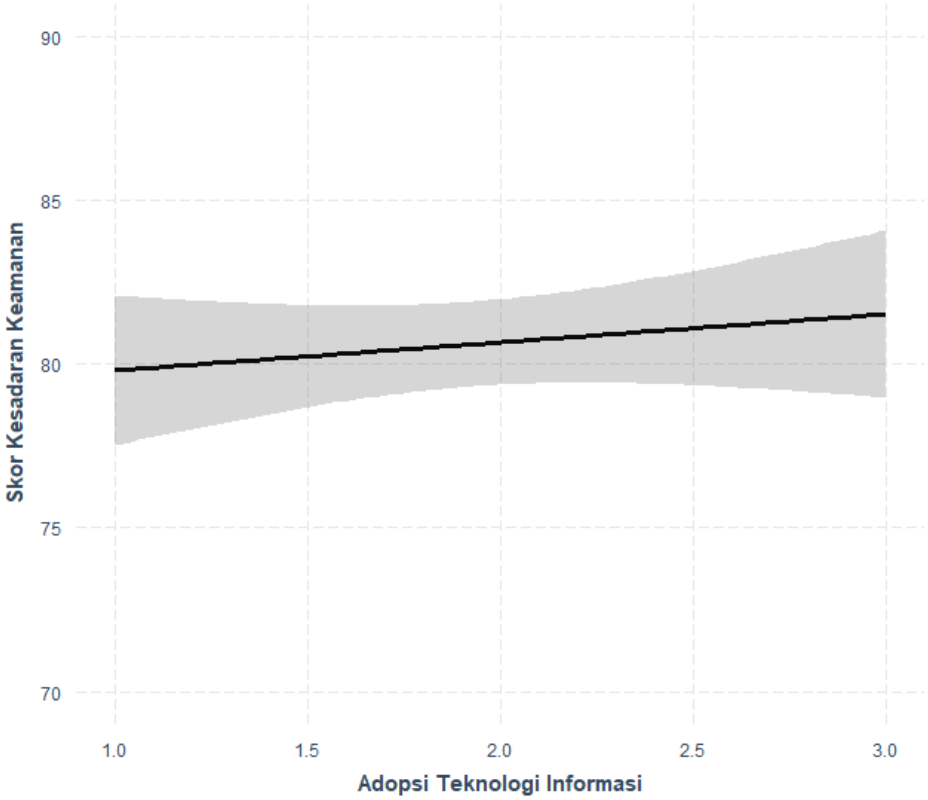


Gambar 4.35 Pengaruh Faktor Pendidikan Terakhir

Dari Gambar 4.35, pengaruh dari faktor pendidikan terakhir sangat terlihat perbedaannya untuk setiap skor kesadaran keamanan walaupun tidak signifikan karena sesuai dari hasil analisis pada Tabel 4.9. Untuk setiap pengguna *smartphone* Android yang memiliki pendidikan tinggi atau sudah lulus kuliah memiliki skor 1,5 poin lebih tinggi dibandingkan pengguna yang memiliki pendidikan rendah atau belum lulus kuliah. Sebaliknya, setiap pengguna *smartphone* Android yang memiliki pendidikan rendah atau belum lulus kuliah memiliki skor 1,5 poin lebih rendah dibandingkan dengan pengguna yang memiliki pendidikan tinggi atau sudah lulus kuliah.

4.4.6 Visualisasi Efek Faktor Adopsi Teknologi Informasi

Dari hasil analisis regresi linear berganda faktor pendidikan yaitu *Laggard, Majority* dan *Early Adopter*, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.36.

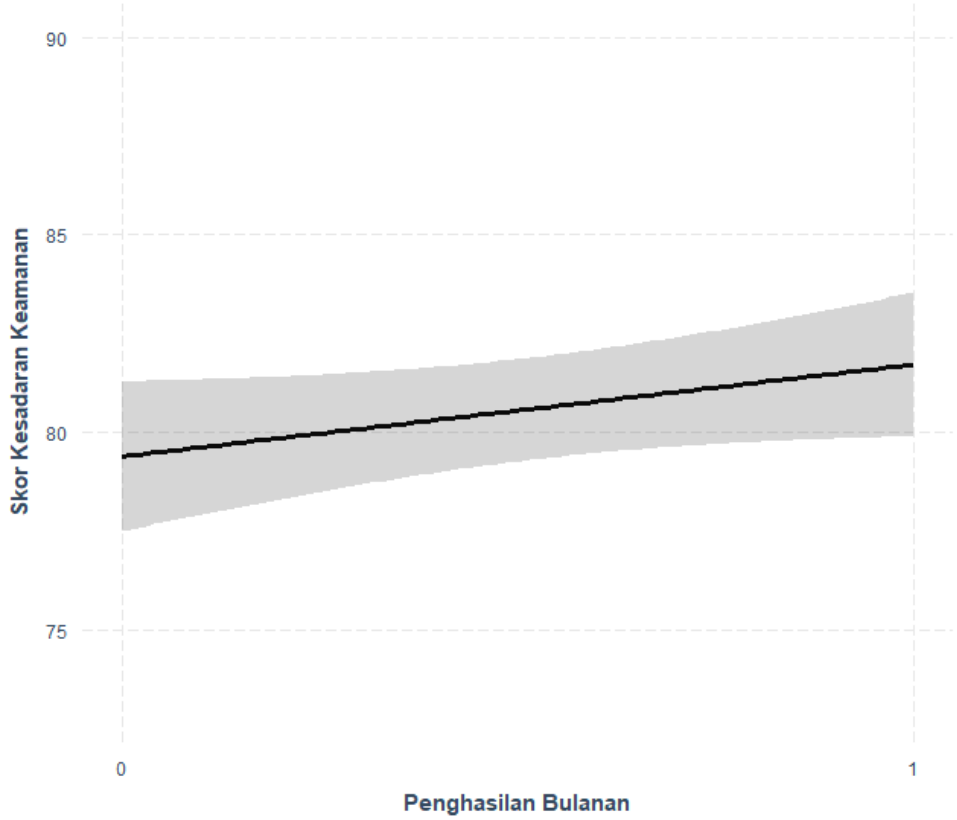


Gambar 4.36 Pengaruh Faktor Adopsi Teknologi Informasi

Dari Gambar 4.36, pengaruh dari faktor adopsi teknologi informasi terlihat ada perbedaan untuk setiap skor kesadaran keamanan walaupun tidak signifikan sesuai dengan Tabel 4.9. Semakin tidak mengikuti perkembangan teknologi terbaru dan tidak menggunakannya pengguna *smartphone* Android tersebut maka akan turun skor kesadaran keamanannnya sebanyak 0,9 poin. Sebaliknya, semakin berusaha selalu mengikuti perkembangan terbaru dan sering kali termasuk yang pertama kali menggunakan *smartphone* Android tersebut maka akan naik skor kesadaran keamanannya sebanyak 0,9 poin.

4.4.7 Visualisasi Efek Faktor Penghasilan Bulanan

Dari hasil analisis regresi linear berganda faktor penghasilan bulanan yaitu kurang dari satu juta dan lebih dari satu juta, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.37.



Gambar 4.37 Pengaruh Faktor Penghasilan Bulanan

Dari Gambar 4.37, pengaruh dari faktor penghasilan bulanan cukup terlihat perbedaannya untuk setiap skor kesadaran keamanan walaupun tidak signifikan karena sesuai dari hasil analisis pada Tabel 4.9. Untuk setiap pengguna *smartphone* Android yang memiliki penghasilan bulanan kurang dari 1 juta rupiah memiliki skor 2,3 poin lebih rendah dibandingkan yang berpenghasilan 1 juta ke atas per bulannya. Sebaliknya, setiap pengguna *smartphone* Android yang memiliki penghasilan bulanan 1 juta ke atas memiliki skor 2,3 poin lebih tinggi dibandingkan yang berpenghasilan kurang dari 1 juta per bulannya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

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 4.9 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, Apps* dan Android OS yang cukup tertinggal jika dibandingkan dengan area fokus *Permission*. Pada keempat area tersebut, perlu dilakukan upaya-upaya khusus dalam bentuk edukasi pengguna dalam bentuk literasi digital guna meningkatkan kesadaran keamanan informasi terutama pada pengguna *smartphone* Android untuk menghindari ancaman serangan *backdoor* yang bisa saja terjadi kapan saja.

Selain itu, peneliti ini juga menemukan perbedaan tingkat kesadaran keamanan pengguna *smartphone* Android di Indonesia berdasarkan faktor demografis seperti jenis kelamin, usia, lokasi baik berdasarkan pulau maupun kabupaten/kota, tingkat pendidikan, adopsi teknologi informasi dan penghasilan bulanan. Pengguna *smartphone* Android dengan jenis kelamin perempuan memiliki tingkat kesadaran keamanan yang lebih rendah, dibanding pengguna *smartphone* Android dengan jenis kelamin laki-laki. Begitu pula, dengan pengguna *smartphone* Android yang berusia 25 tahun ke atas, memiliki tingkat kesadaran keamanan yang lebih baik dibandingkan pengguna *smartphone* Android dengan usia 25 tahun ke bawah, ini disebabkan usia 25 tahun ke atas sudah matang dari segi pemikiran dan lebih paham dengan apa yang harus dilakukan ketika menggunakan *smartphone* dengan baik dan tepat. Adapun terkait faktor lain seperti lokasi berdasarkan pulau maupun kabupaten/kota, tingkatan pendidikan, adopsi teknologi informasi, dan penghasilan bulanan, terdapat perbedaan, tetapi tidak signifikan antar 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 fokus yang berbeda ke depannya.

5.2 Saran

Masih terdapat beberapa batasan-batasan atau kekurangan yang ada pada penelitian ini, seperti penyusunan pertanyaan yang digunakan untuk menghitung skor kesadaran keamanan

masih perlu ditingkatkan baik dari sisi kuantitas atau jumlahnya maupun kualitas misal dengan melibatkan pakar baik dari sisi keamanan maupun dari sisi pengguna *smartphone* Android dalam proses penyusunannya. Kemudian karakteristik responden yang masih cenderung homogen, baik dari sisi usia maupun lokasi juga berpotensi menyebabkan nilai kesadaran pengguna perlu kehati-hatian lebih jika akan dilakukan proses generalisasi ke seluruh pengguna *smartphone* Android di Indonesia.

DAFTAR PUSTAKA

Adenansi, R., & Novarina, L. A. (2017). Malware dynamic. *Jurnal of Education and Information Communication Technology*, *1*(1), 37–43.

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 115.

Alexander, M. (2018). Protect, Detect and Correct Methodology to Mitigate Incidents: Insider Threats. *Isaca Journal*, *3*, 1–7.

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*(May), 56–65. https://doi.org/10.1016/j.cose.2014.01.005

Amin, M. (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *5*(1), 15–24.

Andi, J. (2015). Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-GPS) Dengan Platform Android. *Jurnal Ilmiah Komputer Dan Informatika (KOMPUTA)*, *1*(1), 1–8. elib.unikom.ac.id/download.php?id=300375

Aptaguna, A., & Pitaloka, E. (2016). Pengaruh Kualitas Layanan Dan Harga Terhadap Minat Beli Jasa Go-Jek. *Widyakala Journal*, *3*(2012), 49.

Badan Pusat Statistik. (2019). Statistik Indonesia 2019. *BPS, 2019 (Indonesian Statistics)*, Jakarta: Badan Pusat Statistik.

Barrera, D., Kayacik, H. G., Van Oorschot, P. C., & Somayaji, A. (2010). A methodology for empirical analysis of permission-based security models and its application to Android. *Proceedings of the ACM Conference on Computer and Communications Security*, *1*, 73–84.

Chan, H., & Mubarak, S. (2012). Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications*, *60*(10), 23–31.

Common, C., & Curricula, C. (2012). *California Common Core Curricula for Child Welfare Workers Trainee ' s Guide Child and Youth Development in a Child Welfare Context Acknowledgments*.

Douglas D. Heckathorn. (2010). *Snowball Versus Respondent-Driven Sampling*. *51*(6), 656–

679. http://dx.doi.org/10.1016/j.ijar.2010.01.005

Etikan, I. (2016). Comparision of Snowball Sampling and Sequential Sampling Technique. *Biometrics & Biostatistics International Journal*, *3*(1), 1–2. https://doi.org/10.15406/bbij.2016.03.00055

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android security: A survey of issues, malware penetration, and defenses. *IEEE Communications Surveys and Tutorials*, *17*(2), 998–1022.

Ghozali, I. (2009). *Ekonometrika: Teori, Konsep, dan Aplikasi dengan SPSS 17. Semarang: Badan Penerbit Universitas Diponegoro. August*, 112–116.

Gio, P. U., & Effendie, A. R. (2018). *Belajar Bahasa Pemrograman R*. https://doi.org/10.31227/osf.io/ktmy2

Glanz, K., Rimer, B. k., & Viswanath, K. (2002). *Health Behavior and Health Education*.

Harlan, J. (2018). Analisis Regresi Linear. In *Journal of Chemical Information and Modeling* (Vol. 53, Issue 9).

Janna, N. M. (2020). *Variabel dan skala pengukuran statistik*. 1–8.

Kartika, H. D. (2019). *Pengukuran Tingkat Kesaranan Keamanan Infomrasi: Studi Kasus PT MNC SKY VISION Tbk.* (Vol. 1, Issue 4).

Khadijah, C. (2019). Transformasi perpustakaan untuk generasi millenial menuju revolusi industri 4.0. *IQRA`: Jurnal Ilmu Perpustakaan Dan Informasi (e-Journal)*, *12*(2), 59.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296.

Kurniawan, B., Akbar, M., & Negara, E. S. (2017). *Analisis Pendeteksian dan Pencegahan Serangan Backdoor Pada Layanan Server*. *12*, 1–10.

Manufaktur, P. (2013). Faktor-Faktor Yang Mempengaruhi Audit Delay Pada Perusahaan Manufaktur. *Accounting Analysis Journal*, *2*(1), 1–4.

Ramadhani, S. (2019). *Inilah Urutan Versi Android dari Awal Hingga Terbaru*. 1–23. https://www.dicoding.com/blog/urutan-versi-android/

Saragih, S. H. (2013). *Penerapan Metode Analytical Hierarchy Process (AHP) pada Sitem Pendukung Keputusan Pemilihan Laptop*. 82–88.

Sari, K., & Candiwan. (2014). Measuring information security awareness of Indonesian smartphone users. *Telkomnika (Telecommunication Computing Electronics and Control)*, *12*(2), 493–500. https://doi.org/10.12928/TELKOMNIKA.v12i2.2015

Silvia, A. F., Haritman, E., & Muladi, Y. (2014). Rancang Bangun Akses Kontrol Pintu

Gerbang Berbasis Arduino Dan Android. *Electrans*, *13*(1), 1–10.

Sugiyono, S. (2015). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, dan R&D*. *47*(6), 506.

Tan, T. S. E. G. (2020). *Isu Keselamatan Peranti Mudah Alih Dalam Dunia Digital untuk Institusi Pengajian Tinggi*. *November 2019*, 119–129.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.

เพ็ชราภรณ์, ช. (2557). No Titleภาวะผู้นำองค์กรและการจัดการที่มีประสิทธิภาพโรงพยาบาลรัฐ. In *วารสารสังคมศาสตร์วิชาการ* (Vol. 7, Issue 2).

LAMPIRAN

Survei Analisis Kesadaran Keamanan di Kalangan Pengguna Smartphone Android Atas S

Questions Responses 396

Section 1 of 7

Survei Analisis Kesadaran Keamanan di Kalangan Pengguna Smartphone Android Atas Serangan Berbasis Backdoor

Assalamu'alaikum wr.wb,

Bapak/Ibu/Saudara/Saudari yang saya hormati,

Perkenalkan, saya Muhammad Raffi Akhyari. Mahasiswa Tingkat Akhir Program Studi Informatika - Program Sarjana di Universitas Islam Indonesia, Yogyakarta.

Saat ini, saya sedang melakukan penelitian tentang kesadaran keamanan di kalangan pengguna smartphone Android atas serangan berbasis backdoor di bawah bimbingan Bapak Ahmad R. Pratama, Ph.D.

Hasil penelitian ini akan memajukan Literasi Digital dan meningkatkan Kesadaran Keamanan di kalangan pengguna smartphone Android atas serangan berbasis Backdoor terutama para pengguna smartphone di Indonesia. Kami berharap Bapak/Ibu/Saudara/Saudari bersedia meluangkan waktu untuk mengisi survei ini.

Sesuai dengan kode etik penelitian, semua data yang Bapak/Ibu/Saudara/Saudari isikan akan saya jaga kerahasiaannya dan hanya digunakan untuk kepentingan penelitian semata. Partisipasi dalam penelitian ini bersifat sukarela yang berarti tidak ada unsur pemaksaan.

kemudian, sepuluh (10) responden terpilih akan mendapatkan hadiah pulsa atau uang digital sebesar masing-masing sebesar Rp. 50.000,- sebagai rasa terima kasih kami atas partisipasi responden didalam penelitian ini.

Atas Ketersediaan Bapak/Ibu/Saudara/Saudari untuk mengisi survei ini saya ucapkan Terima Kasih

Hormat Peneliti,
Muhammad Raffi Akhyari

Ya

After section 1 Continue to next section

Section 2 of 7

Section title (optional)

Description (optional)

Perangkat yang sekarang Anda gunakan untuk mengisi kuesioner ini *

- Komputer Desktop
- Laptop
- Smartphone
- Tablet
- Other...

Undian Berhadiah

Bagian ini dapat diisi apabila Anda menginginkan hadiah yang akan kami berikan secara acak. Bagi Anda yang tidak menginginkan hadiah, maka Anda dapat menuju ke bagian berikutnya

Pilihan untuk Hadiah yang Diinginkan (bila berkenan)

- Pulsa
- Ovo

Dana

Link Aja

Nomor HP untuk Hadiah (bila berkenan)

Short answer text

After section 2 Continue to next section

Section 3 of 7

Demografi

Description (optional)

Jenis Kelamin *

Laki-Laki

Perempuan

Usia (dalam Tahun) *

Short answer text

Asal Daerah (Provinsi) *

2. Sumatera Utara
3. Sumatera Barat
4. Riau
5. Kepulauan Riau
6. Jambi
7. Bengkulu
8. Sumatera Selatan
9. Kepulauan Bangka Belitung
10. Lampung
11. Banten
12. DKI Jakarta
13. Jawa Barat
14. Jawa Tengah
15. Daerah Istimewa Yogyakarta
16. Jawa Timur
17. Bali
18. Nusa Tenggara Barat
19. Nusa Tenggara Timur
20. Kalimantan Utara
21. Kalimantan Barat

23. Kalimantan Selatan
24. Kalimantan Timur
25. Gorontalo
26. Sulawesi Utara
27. Sulawesi Barat
28. Sulawesi Tengah
29. Sulawesi Selatan
30. Sulawesi Tenggara
31. Maluku Utara
32. Maluku
33. Papua Barat
34. Papua

Asal Daerah *

- ○ Kabupaten
- ○ Kota

Nama Kabupaten/Kota *

Short answer text

*

1. Tidak Tamat SD/sederajat
2. Tamat SD/sederajat
3. Tamat SMP/sederajat
4. Tamat SMA/sederajat
5. Tamat Diploma
6. Tamat Sarjana
7. Tamat Pascasarjana

Bidang Pekerjaan *

1. Pelajar/Mahasiswa
2. Pemerintah dan Administrasi Publik
3. Pendidikan
4. Perbankan dan Jasa Keuangan Lainya
5. Teknologi Informasi & Komunikasi
6. Wiraswasta
7. Tidak Bekerja
8. Lainya

Penghasilan Bulanan *

1. Kurang dari Rp. 1.000.000
2. Rp. 1.000.000 - Rp. 2.999.999
3. Rp. 3.000.000 - Rp. 4.999.999
4. Rp. 4.000.000 - Rp. 9.999.999
5. Rp. 10.000.000 - Rp. 19.999.999
6. Rp. 20.000.000 - Rp. 49.999.999
7. Rp. 50.000.000 atau lebih

Level Adopsi Teknologi *

Mana yang paling cocok menggambarkan diri Anda dalam hal perkembangan terbaru di dunia teknologi perangkat bergerak (hp, tablet dan sejenisnya).

- ○ Saya berusaha selalu mengikuti perkembangan terbaru dan seringkali termasuk yang pertama kali men...
- ○ Saya mengikuti kebanyakan orang lain, menunggu beberapa saat sebelum memutuskan untuk menggu...
- ○ Saya tidak mengikuti perkembangan teknologi terbaru dan tidak menggunakannya sampai semua orang...

Merk Smartphone *

Pilih semua yang Anda miliki saat ini, bisa lebih dari satu jika memang Anda memiliki beberapa smartphone Android.

- ☐ Asus
- ☐ Google Pixel
- ☐ Huawei
- ☐ Lenovo

- [ ] Mobicel
- [ ] Motorola
- [ ] Nokia
- [ ] OnePlus
- [ ] OPPO
- [ ] Realme
- [ ] Samsung
- [ ] Vivo
- [ ] Xiaomi
- [ ] Other...

Versi Android di Smartphone Anda *

Pilih semua yang Anda miliki saat ini, bisa lebih dari satu jika memang Anda memiliki beberapa smartphone Android.

- [ ] Android 4.4 KitKat atau versi sebelumnya
- [ ] Android 5 Lollipop
- [ ] Android 6 Marshmallow
- [ ] Android 7 Nougat
- [ ] Android 8 Oreo
- [ ] Android 9 Pie
- [ ] Android 10

Tidak Tahu

Harga Smartphone *

Pilih semua yang Anda miliki saat ini, bisa lebih dari satu jika memang Anda memiliki beberapa smartphone Android.

- [ ] Kurang dari Rp 1.000.000
- [ ] Rp. 1.000.000 - Rp. 2.999.999
- [ ] Rp. 3.000.000 - Rp. 4.999.999
- [ ] Rp. 5.000.000 - Rp. 9.999.999
- [ ] Rp. 10.000.000 atau lebih

After section 3 Continue to next section

Section 4 of 7

Bagian 1

Description (optional)

Backdoor adalah perangkat lunak yang digunakan untuk mengakses sistem, aplikasi, atau jaringan tanpa harus menangani proses autentikasi. Backdoor dapat membantu user yang membuat backdoor (peretas) dapat masuk ke dalam sistem tanpa harus melewati proses autentifikasi. Backdoor juga dapat diartikan sebagai mekanisme yang digunakan untuk mengakses sistem atau jaringan.

Description (optional)

Description (optional)

Smartphone berbasis Android berpotensi mendapatkan serangan berbasis backdoor yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna. *

- Benar
- Salah
- Tidak Tahu

Proses rooting sistem operasi Android dapat meningkatkan risiko serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Penggunaan aplikasi yang tidak diunduh dari Google Play Store atau repository resmi lainnya dapat meningkatkan risiko serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Beberapa smartphone Android tertentu sudah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya. *

Salah

Tidak Tahu

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. *

Benar

Salah

Tidak Tahu

Smartphone yang tidak dikunci dengan lockscreen atau biometrik dapat memperbesar peluang terjadinya serangan berbasis backdoor. *

Benar

Salah

Tidak Tahu

Penggunaan sistem operasi tidak resmi (Custom ROM) dapat memperbesar peluang terjadinya serangan berbasis backdoor. *

Benar

Salah

Tidak Tahu

- Benar
- Salah
- Tidak Tahu

Update aplikasi secara teratur dapat meningkatkan keamanan dari serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Sebelum menginstall suatu aplikasi (termasuk dari Google Play Store atau repository resmi lainnya), perlu dipertimbangkan hak akses apa saja yang dibutuhkannya untuk berjalan. *

- Benar
- Salah
- Tidak Tahu

Pengecekan secara berkala akan hak akses semua aplikasi yang telah terinstall dapat mencegah serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Tidak semua hak akses yang diminta aplikasi perlu diizinkan demi mencegah serangan berbasis backdoor *

- Benar
- Salah
- Tidak Tahu

After section 4 Continue to next section

Section 5 of 7

Bagian 2

Description (optional)

Untuk masing-masing butir pernyataan berikut ini, silakan pilih jawaban yang paling sesuai dengan kondisi Anda.

Description (optional)

Saya sadar bahwa smartphone berbasis Android berpotensi mendapatkan serangan berbasis backdoor yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna. *

- Benar
- Salah
- Tidak Tahu

- Benar
- Salah
- Tidak Tahu

Saya sadar bahwa penggunaan aplikasi tidak diunduh dari Google Play Store atau repository resmi dapat meningkatkan risiko serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Saya sadar bahwa beberapa smartphone Android tertentu sudah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya. *

- Benar
- Salah
- Tidak Tahu

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. *

- Benar
- Salah

Saya sadar bahwa smartphone yang tidak dikunci dengan lockscreen atau biometrik dapat memperbesar peluang terjadinya serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Saya sadar bahwa penggunaan sistem operasi tidak resmi (Custom ROM) dapat membuka peluan lebih besar akan terjadinya serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Saya sadar bahwa update versi sistem operasi Android secara teratur dapat meningkatkan keamanan dari serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Saya sadar bahwa update aplikasi secara teratur dapat meningkatkan keamanan dari serangan berbasis backdoor *

- Benar

Tidak Tahu

Saya sadar untuk mempertimbangkan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum menginstallnya (termasuk dari Google Play Store atau repository resmi lainnya) *

- Benar
- Salah
- Tidak Tahu

Saya sadar untuk melakukan pengecekan secara berkala akan hak akses semua aplikasi yang telah terinstall demi mencegah serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

Saya sadar bahwa tidak semua hak akses yang diminta aplikasi perlu saya berikan demi mencegah serangan berbasis backdoor. *

- Benar
- Salah
- Tidak Tahu

After section 5 Continue to next section

Bagian 3

Description (optional)

Untuk masing-masing butir pernyataan berikut ini, silakan pilih jawaban sesuai dengan kebiasaan Anda.

Description (optional)

Saya terbiasa untuk melakukan langkah-langkah pencegahan atas serangan berbasis backdoor di smartphone Android saya. *

- Benar
- Salah

Saya terbiasa untuk tidak melakukan proses rooting sistem operasi Android. *

- Benar
- Salah

Saya terbiasa untuk tidak menggunakan aplikasi yang tidak diunduh dari Google Play Store atau repository resmi lainnya. *

- Benar
- Salah

Saya terbiasa untuk tidak menggunakan smartphone Android tertentu yang berpotensi telah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya. *

Salah

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. *

Benar

Salah

Saya terbiasa menggunakan lockscreen atau biometrik di smartphone Android saya. *

Benar

Salah

Saya terbiasa untuk tidak menggunakan sistem operasi tidak resmi (Custom ROM) yang bisa memperbesar peluang terjadinya serangan

Multiple choice

Benar

Salah

Add option or add "Other"

Required

Saya terbiasa untuk melakukan update versi sistem operasi Android secara teratur. *

Salah

Saya terbiasa untuk melakukan update aplikasi secara teratur. *

Benar

Salah

Saya terbiasa melakukan pertimbangan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum menginstallnya, termasuk dari Google play Store atau repository resmi lainnya. *

Benar

Salah

Saya terbiasa untuk melakukan pengecekan secara berkala akan hak akses semua aplikasi yang telah terinstall di smartphone saya. *

Benar

Salah

Saya terbiasa untuk tidak begitu saja memberikan semua hak akses yang diminta oleh aplikasi apapun yang berjalan di smartphone saya. *

Benar

Salah

After section 6 Continue to next section

Section 7 of 7

Penutup

Terima kasih atas partisipasi Bapak/Ibu/Saudara/Saudari dalam mengisi survei ini

Semoga penelitian ini dapat bermanfaat untuk kita ketahui seberapa pentingnya kesadaran keamanan ketika menggunakan smartphone Android atau alat digital lainnya.

Jika Anda memiliki masukan untuk penelitian ini, Anda dapat menuliskannya di bagian ini (opsional):

Short answer text

Apabila Anda ingin menarik isian Anda dari penelitian ini, Anda dapat menghubungi saya melalui email di muhammad.akhyari@students.uii.ac.id

Description (optional)

Terima kasih atas partisipasi Bapak/Ibu/Saudara/Saudari dalam mengisi survei ini.

Description (optional)