

**ANALISIS KESADARAN *CYBERSECURITY* PADA  
KALANGAN MAHASISWA DI INDONESIA**



Disusun Oleh:

N a m a : Raja Rizky Riyandhika  
NIM : 16523195

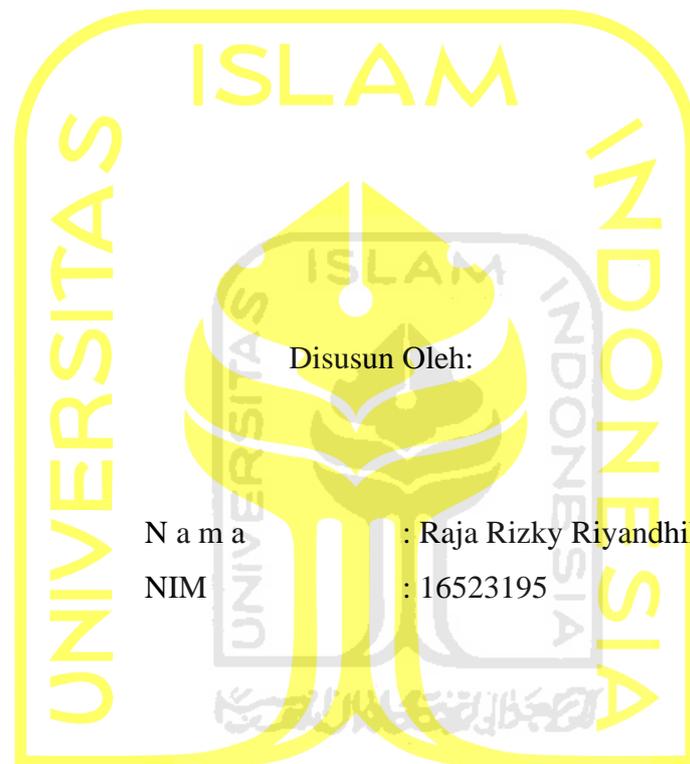
**PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS ISLAM INDONESIA**

**2020**

HALAMAN PENGESAHAN DOSEN PEMBIMBING

**ANALISIS KESADARAN *CYBERSECURITY* PADA  
KALANGAN MAHASISWA DI INDONESIA**

**TUGAS AKHIR**



Disusun Oleh:  
Nama : Raja Rizky Riyandhika  
NIM : 16523195



Yogyakarta, 24 Juli 2020

Pembimbing,

A handwritten signature in blue ink, belonging to the supervisor, Ahmad Munasir Raf'ie Pratama.

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

**HALAMAN PENGESAHAN DOSEN PENGUJI**

**ANALISIS KESADARAN *CYBERSECURITY* PADA  
KALANGAN MAHASISWA DI INDONESIA**

**TUGAS AKHIR**

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

Yogyakarta, 24 Juli 2020

Tim Penguji

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

**Anggota 1**

Andhika Giri Persada, S.Kom., M.Eng.

---

**Anggota 2**

Fayruz Rahma, S.T., M.Eng.

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 : Raja Rizky Riyandhika

NIM : 16523195

Tugas akhir dengan judul:

**ANALISIS KESADARAN *CYBERSECURITY* PADA  
KALANGAN MAHASISWA DI INDONESIA**

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian 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 risiko dan konsekuensi apapun.

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

Yogyakarta, 24 Juli 2020



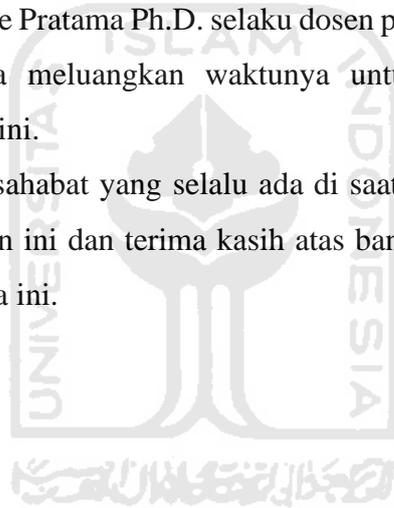
( Raja Rizky Riyandhika )

## HALAMAN PERSEMBAHAN

Segala puji bagi Allah Tuhan semesta alam, atas limpahan rahmat dan karunia yang tiada henti-hentinya kepada saya, sehingga saya masih bisa merasakan nikmat islam, iman, serta nikmat kesehatan hingga saat ini.

Sholawat bertangkaikan salam selalu tercurahkan kepada proklamator keimanan Nabi besar Muhammad shallahu ‘alaihi Wasallam. Yang telah membawa kita menuju zaman yang penuh akan ilmu pengetahuan. Semoga kita termasuk orang-orang yang akan mendapatkan syafaat dari Nabi Muhammad shalallahu “Alaihi Wasallam di hari akhir kelak. Tugas akhir ini saya persembahkan kepada:

1. Orang tua saya Raja Marzuni S.Pd.I dan Wan Hidayati S.Pd dan seluruh keluarga yang telah senantiasa mendukung dan mendoakan saya.
2. Kepada bapak Ahmad Raf'ie Pratama Ph.D. selaku dosen pembimbing pada tugas akhir saya, yang telah bersedia meluangkan waktunya untuk membantu saya dalam menyelesaikan tugas akhir ini.
3. Kepada teman-teman dan sahabat yang selalu ada di saat suka maupun duka selama menjalani masa perkuliahan ini dan terima kasih atas bantuan, nasehat dan pelajaran yang telah diberikan selama ini.



## HALAMAN MOTO

“Dan janganlah kamu berputus asa dari rahmat Allah. Sesungguhnya yang berputus asa dari rahmat Allah, hanyalah orang-orang yang kafir.”

**(Qs. Yusuf: 87)**

"Barang siapa yang bersungguh-sungguh, sesungguhnya kesungguhan tersebut untuk kebaikan dirinya sendiri"

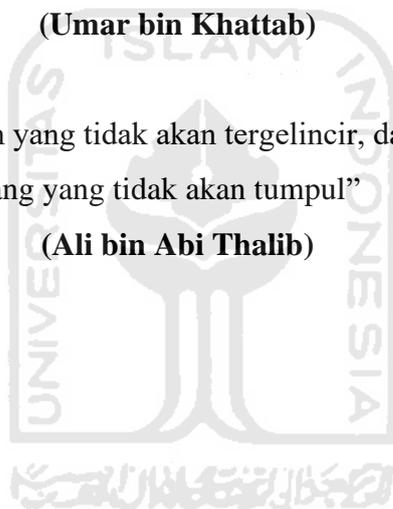
**(Qs. Al-Ankabut: 6)**

“Dunia itu hanyalah cita-cita yang sirna, ajal yang berkurang, dan jalan menuju akhirat serta perjalanan menuju kematian”

**(Umar bin Khattab)**

“Kesabaran adalah kendaraan yang tidak akan tergelincir, dan sikap menerima adalah pedang yang tidak akan tumpul”

**(Ali bin Abi Thalib)**



## KATA PENGANTAR

*Assalamu 'alaikum warahmatullahi Wabarakatuh*

Bismillahirrohmanirrohim, Alhamdulillahirrobbil'alamin, Puji Syukur selalu kami haturkan atas ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis bisa menyelesaikan Tugas Akhir yang berjudul **“Analisis Kesadaran Cybersecurity pada Kalangan Mahasiswa di Indonesia”**

Laporan Tugas Akhir ini dibuat sebagai syarat untuk memperoleh gelar sarjana di Jurusan Informatika Universitas Islam Indonesia. Penulis menyadari bahwa dalam pelaksanaan tugas akhir dan penyusunan laporan ini tidak akan lepas dari bimbingan, dukungan, dan bantuan dari berbagai pihak. Oleh karena itu, perkenankanlah penulis untuk mengucapkan terima kasih dan penghargaan setinggi-tingginya kepada:

1. Allah SWT karena atas RahmatNya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik, dan semoga Tugas Akhir ini dapat memberikan manfaat di kemudian hari.
2. Orang tua dan keluarga penulis atas segala doa dan dukungan selama penulis melaksanakan Tugas Akhir.
3. Bapak Fathul Wahid, S.T., M.Sc., Ph.D., selaku selaku Rektor Universitas Islam Indonesia.
4. Bapak Prof. Dr. Ir. Hari Purnomo selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
5. Bapak Hendrik, ST., M.Sc, selaku Ketua Jurusan Informatika Universitas Islam Indonesia.
6. Bapak Dr. Raden Teduh Dirgahay, S.T., M.Sc. selaku Ketua Program Studi Informatika Program Sarjana Universitas Islam Indonesia.
7. Bapak Ahmad Raf'ie Pratama Ph.D. selaku Dosen Pembimbing Tugas Akhir pada Program Studi Informatika Program Sarjana Universitas Islam Indonesia.
8. Bapak Kholid Haryono S.T., M.Kom. selaku Dosen Pembimbing Akademik pada Program Studi Informatika Program Sarjana Universitas Islam Indonesia

Akhir kata, peneliti berharap agar penelitian ini bisa bermanfaat bagi kemajuan ilmu pengetahuan ke depannya. Peneliti juga menyadari jika penelitian ini masih jauh dari kata sempurna, oleh karena itu peneliti berharap akan ada perbaikan untuk penelitian selanjutnya dan kritik dan saran dari pembaca akan diterima dengan senang hati.

*Wassalamu 'alaikum warahmatullahi Wabarakatuh*

## SARI

*Cybersecurity* adalah sebuah teknologi dan ilmu yang digunakan untuk membantu kita dalam hal menjaga keamanan data kita saat kita sedang berinteraksi dengan Internet, karena saat ini penggunaan Internet pada berbagai kalangan sudah sangat tinggi baik di dunia maupun khususnya di Indonesia. Di antara kalangan yang menggunakan Internet tersebut, kalangan mahasiswa mungkin menjadi kalangan yang paling banyak menggunakan Internet untuk keperluan sehari-hari mereka. Karena banyaknya jumlah pemakaian Internet tersebut maka tingkat kejahatan yang ada di Internet juga semakin banyak dan bervariasi. Hal ini mungkin saja terjadi karena kurangnya kesadaran tentang bahaya yang akan terjadi di Internet maupun cara untuk mengamankan diri mereka dari bahaya yang berada di dunia Internet. Karena hal tersebut, penelitian ini dilakukan untuk mengetahui tingkat kesadaran akan *cybersecurity* yang dimiliki oleh mahasiswa yang ada di Indonesia.

Untuk melakukan pengumpulan data yang diperlukan dalam penelitian ini, peneliti menggunakan metode survei kuesioner yang disebarakan secara online kepada seluruh mahasiswa yang ada di Indonesia. Untuk mengolah data yang sudah didapatkan, peneliti menggunakan dua teknik analisis yaitu teknik analisis deskriptif dan teknik analisis regresi. Penggunaan dari dua teknik analisis tersebut bertujuan untuk bisa menyelesaikan rumusan masalah yang ada.

Hasil dari penelitian ini menunjukkan jika, tingkat kesadaran yang dimiliki oleh mahasiswa di Indonesia sudah relatif tinggi. Faktor yang memengaruhi tingkat kesadaran tersebut ialah faktor jenis kelamin, domisili, uang saku dan usia dari masing-masing mahasiswa tersebut.

Kata kunci: *cybersecurity*, *Struktural Equation Modeling*, pengetahuan, kesadaran, kebiasaan

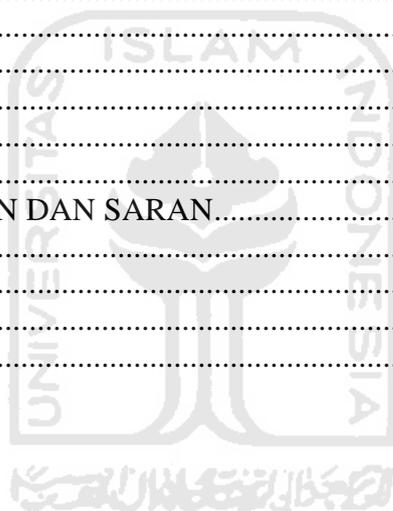
## GLOSARIUM

|                            |   |
|----------------------------|---|
| <i>critical ratio (CR)</i> | Rasio deviasi tertentu dari nilai rata-rata standard deviasi. Nilai ini diperoleh dari estimasi parameter dibagi dengan standard error  |
| <i>Cronbach's alpha</i>    | Sebuah rumus statistik yang digunakan untuk menguji reliabilitas suatu data   |
| <i>Cyber attack</i>        | Sebuah serangan yang dilancarkan oleh peretas untuk menyerang sebuah sistem komputer, yang bertujuan untuk mendapatkan sejumlah keuntungan.   |
| <i>Cybercrime</i>          | Sebuah kejahatan yang ada pada dunia internet   |
| <i>Cybersecurity</i>       | sebuah teknologi, proses dan praktik yang berguna untuk melindungi diri kita dari bahaya <i>cybercrime</i>  |
| HTTPS                      | <i>Hypertext Transfer Protocol Secure</i> adalah suatu system keamanan yang dimiliki pada web.  |
| Kesadaran                  | Sebuah kemauan yang disertai dengan tindakan dari refleksi terhadap kenyataan   |
| Nilai <i>Loading</i>       | Sebuah bobot regresi yang menyatakan relasi setiap indikator terhadap variabel yang dibangun  |
| Pengetahuan                | Sesuatu yang diketahui berdasarkan pengalaman manusia itu sendiri dan pengetahuan tersebut akan bertambah sesuai dengan pengalaman yang dimiliki  |
| <i>p-value</i>             | Nilai peluang terkecil dari suatu pengujian hipotesis   |
| Regresi                    | Suatu metode analisis statistik yang digunakan untuk melihat pengaruh antara dua atau lebih banyak variabel.  |
| SSL                        | <i>Secure Socket Layer</i> adalah suatu sertifikasi keamanan pada web yang apabila system ini ditambahkan pada web maka web tersebut akan berubah menjadi HTTPS.  |
| VPN                        | <i>Virtual Private Network</i> adalah layanan koneksi yang memberikan kita akses ke website secara aman (secure) dan pribadi (private) dengan mengubah jalur koneksi melalui server dan menyembunyikan pertukaran data yang terjadi |

## DAFTAR ISI

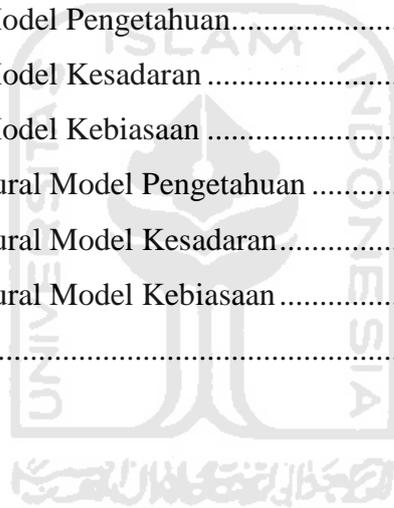
|   |      |
|---|------|
| HALAMAN JUDUL .....                                   | i    |
| HALAMAN PENGESAHAN DOSEN PEMBIMBING.....              | ii   |
| HALAMAN PENGESAHAN DOSEN PENGUJI .....                | iii  |
| HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR .....         | iv   |
| HALAMAN PERSEMBAHAN .....                             | v    |
| HALAMAN MOTO .....                                    | vi   |
| KATA PENGANTAR .....                                  | vii  |
| SARI.....   | viii |
| GLOSARIUM.....  | ix   |
| DAFTAR ISI .....                                      | x    |
| DAFTAR TABEL .....                                    | xii  |
| DAFTAR GAMBAR.....                                    | xiii |
| BAB I PENDAHULUAN .....                               | 1    |
| 1.1 Latar Belakang .....                              | 1    |
| 1.2 Rumusan Masalah .....                             | 2    |
| 1.3 Batasan Masalah .....                             | 2    |
| 1.4 Tujuan Penelitian .....                           | 2    |
| 1.5 Manfaat Penelitian .....                          | 3    |
| 1.6 Sistematika Penulisan .....                       | 3    |
| BAB II LANDASAN TEORI.....                            | 4    |
| 2.1 Kesadaran dan Pengetahuan.....                    | 4    |
| 2.2 Demografi .....                                   | 4    |
| 2.3 <i>Cyberspace</i> .....                           | 5    |
| 2.4 <i>Cybersecurity</i> .....                        | 6    |
| 2.5 <i>Cyber Attack</i> .....                         | 7    |
| 2.6 Teori Analisis Data .....                         | 8    |
| 2.6.1 <i>Exploratory Factor Analysis (EFA)</i> .....  | 9    |
| 2.6.2 <i>Structural Equation Modeling (SEM)</i> ..... | 9    |
| BAB III METODOLOGI.....                               | 12   |
| 3.1 Sampel dan Populasi .....                         | 12   |
| 3.2 Data Primer .....                                 | 12   |
| 3.3 Data Responden .....                              | 13   |
| 3.3.1 Usia.....                                       | 13   |
| 3.3.2 Jenis Kelamin .....                             | 13   |
| 3.3.3 Domisili .....                                  | 14   |
| 3.3.4 Uang Saku .....                                 | 15   |
| 3.3.5 Jenjang Pendidikan.....                         | 15   |
| 3.3.6 Jenis Perguruan Tinggi.....                     | 16   |
| 3.3.7 Jurusan.....                                    | 16   |
| 3.4 Variabel Penelitian .....                         | 17   |
| 3.5 Model dan Indikator Penelitian.....               | 21   |
| 3.6 Hipotesis.....                                    | 24   |
| 3.7 Uji Validitas dan Reliabilitas Data.....          | 26   |
| 3.8 Metode Analisis Data.....                         | 26   |
| 3.8.1 Analisis Statistik Deskriptif.....              | 26   |
| 3.8.2 Analisis Kuantitatif.....                       | 27   |
| BAB IV HASIL DAN PEMBAHASAN .....                     | 28   |

|        |  |    |
|--------|--|----|
| 4.1    | Pengujian Kuesioner .....              | 28 |
| 4.1.1  | Uji Validitas .....                    | 28 |
| 4.1.2  | Uji Reliabilitas.....                  | 30 |
| 4.2    | Uji Hipotesis .....                    | 31 |
| 4.2.1  | Hasil Analisis deskriptif .....        | 31 |
| 4.2.2  | Kesadaran .....                        | 32 |
| 4.2.3  | Pengetahuan.....                       | 33 |
| 4.2.4  | Hasil Uji <i>Goodness of Fit</i> ..... | 35 |
| 4.2.5  | Uji Struktural Model .....             | 36 |
| 4.3    | Pembahasan Hipotesis.....              | 38 |
| 4.3.1  | H1 .....                               | 39 |
| 4.3.2  | H2 .....                               | 39 |
| 4.3.3  | H1.2 .....                             | 39 |
| 4.3.4  | H1.3 .....                             | 40 |
| 4.3.5  | H1.4.....                              | 40 |
| 4.3.6  | H1.7 .....                             | 41 |
| 4.3.7  | H2.1 .....                             | 41 |
| 4.3.8  | H2.2 .....                             | 41 |
| 4.3.9  | H2.3 .....                             | 42 |
| 4.3.10 | H2.4 .....                             | 42 |
| 4.3.11 | H3.1 .....                             | 43 |
| 4.3.12 | H3.4.....                              | 43 |
| 4.3.13 | H3.6 .....                             | 44 |
|        | BAB V KESIMPULAN DAN SARAN.....        | 45 |
| 5.1    | Kesimpulan .....                       | 45 |
| 5.2    | Saran.....                             | 45 |
|        | DAFTAR PUSTAKA .....                   | 47 |
|        | LAMPIRAN .....                         | 49 |



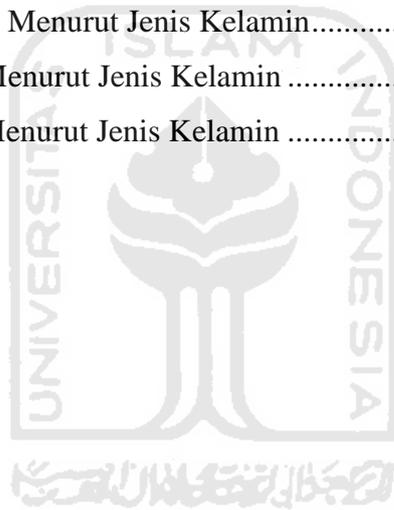
## DAFTAR TABEL

|  |    |
|--|----|
| Tabel 3. 1 Tabel Skala Likert.....                             | 12 |
| Tabel 3. 2 Hasil Analisis Factor Kebiasaan .....               | 18 |
| Tabel 3. 3 Hasil Analisis Factor Kesadaran.....                | 18 |
| Tabel 3. 4 Hasil Analisis Factor Pengetahuan .....             | 19 |
| Tabel 3. 5 Metode Pengubah Data .....                          | 21 |
| Tabel 4. 1 Hasil Uji Validitas .....                           | 28 |
| Tabel 4. 2 Hasil Uji Reliabilitas.....                         | 30 |
| Tabel 4. 3 Tabel Pengelompokan Skala Likert.....               | 31 |
| Tabel 4. 4 Hasil Analisis Deskriptif Kesadaran.....            | 32 |
| Tabel 4. 5 Hasil Analisis Deskriptif Pengetahuan .....         | 34 |
| Tabel 4. 6 Kriteria Goodness of Fit .....                      | 35 |
| Tabel 4. 7 Hasil Goodness of Fit Model Pengetahuan.....        | 35 |
| Tabel 4. 8 Hasil Goodness of Fit Model Kesadaran .....         | 35 |
| Tabel 4. 9 Hasil Goodness of Fit Model Kebiasaan .....         | 36 |
| Tabel 4. 10 Hasil Pengujian Struktural Model Pengetahuan ..... | 36 |
| Tabel 4. 11 Hasil Pengujian Struktural Model Kesadaran.....    | 37 |
| Tabel 4. 12 Hasil Pengujian Struktural Model Kebiasaan.....    | 37 |
| Tabel 4. 13 Status Hipotesis.....                              | 38 |



**DAFTAR GAMBAR**

|  |    |
|--|----|
| Gambar 3. 1 Diagram Usia .....                             | 13 |
| Gambar 3. 2 Diagram Jenis Kelamin .....                    | 14 |
| Gambar 3. 3 Diagram Domisili.....                          | 14 |
| Gambar 3. 4 Diagram Uang Saku .....                        | 15 |
| Gambar 3. 5 Diagram Jenjang Pendidikan .....               | 16 |
| Gambar 3. 6 Diagram Jenis Perguruan Tinggi.....            | 16 |
| Gambar 3. 7 Diagram Jurusan .....                          | 17 |
| Gambar 3. 8 Hasil Faktor Kebiasaan .....                   | 20 |
| Gambar 3. 9 Hasil Faktor Kesadaran .....                   | 20 |
| Gambar 3. 10 Hasil Faktor Pengetahuan .....                | 20 |
| Gambar 4. 1 Diagram Pengetahuan Menurut Jenis Kelamin..... | 40 |
| Gambar 4. 2 Diagram Kesadaran Menurut Jenis Kelamin .....  | 42 |
| Gambar 4. 3 Diagram Kebiasaan Menurut Jenis Kelamin .....  | 43 |



## BAB I PENDAHULUAN

### 1.1 Latar Belakang

Pada saat ini Internet sudah menjadi hal pokok yang sangat dibutuhkan oleh semua orang di seluruh dunia dan tak terkecuali di Indonesia, semua orang pada saat ini sudah menggunakan Internet baik dari kalangan anak – anak, dewasa bahkan lansia sekalipun sudah menggunakan Internet. Menurut data yang dirilis Perserikatan Bangsa – Bangsa (PBB) pada tahun 2018 saat ini ada 3,9 miliar orang atau lebih dari populasi dunia yang sudah menggunakan Internet. Komisi Telekomunikasi Internasional (*International Telecommunication Union/ ITU*) memprediksi pada akhir tahun 2018 pengguna Internet mencapai 51,2 persen dari seluruh populasi dunia. Di Indonesia sendiri jumlah pengguna Internet pada Maret 2019 sudah mencapai 143,26 juta pengguna yang membawa Indonesia menjadi negara dengan jumlah pengguna Internet terbesar ke-5 di dunia. (CNN, 2018). Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), di Indonesia sendiri jumlah pengguna Internet pada periode Maret hingga April 2019 sudah mencapai 171,17 juta pengguna atau sekitar 64,8 penduduk Indonesia yang sudah terkoneksi dengan Internet (APJII, 2019)

Menurut Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) pada tahun 2014 mencatat bahwa terdapat 48,8 juta serangan siber yang ada di Indonesia yang disebabkan oleh adanya aktivitas *malware* 12.007.808 insiden yang meliputi 24.168 kasus kebocoran keamanan, kebocoran rekam jejak atau *record leakage* sebanyak 5.970 kasus, serangan melalui *password* harvesting sebanyak 1.730 kasus, dan serangan akibat kebocoran domain sebanyak 215 kasus.

Dari banyaknya jumlah serangan tersebut, kerugian yang dihasilkan dari penyerangan tersebut juga sangatlah besar. Di Indonesia sendiri kerugian yang dicapai akibat serangan siber tersebut mencapai *USD 895 billion* yang mana nilai ini mencapai 1,20% dari total kerugian di seluruh dunia yang mencapai *USD 71,620 billion*. (Ardiyanti, 2014)

Data diatas bisa kita ketahui bahwa Internet sudah menjadi kebutuhan yang penting bagi seluruh kalangan manusia di dunia baik itu anak-anak, pemuda, maupun lansia sekalipun. Dari semua kalangan yang menggunakan Internet di dunia khususnya di Indonesia tidak bisa kita pungkiri bahwa kalangan yang paling banyak menggunakan dan sangat membutuhkan Internet saat ini adalah dari kalangan mahasiswa. Dari banyaknya jumlah pengguna Internet di kalangan

mahasiswa tersebut, jumlah kejahatan yang terjadi di dunia Internet atau dikenal sebagai *cybercrime* juga semakin banyak terjadi. Hal ini mungkin saja terjadi karena kurangnya tentang bahaya yang akan terjadi di Internet maupun cara untuk mengamankan diri mereka dari bahaya yang berada di dunia Internet.

Dari banyaknya jumlah pengguna Internet dari kalangan mahasiswa itulah yang membuat peneliti tertarik untuk melakukan penelitian dengan judul “Analisis Kesadaran *Cybersecurity* pada Kalangan Mahasiswa di Indonesia”. Penelitian ini bertujuan untuk melihat tingkat kesadaran, pengetahuan dan kebiasaan yang dimiliki mahasiswa di Indonesia dalam berinteraksi dengan dunia Internet tersebut.

## 1.2 Rumusan Masalah

Dari uraian latar belakang diatas, peneliti mengajukan permasalahan pada penelitian ini sebagai berikut:

1. Bagaimana tingkat kesadaran dan pengetahuan tentang *cybersecurity* pada kalangan mahasiswa di Indonesia
2. Faktor apa saja yang memengaruhi kesadaran dan pengetahuan yang dimiliki mahasiswa di Indonesia.
3. Bagaimana faktor kesadaran dan pengetahuan bisa berpengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa di seluruh Indonesia

## 1.3 Batasan Masalah

- a. Responden dari penelitian ini hanya dari kalangan mahasiswa di Indonesia
- b. Penelitian yang dilakukan hanya sebatas untuk mengetahui tingkat kesadaran *cybersecurity* mahasiswa yang ada di Indonesia
- c. Hasil penelitian memungkinkan terjadinya perbedaan tingkat kesadaran *cybersecurity* di sejumlah daerah di Indonesia

## 1.4 Tujuan Penelitian

- a. Melihat bagaimana tingkat kesadaran dan pengetahuan pada kalangan mahasiswa di Indonesia tentang *cybersecurity*
- b. Melihat faktor apa saja yang memengaruhi kesadaran dan pengetahuan yang dimiliki mahasiswa di Indonesia.

- c. Melihat apakah faktor kesadaran dan pengetahuan bisa berpengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa di seluruh Indonesia

### 1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini antara lain:

- a. Mengetahui tingkat kesadaran mahasiswa di Indonesia tentang *cybersecurity*
- b. Mengetahui faktor apa saja yang bisa memengaruhi tingkat kesadaran mahasiswa di Indonesia tentang *cybersecurity*
- c. Sebagai pengembangan ilmu pengetahuan tentang *cybersecurity* dan dapat digunakan sebagai referensi untuk penelitian selanjutnya

### 1.6 Sistematika Penulisan

Untuk mempermudah dalam penulisan tugas akhir ini, peneliti membagi penyusunannya menjadi 5 bab yaitu:

**Bab I Pendahuluan** bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian dan sistematika penulisan yang digunakan dalam penelitian ini

**Bab II Landasan Teori** bab ini menjelaskan landasan teori yang dipakai pada penelitian ini dan juga berisi uraian tentang dasar teori yang digunakan pada penelitian ini.

**Bab III Metodologi** bab ini menjelaskan tentang metode yang akan digunakan dalam proses penelitian ini dan menguraikan langkah-langkah yang dijalankan untuk menyelesaikan penelitian.

**Bab IV Hasil dan Pembahasan** pada bab ini akan dijelaskan hasil yang didapatkan pada penelitian yang telah dilakukan sebelumnya.

**Bab V Kesimpulan dan Saran** bab ini berisi tentang kesimpulan yang didapat pada penelitian yang sudah dilakukan dan juga saran perbaikan agar terciptanya hasil yang lebih baik lagi untuk penelitian selanjutnya.

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Kesadaran dan Pengetahuan**

Menurut Kamus Besar Bahasa Indonesia (KBBI), kesadaran adalah keinfasan, keadaan mengerti, hal yang dirasakan atau yang dialami oleh seseorang. Menurut Freira (2002) “kesadaran merupakan sebuah kemauan yang disertai dengan tindakan dari refleksi terhadap kenyataan”. Sementara itu, kesadaran tentang *cybersecurity* adalah tingkat pemahaman pengguna tentang bagaimana pentingnya untuk menjaga keamanan informasi mereka serta melakukan kontrol terhadap keamanan informasi tersebut demi melindungi keamanan data mereka (Shaw, Chen, Harris, & Huang, 2009).

Pengetahuan adalah sesuatu yang diketahui berdasarkan pengalaman manusia itu sendiri dan pengetahuan tersebut akan bertambah sesuai dengan pengalaman yang dimiliki (Mubarak, 2011). Menurut Kamus Besar Bahasa Indonesia (KBBI) pengetahuan berasal dari kata “tahu” yang artinya mengerti sesudah melihat (menyaksikan, mengalami, dan sebagainya). Bisa disimpulkan jika pengetahuan merupakan segala sesuatu yang berasal dari pengalaman yang bisa dilihat, disaksikan dan dialami oleh manusia itu sendiri dan pengetahuan tersebut akan terus bertambah seiring dengan bertambahnya pengalaman.

#### **2.2 Demografi**

Demografi berasal dari kata Yunani yaitu “*demos*” yang berarti rakyat atau penduduk dan “*graphein*” yang berarti melukis. Dalam Kamus Besar Bahasa Indonesia (KBBI) demografi merupakan suatu bidang ilmu yang berisi tentang susunan, jumlah, dan perkembangan penduduk yang dilihat dari sudut pandang sosial politik dan ilmu kependudukan. Menurut Achille Guillard demografi adalah sebuah ilmu yang segala sesuatu dari keadaan dan sikap manusia yang dapat diukur. Demografi juga merupakan gambaran penduduk dari suatu tempat tertentu.

Dalam penelitian ini peneliti akan mengambil beberapa aspek demografi yang akan digunakan pada penelitian ini yaitu:

- a. **Usia** yaitu lamanya seorang individu hidup yang terhitung dari dia lahir sampai dengan sekarang.

- b. **Jenis Kelamin** adalah sebuah pembagian dua jenis kelamin yang ditentukan secara biologis.
- c. **Domisili** adalah sebuah tempat tinggal yang sah dan dijadikan tempat kediaman oleh individu tersebut.
- d. **Uang Saku** umumnya diartikan sebagai uang diberikan (disediakan) untuk dibelanjakan sewaktu-waktu (Departemen Pendidikan Nasional, 2008:1512), hal ini biasanya diterima oleh anak-anak yang masih belum memiliki penghasilan.
- e. **Jenjang Pendidikan** ialah tingkat pendidikan terakhir yang telah dilalui oleh seorang individu.
- f. **Jenis Perguruan Tinggi** adalah jenis perguruan tinggi yang mereka pilih untuk studi mereka.
- g. **Jurusan** ialah jenis jurusan apa yang mereka pilih dalam melakukan studi mereka.

### 2.3 Cyberspace

*Cyberspace* atau dunia siber ialah sebuah media elektronik dalam jaringan komputer yang digunakan untuk melakukan komunikasi satu atau dua arah secara online. Menurut John Perry (1990) dunia siber diaplikasikan hanya untuk dunia yang terhubung atau online ke Internet. Dunia siber ini berfungsi sebagai penghubung dari berbagai peralatan elektronik dan komunikasi yang tersebar di seluruh dunia.

*Cyberspace* merupakan sebuah ruang yang tidak dapat dilihat yang tercipta dari terjadinya hubungan komunikasi, yang ditujukan untuk menyebarkan informasi dan tidak terpengaruh oleh jarak secara fisik (Chairisda, 2020).

Istilah dari *Cyberspace* sendiri, pertama kali digunakan oleh William Gibson dalam novelnya yang berjudul *Neuromancer* yang terbit pada tahun 1984, dalam novel tersebut William mengibaratkan jika dunia siber dan dunia nyata itu ibaratnya seperti 2 sisi koin logam, yang mana keduanya adalah dunia yang tidak bisa dipisahkan satu sama lain (Joanna Buick, 1997).

Dengan adanya dunia baru yang bernama *cyberspace* ini pun, ada juga berbagai macam kejahatan yang mengancam jika kita tidak berhati-hati jika sedang berada dalam dunia tersebut. Untuk melindungi diri kita dari risiko tersebut maka muncullah sebuah teknologi atau ilmu yang berguna untuk melindungi diri kita dari berbagai macam kejahatan yang ada di dunia tersebut, dan teknologi itu bernama *cybersecurity*.

## 2.4 Cybersecurity

Pada saat ini penggunaan Internet di seluruh dunia khususnya di Indonesia sudah sangat banyak dan sudah menjadi kebutuhan pokok manusia di dunia pada saat ini, dari banyaknya jumlah pengguna Internet pada saat ini banyak pula terjadi serangkaian kejahatan-kejahatan di Internet yang disebut juga dengan *cybercrime*. Untuk mencegah terjadinya tindak kejahatan di Internet ada sebuah teknologi atau bidang ilmu yang berguna untuk melindungi diri kita dari bahaya *cybercrime* yang bisa kita sebut sebagai *cybersecurity*

*Cybersecurity* adalah sebuah teknologi, proses dan praktik yang berguna untuk melindungi diri kita dari bahaya *cybercrime*, *cybersecurity* dirancang untuk melindungi jaringan, komputer, program, dan data kita dari sejumlah serangan yang dilancarkan oleh orang yang tidak bertanggung jawab untuk mendapatkan keuntungan dari apa yang mereka dapat dari komputer kita, terutama data penting yang ada di dalam komputer, jaringan, dan program kita.

*Cybersecurity* sendiri memiliki pengertian yang sangat luas tetapi didasari dari 3 konsep dasar yang disebut sebagai *The CIA Triad*, konsep ini terdiri dari:

### A. Confidentiality

*Confidentiality* atau kerahasiaan merupakan sebuah aturan yang membatasi akses yang dimiliki seseorang atau organisasi agar informasi tersebut tidak dapat diakses oleh orang lain.

### B. Integrity

atau disebut juga integritas ialah bagaimana kita bisa memastikan data yang kita miliki itu konsisten, akurat, dan dapat dipercaya selama periode tertentu. Hal ini berarti sebuah data tidak bisa diubah, dihapus ataupun diakses secara ilegal

### C. Availability

Atau disebut juga ketersediaan, ketersediaan disini ialah mencakup ketersediaan perangkat keras, perangkat lunak, dan jaringan yang harus dipelihara dan ditingkatkan performanya agar bisa melindungi data kita secara maksimal

Melindungi informasi yang terdapat pada komputer kita sudah menjadi hal yang sangat penting sekarang baik dari segi individu hingga ke sebuah organisasi atau perusahaan yang pasti memiliki data penting yang tidak boleh bocor ke luar organisasi atau perusahaan terkait. Maka dari itu penggunaan teknologi *cybersecurity* menjadi sangat penting untuk melindungi data berharga yang dimiliki individu, organisasi, maupun perusahaan.

## 2.5 *Cyber Attack*

*Cyber attack* adalah sebuah serangan yang dilancarkan oleh peretas untuk menyerang sebuah sistem komputer perseorangan atau organisasi, yang bertujuan untuk mendapatkan sejumlah keuntungan dari korban yang diretas.

Saat ini jenis-jenis *cyber attack* sudah semakin canggih dan bervariasi seiring berkembangnya teknologi informasi, ada beberapa jenis serangan *cyber* biasa disebut dengan *cyber attack* yang ada saat ini yaitu:

- *Phishing*

Merupakan sebuah usaha kejahatan untuk mencuri data pengguna seperti nomor kartu kredit, *password* atau data penting lainnya dengan menggunakan sebuah skema atau cara dengan menjadi sosok atau individu yang dipercaya pengguna dan kemudian menyuruh pengguna untuk membuka sebuah pesan teks, email, atau pesan instan yang bisa menyebabkan pembekuan sistem sebagai bagian dari serangan *ransomware*, membuka informasi pengguna, atau pemasangan *malware* pada sistem korban. Hal ini dapat menyebabkan kerugian pada pengguna berupa pencurian identitas, pencurian data, atau pembelian tanpa izin.

- *Malware*

Merupakan sebuah kode program yang dibuat untuk memengaruhi sistem komputer yang disusupi tanpa sepengetahuan pengguna. *Malware* bisa sangat berbahaya karena bisa menyebar melalui jaringan Internet yang bisa menyebabkan perubahan dan kerusakan pada sistem tetapi tidak bisa terdeteksi.

- *Worms*

Adalah sebuah program mandiri yang bisa menyebar melalui jaringan dan komputer, biasanya worms menyebar melalui sebuah lampiran email, membuka lampiran yang ada pada sebuah *website*. *Worms* bisa menyebabkan serangan penolakan layanan terhadap *node* pada jaringan.

- *Ransomware*

Merupakan sebuah jenis serangan yang memblokir pengguna untuk mengakses data pengguna itu sendiri dan biasanya pelaku akan meminta uang tebusan supaya pengguna bisa

mengakses datanya lagi. Serangan ini sudah menyebabkan kerugian bagi pengguna Internet di seluruh dunia tak terkecuali di Indonesia.

- *Trojan Horse*

Merupakan sebuah program berbahaya yang bisa membuat seolah dirinya itu berguna bagi sistem. Trojan menyebar melalui jaringan dengan cara terlihat seperti *software* rutin sehingga dapat mengelabui pengguna untuk meng-*install* aplikasi tersebut. Trojan dianggap berbahaya karena bisa mencuri informasi keuangan pengguna.

- *Denial of Service (DDoS)*

Merupakan sebuah serangan terhadap komputer yang dapat menghabiskan *resource* yang dimiliki oleh komputer sehingga komputer tersebut tidak bisa lagi melayani atau menjalankan fungsinya dengan benar sehingga pengguna tidak dapat lagi mengakses komputer tersebut.

Ada beberapa cara yang bisa digunakan penyerang untuk melumpuhkan sistem yang akan diakses oleh pengguna.

Yang pertama yaitu dengan membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. teknik ini disebut sebagai *traffic flooding*.

Yang kedua yaitu dengan membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. teknik ini disebut sebagai *request flooding*.

Cara yang ketiga yaitu dengan mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan merusak fisik terhadap komponen dan server.

## 2.6 Teori Analisis Data

Saat merencanakan penelitian, peneliti sudah harus mempersiapkan teknik analisis data yang akan digunakan untuk pemeriksaan data, pembuatan kode dan penyusul tabel (Wahyuni,dkk.,2006). Analisis hubungan adalah bentuk analisis variabel yang bertujuan untuk mengetahui derajat atau kekuatan hubungan antar variabel dan besarnya pengaruh yang dimiliki antara variabel independen terhadap variabel dependen (Hasan, 2004).

Dalam penelitian ini teknik yang digunakan untuk melakukan analisis hubungan ialah teknik analisis regresi linear yang mana teknik tersebut adalah *Exploratory Factor Analysis*

(EFA) untuk mencari relasi yang dimiliki antar variabel dan menentukan faktor yang akan digunakan untuk menentukan model yang digunakan pada teknik analisis selanjutnya yaitu teknik analisis *Structural Equation Modeling* (SEM).

### 2.6.1 *Exploratory Factor Analysis (EFA)*

*Exploratory Factor Analysis* atau EFA adalah sebuah model yang digunakan dalam melakukan explorasi data yang ada untuk melihat karakteristik dan hubungan yang dimiliki data tersebut. Dalam *statistic multivariat*, EFA adalah sebuah metode statistik yang bertujuan untuk membentuk faktor dari sekumpulan variabel yang banyak, EFA juga sering digunakan dalam melakukan penelitian untuk mencari sebuah struktur yang ada pada sebuah variabel, metode ini sering juga disebut reduksi data. EFA juga mampu menelusuri korelasi yang dimiliki pada sebuah data aktual.

EFA juga salah satu analisis faktor yang bertujuan untuk mengidentifikasi hubungan antar variabel manifes atau variabel indikator dalam membangun sebuah konstruk. Metode ini digunakan dalam situasi jika peneliti belum mengetahui informasi atau hipotesis yang diperlukan untuk menentukan kelompok dari masing-masing indikator variabel (Finch & West, 1997).

Nilai faktor *loading* dari suatu variabel akan menjadi patokan dalam menentukan hubungan yang dimiliki oleh masing-masing variabel tersebut, ketika nilai *loading* dari suatu variabel lebih besar terhadap faktor tertentu, maka variabel tersebut bisa dikelompokkan ke dalam faktor tersebut.

### 2.6.2 *Structural Equation Modeling (SEM)*

*Structural Equation Modeling* (SEM) merupakan suatu teknik statistik yang memiliki kemampuan untuk melakukan analisis terhadap pola hubungan yang dimiliki suatu variabel laten terhadap indikatornya. Metode ini adalah hasil dari pengembangan dari analisis multivariat yaitu analisis faktor dan regresi.

Menurut Latan (2012 :1), terciptanya perangkat lunak SEM berasal dari dikembangkannya *analysis covariance* oleh Joreskog (1973), Keesling (1972) dan Wiley (1973). Perangkat lunak SEM pertama yang dihasilkan adalah LISREL (*Linear Structural Relationship*) yang dikembangkan oleh Joreskog dan Dag Sorbom pada tahun 1974. Tujuan utama dari pengembangan perangkat lunak SEM saat itu ialah untuk menghasilkan suatu

perangkat untuk melakukan analisis yang lebih *powerfull* dan dapat menjawab berbagai masalah riset yang lebih substantif dan komprehensif.

SEM merupakan gabungan dari dua metode analisis statistik yang terpisah yaitu analisis faktor yang dikembangkan dalam psikologi dan psikometri, dan model persamaan simultan (*simultaneous equation modeling*) yang dikembangkan dalam ekonometrika (Ghozali, 2008).

Secara umum, SEM dapat digunakan untuk menganalisis model penelitian yang memiliki banyak variabel independen dan variabel dependen.

Untuk lebih khusus menurut Latan (2012), Ghozali (2008), Jogiyanto (2011) dan Wijaya (2009) ada beberapa manfaat yang bisa didapatkan jika kita menggunakan SEM dalam melakukan analisis, seperti:

1. Dapat membangun model penelitian dari banyak variabel
2. Dapat meneliti sebuah variabel yang tidak bisa teramati atau diukur secara langsung
3. Menguji kesalahan pengukuran untuk variabel atau konstruk yang sudah teramati
4. Mengonfirmasi teori yang digunakan sudah sesuai dengan data yang digunakan pada penelitian
5. Dapat menjawab berbagai macam masalah dalam penelitian secara lebih sistematis dan komprehensif
6. Lebih ilustratif, kokoh dan handal dibanding dengan model regresi dalam memodelkan interaksi, *non-linieritas*, pengukuran kesalahan, korelasi *error terms*, dan korelasi antar variabel laten independen berganda
7. Melakukan analisis faktor, jalur dan regresi
8. Memiliki fleksibilitas yang lebih tinggi bagi peneliti dalam menggabungkan teori dengan data yang digunakan

Ada dua jenis SEM yang bisa digunakan untuk melakukan penelitian bagi para peneliti yaitu:

#### A. *Covariance Based Structural Equation Modeling* (CB-SEM)

CB-SEM pertama kali dikembangkan oleh Joreskog (1973), Keesling (1972) dan Wiley (1973), dan jenis ini mulai digunakan pada tahun 1970-an setelah Joreskog dan Sorbom mengembangkan sebuah program yang bernama LISREL III (Ghozali, 2008). Fungsi dari CB-SEM ini ialah untuk meminimumkan perbedaan antara *covariance matrix* sampel dengan *covariance matrix* prediksi oleh model yang teoritis, sehingga proses estimasi menghasilkan *residual covariance matrix* yang nilainya mendekati nol.

## A. *Variance atau Component Based SEM* (VB-SEM)

### a. PLS-SEM

Ialah sebuah model yang bertujuan untuk menguji sebuah hubungan prediktif antar konstruk dengan melihat apakah ada hubungan atau pengaruh yang dimiliki antar variabel tersebut.

### b. GSCA

Model ini adalah hasil dari gabungan karakteristik yang dimiliki pada CB-SEM dengan PLS-SEM, GSCA dapat memproses sebuah variabel laten dengan banyak indikator seperti PLS-SEM, dan mensyaratkan kriteria *goodness of fit* yang dimiliki model serta indikator dan konstruknya harus berkorelasi seperti CB-SEM.

Model ini memiliki tujuan yang sama seperti PLS-SEM, yang mana tidak mensyaratkan asumsi *multivariate normality data*. Juga bisa melakukan pengujian tanpa dasar teori yang kuat dengan jumlah sampel yang kecil.



## BAB III METODOLOGI

### 3.1 Sampel dan Populasi

Pengambilan sampel pada penelitian ini menggunakan metode survei kuesioner yang telah dibuat oleh peneliti dan disebarakan secara *online* oleh peneliti. Metode survei kuesioner ialah sebuah teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan kepada responden untuk dijawab (Sugiyono, 2008). Proses pengambilan data dilakukan secara acak yang bertujuan untuk dijadikan ukuran dalam menentukan populasi atau generalisasi

Populasi dalam penelitian ini adalah seluruh mahasiswa yang ada di Indonesia dan pengambilan sampel ini akan dilakukan secara *random sampling*. Karena teknik yang digunakan untuk melakukan analisis ini adalah teknik SEM maka sampel yang diperlukan atau disarankan minimal sebanyak 100 – 200 sampel (E. J. Wolf, 2013). Sampel yang berhasil didapatkan dalam proses pengumpulan data sebelumnya adalah 387, dan hasil tersebut telah berhasil memenuhi jumlah yang harus dipenuhi untuk menerapkan teknik SEM.

### 3.2 Data Primer

Data yang digunakan pada penelitian ini adalah data yang dihasilkan dari proses survei kuesioner yang disebarakan secara *online* kepada mahasiswa yang ada di seluruh Indonesia. Skala yang digunakan di dalam kuesioner yang disebarakan adalah skala Likert, skala ini berfungsi untuk mengukur nilai yang ada pada variabel penelitian. Bobot nilai dari skala Likert yang dipakai pada penelitian ini adalah, 5 sebagai bobot nilai paling tinggi sedangkan 1 sebagai bobot nilai paling rendah. Lebih jelasnya bisa dilihat pada tabel 3.1 berikut:

Tabel 3. 1 Tabel Skala Likert

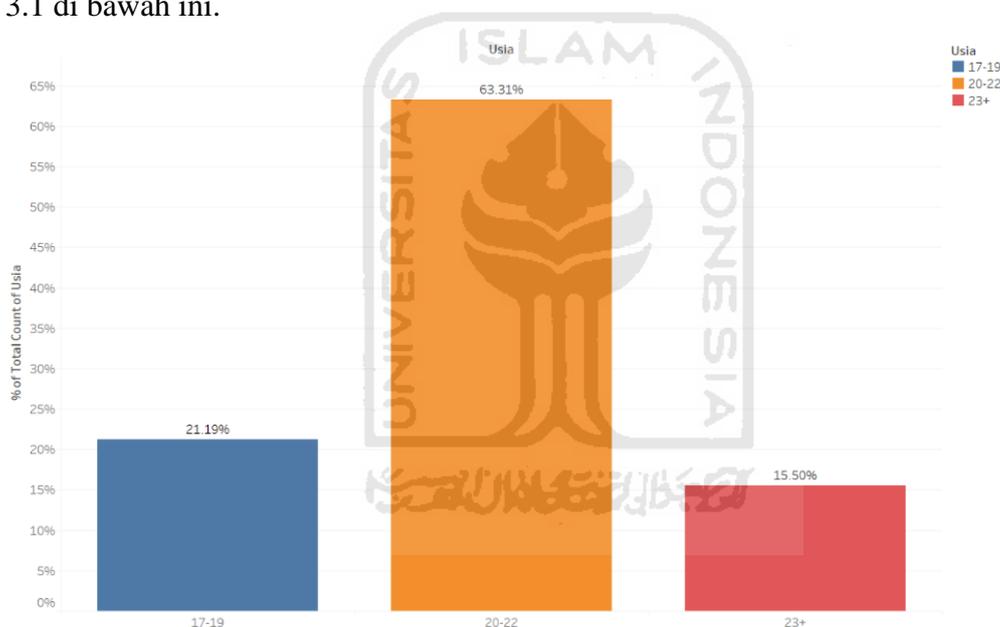
| No | Jawaban             | Kode | Bobot |
|----|---------------------|------|-------|
| 1  | Sangat Tidak Setuju | STS  | 1     |
| 2  | Tidak Setuju        | TS   | 2     |
| 3  | Netral              | N    | 3     |
| 4  | Setuju              | S    | 4     |
| 5  | Sangat Setuju       | SS   | 5     |

### 3.3 Data Responden

Populasi dari data yang didapatkan adalah seluruh mahasiswa yang ada di Indonesia dan tidak ada batas umur dalam pengisian kuesioner ini. Kuesioner disebarakan melalui Google Forms dan berhasil mengumpulkan sebanyak 387 responden. Peneliti menggunakan aplikasi Tableau untuk melakukan visualisasi pada data, dengan tujuan untuk mempermudah melihat komposisi data yang akan digunakan untuk melakukan analisis selanjutnya.

#### 3.3.1 Usia

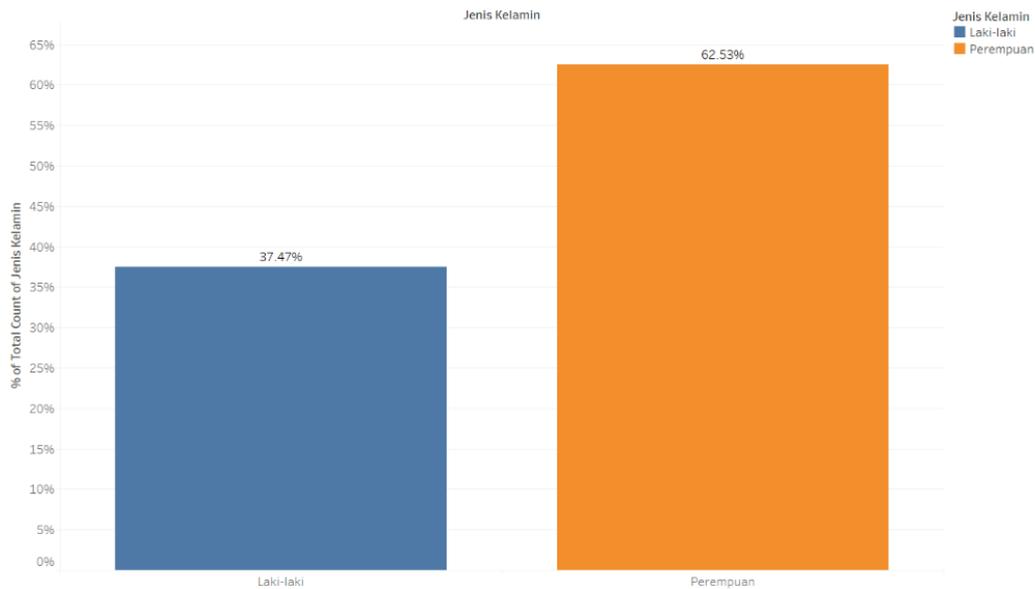
Dari data yang didapatkan, rentang usia responden adalah 17 hingga 50 tahun dengan nilai rerata 21 tahun dan simpangan baku 3 tahun. Peneliti mengelompokkan usia responden menjadi 3 kelompok yaitu 17-19, 20-22, dan 23+. Untuk lebih lengkapnya bisa dilihat pada gambar 3.1 di bawah ini.



Gambar 3. 1 Diagram Usia

#### 3.3.2 Jenis Kelamin

Dari data jenis kelamin yang berhasil dikumpulkan data yang dominan adalah data perempuan yang berjumlah 62% dari total data yang terkumpul. Untuk lebih jelas bisa dilihat pada gambar 3.2 di bawah ini.



Gambar 3. 2 Diagram Jenis Kelamin

### 3.3.3 Domisili

Pada data domisili peneliti mengelompokkan domisili menjadi 2 kelompok yaitu kelompok domisili yang berada di Pulau Jawa dan kelompok domisili yang berada di luar Pulau Jawa.

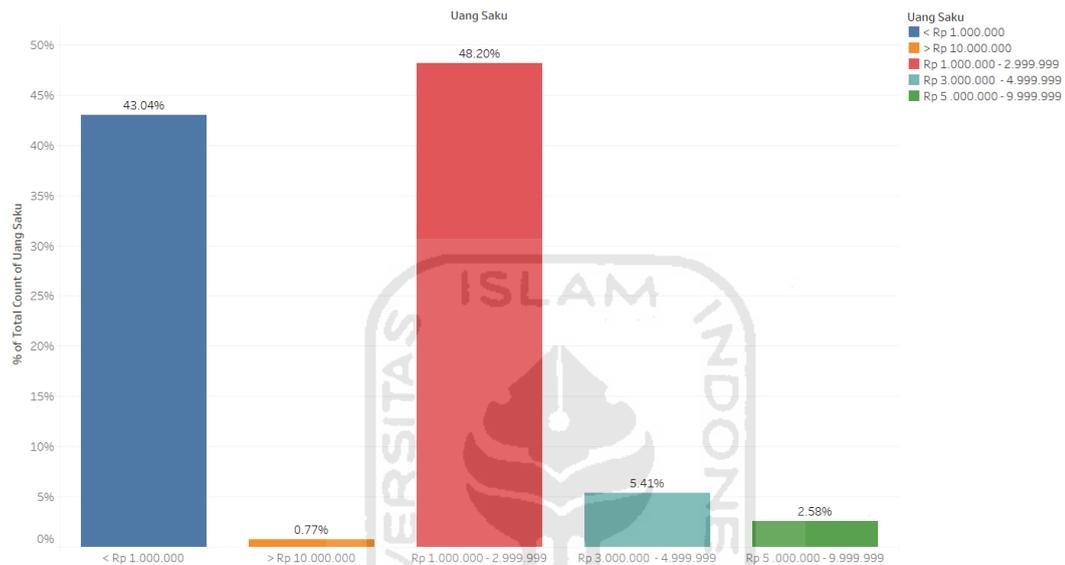
Responden yang menjadi dominan dalam survei ini adalah responden yang berdomisili di Pulau Jawa yang berjumlah 65%, sedangkan yang berada di luar Jawa adalah sekitar 35%. Untuk lebih lengkapnya bisa dilihat pada gambar 3.3 di bawah ini.



Gambar 3. 3 Diagram Domisili

### 3.3.4 Uang Saku

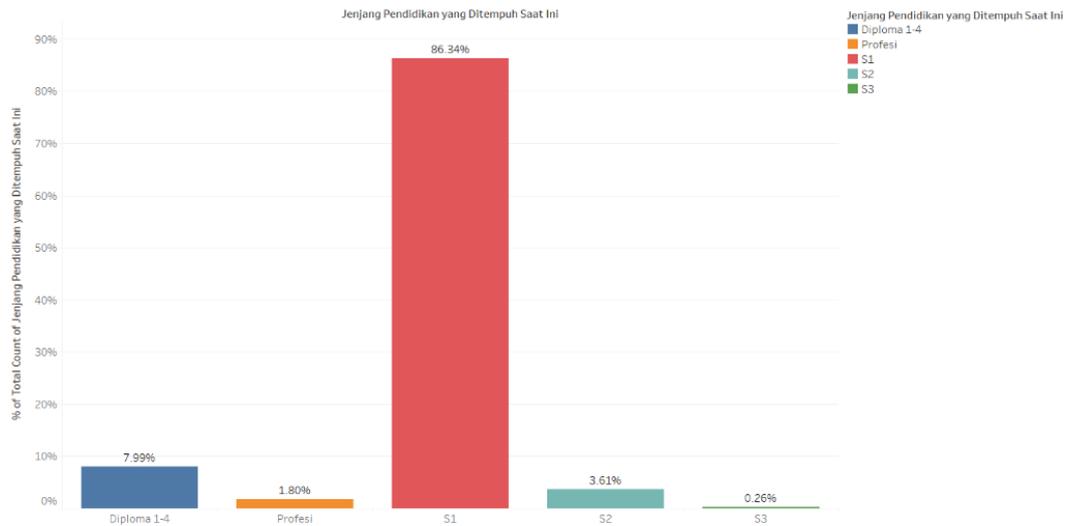
Dari hasil survei yang berhasil dikumpulkan dapat dilihat jika kebanyakan mahasiswa yang mengisi responden ini memiliki uang saku senilai Rp1-3 juta karena data yang ditunjukkan bahwa mahasiswa yang mendapat uang saku Rp1-3 juta per bulannya mencapai 57% dari total data yang didapatkan. Untuk lebih lengkapnya bisa dilihat pada gambar 3.4 di bawah ini.



Gambar 3. 4 Diagram Uang Saku

### 3.3.5 Jenjang Pendidikan

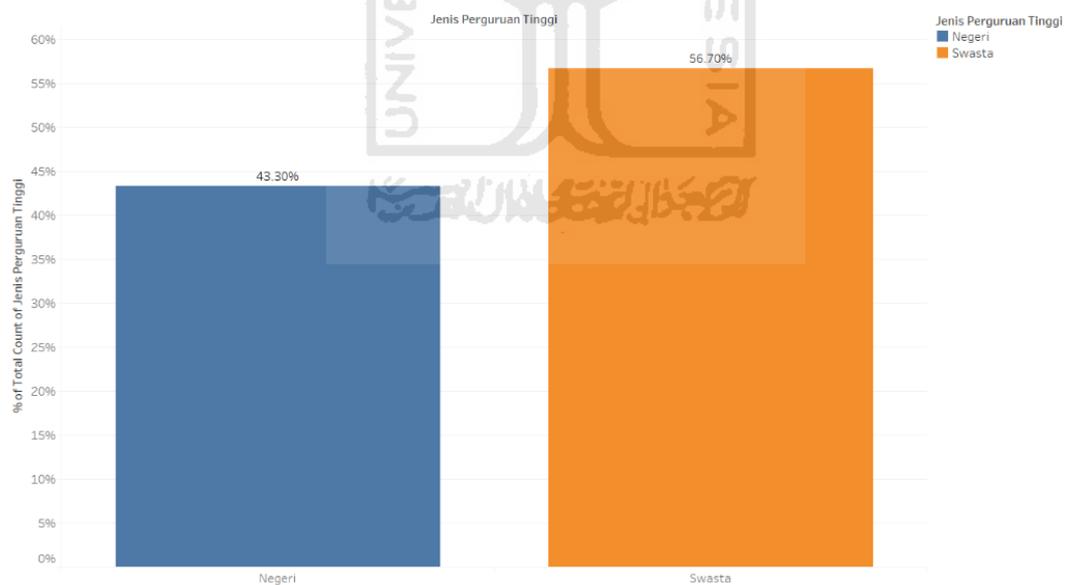
Dari Jumlah responden yang terkumpul, responden yang paling banyak mengisi survei kuesioner ini adalah responden yang masih menjalani Pendidikan S1 yang mana dari data yang dihasilkan dapat dilihat bahwa jumlah responden yang masih menempuh Pendidikan S1 adalah sejumlah 86% dari jumlah total responden. Oleh karena itu, peneliti menggunakan data S1 sebagai induk dari variabel Jenjang Pendidikan ini, yang mana S1 diberi nilai 1 dan selain S1 diberi nilai 0. Untuk lebih lengkapnya bisa dilihat pada gambar 3.5 di bawah ini.



Gambar 3. 5 Diagram Jenjang Pendidikan

### 3.3.6 Jenis Perguruan Tinggi

Jenis perguruan tinggi yang dominan dalam data ini adalah dari kalangan perguruan tinggi swasta dengan total responden 220 dari 387 responden yang mengisi kuesioner sedangkan sisanya adalah dari perguruan tinggi Negeri. Untuk lebih jelas bisa dilihat pada gambar 3.6 di bawah ini:

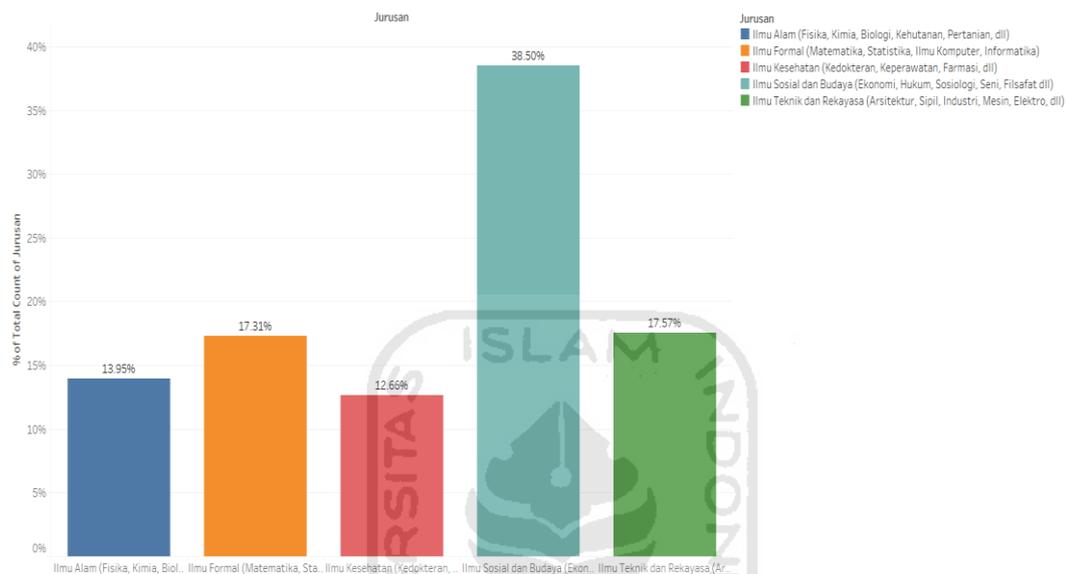


Gambar 3. 6 Diagram Jenis Perguruan Tinggi

### 3.3.7 Jurusan

Dalam kuesioner yang disebar, peneliti membagi jurusan yang ada pada perguruan tinggi menjadi 5 kelompok yaitu Ilmu Alam, Ilmu Kesehatan, Ilmu Formal, Ilmu Sosial dan

Budaya, dan Ilmu teknik dan Rekayasa. Dari data yang terkumpul, jurusan yang menjadi dominan dalam data ini adalah jurusan Ilmu Sosial dan Budaya yaitu berjumlah 39% dari jumlah total data. Akan tetapi, yang menjadi fokus utama dalam analisis ini adalah jurusan Ilmu Formal yang meliputi rumpun keilmuan Matematika, Ilmu Komputer, Informatika, dan Teknologi Informasi. Hal ini dikarenakan hasil visualisasi dari data jurusan menunjukkan jika jurusan ilmu formal memiliki bentuk data yang berbeda dari jurusan yang lainnya.



Gambar 3. 7 Diagram Jurusan

### 3.4 Variabel Penelitian

Variabel bisa diartikan sebagai atribut suatu objek yang mempunyai variasi antara satu sama lain (Hatch dan Farhady, 1981). Pada penelitian ini ada beberapa macam variabel yang dipakai pada penelitian ini, yang akan dijelaskan di bawah ini.

#### a. Variabel Dependen (Dependent Variable)

Variabel dependen adalah suatu variabel yang dijelaskan atau dipengaruhi oleh independent variabel. Variabel ini disebut juga sebagai variabel yang diduga sebagai akibat, dan variabel dependen bisa juga disebut sebagai variabel konsekuensi (Indriantoro, 1999: 63-68).

#### b. Variabel Independen (*Independent Variable*)

Adalah sebuah variabel yang menjelaskan atau memengaruhi variabel yang lain. Variabel ini disebut juga sebagai yang diduga sebagai sebab, dan variabel ini sering juga disebut sebagai variabel yang mendahului (Indriantoro, 1999: 63-68).

Untuk mempersempit jumlah variabel yang ada dan untuk melihat relasi antar variabel, peneliti menggunakan teknik analisis faktor, dan teknik yang digunakan untuk melakukan analisis ini adalah teknik *Exploratory Factor Analysis (EFA)*.

*Exploratory Factor Analysis (EFA)* adalah sebuah teknik analisis faktor yang bisa digunakan untuk mengeksplorasi sebuah data yang ada (Costello, 2005). Dari hasil analisis faktor yang dapat dilihat pada tabel 3.2, 3.3 dan 3.4 dapat dilihat jika Variabel Kebiasaan(Kb), Kesadaran (Ks) dan Pengetahuan (P) memiliki masing-masing 3 kelompok faktor (MR) dan variabel MR tersebut akan diubah menjadi Kb1, Kb2, Kb3 untuk Kebiasaan, Ks1, Ks2, Ks3 untuk Kesadaran dan P1, P2, P3 untuk Pengetahuan. Visualisasi dari hasil analisis faktor ini, bisa dilihat pada gambar 3.8, 3.9 dan 3.10 di bawah.

Tabel 3. 2 Hasil Analisis Factor Kebiasaan

| <i>Loadings</i>    | MR 1  | MR 2  | MR 3  |
|--------------------|-------|-------|-------|
| kebpasstr          | 0.801 |       |       |
| kebpasunq          | 0.870 |       |       |
| kebpasren          | 0.730 |       |       |
| kebvnt             | 0.372 |       |       |
| kebssl             | 0.618 |       |       |
| kebtfa             | 0.570 |       |       |
| kebpirate          |       | 0.671 |       |
| kebilegal          |       | 0.856 |       |
| kebporno           |       | 0.799 |       |
| kebvpn             |       | 0.404 |       |
| kebjp              |       |       | 0.472 |
| kebt               |       |       | 0.712 |
| <i>SS Loadings</i> | 2.860 | 2.239 | 0.866 |
| Proportion         | 0.238 | 0.187 | 0.072 |
| Cumulative         | 0.238 | 0.425 | 0.497 |

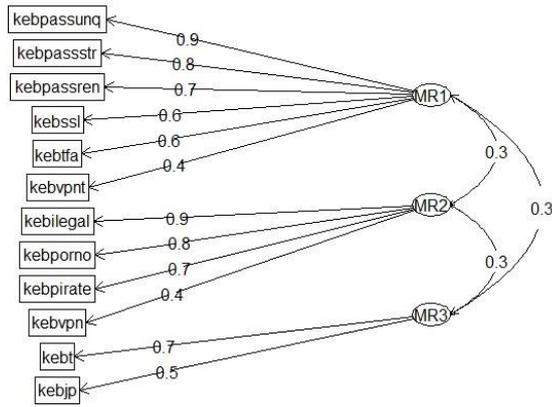
Tabel 3. 3 Hasil Analisis Factor Kesadaran

| <i>Loadings</i> | MR 1  | MR 2 | MR 3 |
|-----------------|-------|------|------|
| kespasstr       | 0.875 |      |      |
| kespasunq       | 0.967 |      |      |

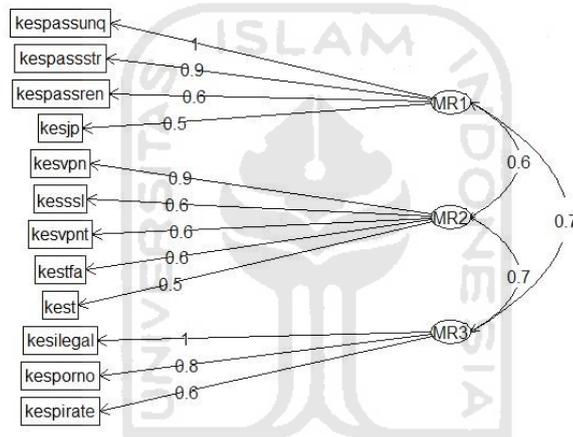
|                    |       |       |       |
|--------------------|-------|-------|-------|
| kespassren         | 0.611 |       |       |
| kesjp              | 0.484 |       |       |
| kest               |       | 0.523 |       |
| kesvpn             |       | 0.921 |       |
| kesvpnt            |       | 0.623 |       |
| kesssl             |       | 0.623 |       |
| kestfa             |       | 0.577 |       |
| kespirate          |       |       | 0.552 |
| kesilegal          |       |       | 0.977 |
| kesporno           |       |       | 0.832 |
| <i>SS Loadings</i> | 2.563 | 2.392 | 2.033 |
| Proportion         | 0.214 | 0.199 | 0.169 |
| Cumulative         | 0.214 | 0.413 | 0.582 |

Tabel 3. 4 Hasil Analisis Factor Pengetahuan

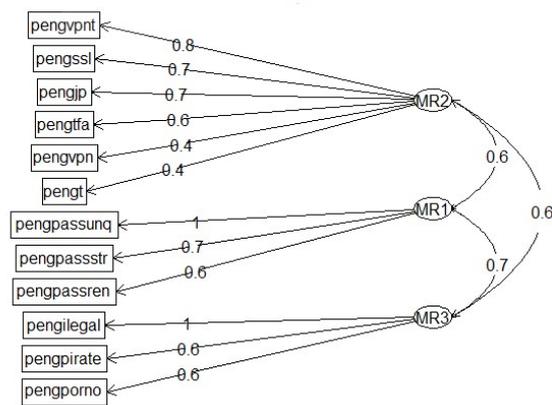
| <i>Loadings</i>    | MR 1   | MR 2  | MR 3  |
|--------------------|--------|-------|-------|
| pengpassstr        | 0.708  |       |       |
| pengpassunq        | 0.984  |       |       |
| pengpassren        | -0.638 |       |       |
| pengjp             |        | 0.704 |       |
| pengt              |        | 0.417 |       |
| pengvpn            |        | 0.421 |       |
| pengvpnt           |        | 0.846 |       |
| pengssl            |        | 0.731 |       |
| pengtfa            |        | 0.574 |       |
| pengpirate         |        |       | 0.640 |
| pengilegal         |        |       | 1.013 |
| pengporno          |        |       | 0.623 |
| <i>SS Loadings</i> | 2.521  | 2.102 | 1.979 |
| Proportion         | 0.210  | 0.175 | 0.165 |
| Cumulative         | 0.210  | 0.385 | 0.550 |



Gambar 3. 8 Hasil Faktor Kebiasaan



Gambar 3. 9 Hasil Faktor Kesadaran



Gambar 3. 10 Hasil Faktor Pengetahuan

### 3.5 Model dan Indikator Penelitian

Dari hasil analisis faktor yang dilakukan sebelumnya dapat diputuskan jika model yang akan digunakan untuk menjawab hipotesis (H) 1.1 sampai 2.7 adalah membuat pengetahuan (P) dan kesadaran (Ks) yang memiliki masing-masing 3 faktor, dijadikan sebagai *Dependent Variable* dan membuat demografi (D) sebagai *Independent Variable*.

Selanjutnya, model yang digunakan untuk menjawab hipotesis(H) 3.1 sampai 3.7. Yang mana pada model ini kebiasaan (Kb) yang memiliki 3 faktor, dijadikan sebagai *Dependent Variable* dan membuat pengetahuan (P), Kesadaran (Ks) dan demografi (D) menjadi *Independent Variable*.

Tabel 3.5 di bawah ini adalah tabel yang menampilkan metode pengubahan data yang digunakan pada analisis berikutnya.

Tabel 3. 5 Metode Pengubah Data

| Jenis                       | Kelompok Variabel | Faktor | Variabel asli  | Peubah      |
|-----------------------------|-------------------|--------|--|-------------|
| <i>Independent Variabel</i> | Demografi(D)      | D      | Umur   | age         |
|                             |                   |        | Jenis Kelamin  | sex         |
|                             |                   |        | Domisili Jawa  | jawa        |
|                             |                   |        | Uang Saku  | income      |
|                             |                   |        | Jenjang Pendidikan   | sarjana     |
|                             |                   |        | Jenis Perguruan Tinggi                                       | ptn         |
|                             |                   |        | Jurusan  | compsci     |
| <i>Dependent Variabel</i>   | Pengetahuan(P)    | P1     | Saya tahu <i>password</i> yang kuat itu seperti apa          | pengpassstr |
|                             |                   |        | Saya tahu apa yang dimaksud dengan <i>password</i> yang unik | pengpassunq |
|                             |                   |        | Saya tahu tentang pembaharuan <i>password</i> secara berkala | pengpassren |
|                             |                   | P2     | Saya tahu jaringan publik mana yang tidak aman               | pengjpp     |

|  |               |     |  |            |
|--|---------------|-----|--|------------|
|  |               |     | Saya tahu risiko-risiko yang ada pada transaksi finansial dan perbankan secara <i>online</i>       | pengt      |
|  |               |     | Saya tahu apa itu Virtual Private Network(VPN)   | pengvpn    |
|  |               |     | Saya tahu VPN yang bisa dipercaya atau tidak dipercaya   | pengvpnt   |
|  |               |     | Saya tahu apa itu SSL dan HTTPS  | pengssl    |
|  |               |     | Saya tahu apa itu Two-Factor Authentications (2FA)   | pengtfa    |
|  |               | P3  | Saya tahu apa itu <i>software</i> bajakan (crack, keygen, dll)                                     | pengpirate |
|  |               |     | Saya tahu apa itu konten video ilegal/bajakan  | pengilegal |
|  |               |     | Saya tahu apa itu konten pornografi  | pengporno  |
|  | Kesadaran(Ks) | Ks1 | Saya sadar bahwa <i>password</i> yang kuat bisa mengurangi risiko pembobolan akun                  | kespasstr  |
|  |               |     | Saya sadar bahwa <i>password</i> yang unik pada setiap akun bisa mengurangi risiko pembobolan akun | kespassunq |
|  |               |     | Saya sadar jika memperbarui <i>password</i> secara berkala bisa mengurangi risiko pembobolan akun  | kespassren |
|  |               |     | Saya sadar menggunakan jaringan publik yang tidak aman bisa meningkatkan risiko keamanan akun      | kesjpb     |

|  |  |               |   |  |  |          |
|--|--|---------------|---|--|--|----------|
|  |  | Ks2           | Saya sadar bahwa melakukan transaksi finansial atau perbankan saat menggunakan jaringan publik sangat tidak aman  | kest   |  |          |
|  |  |               | Saya sadar fungsi dan manfaat VPN pada saat terhubung di jaringan publik  | kesvpn   |  |          |
|  |  |               | Saya sadar bahwa tidak semua VPN bisa dipercaya   | kesvpnt  |  |          |
|  |  |               | Saya sadar fungsi dan manfaat SSL dan HTTPS pada <i>website</i> di Internet                                       | kesssl   |  |          |
|  |  |               | Saya sadar jika menggunakan Two-Factor Authentications (2FA) saat login akun bisa mengurangi risiko keamanan akun | kestfa   |  |          |
|  |  |               | Ks3   | Saya sadar bahwa menggunakan <i>software</i> bajakan akan berbahaya bagi keamanan perangkat dan data | kespirate  |          |
|  |  | Kebiasaan(Kb) | Kb1   | Saya sadar risiko dari mengakses situs-situs penyedia konten video ilegal/bajakan                    | kesilegal  |          |
|  |  |               |   | Saya sadar risiko dari mengakses situs-situs penyedia konten pornografi                              | kesporno   |          |
|  |  |               |   | Saya menggunakan <i>password</i> yang kuat pada setiap akun  | kebpsstr   |          |
|  |  |               |   |  | Saya menggunakan <i>password</i> yang unik untuk setiap akun | kebpsunq |
|  |  |               |   |  | Saya memperbarui <i>password</i> akun secara berkala         | kebpsren |

|  |  |     |  |           |
|--|--|-----|--|-----------|
|  |  |     | Saya hanya menggunakan VPN yang bisa dipercaya saja  | kebvnt    |
|  |  |     | Saya hanya mengunjungi <i>website</i> yang mendukung SSL dan HTTPS                           | kebssl    |
|  |  |     | Saya menggunakan Two-Factor Authentications (2FA) untuk login di setiap akun saya            | kebtfa    |
|  |  | Kb2 | Saya menggunakan <i>software</i> bajakan pada perangkat saya                                 | kebpirate |
|  |  |     | Saya mengakses situs-situs penyedia konten video ilegal                                      | kebilegal |
|  |  |     | Saya mengakses situs-situs penyedia konten pornografi  | kebporno  |
|  |  |     | Saya menggunakan VPN saat terhubung di jaringan publik                                       | kebvnt    |
|  |  | Kb3 | Saya menggunakan jaringan publik untuk berinteraksi di dunia siber                           | kebjp     |
|  |  |     | Saya menggunakan jaringan publik saat transaksi finansial dan perbankan secara <i>online</i> | kebt      |

### 3.6 Hipotesis

Hipotesis merupakan sebuah jawaban sementara terhadap rumusan masalah penelitian (Sugiyono, 2008), dan pada penelitian ini terdapat 25 hipotesis yang akan digunakan untuk menjawab rumusan masalah yang telah ditetapkan. Adapun hipotesis dalam penelitian ini adalah

**H1** : Mahasiswa di Indonesia sudah memiliki pengetahuan yang cukup mengenai *cybersecurity*

**H2** : Mahasiswa di Indonesia sudah memiliki kesadaran yang cukup mengenai *cybersecurity*

**H1.1**: Usia memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa

**H1.2:** Jenis kelamin memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa

**H1.3:** Domisili memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa

**H1.4:** Besar uang saku bulanan memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa

**H1.5:** Jenjang pendidikan memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa

**H1.6:** Jenis Perguruan Tinggi memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa

**H1.7:** Jurusan yang ditempuh memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa

**H2.1:** Usia memiliki pengaruh pada kesadaran akan *cybersecurity* pada mahasiswa

**H2.2:** Jenis kelamin memiliki pengaruh pada kesadaran akan *cybersecurity* pada mahasiswa

**H2.3:** Domisili memiliki pengaruh pada kesadaran akan *cybersecurity* pada mahasiswa

**H2.4:** Besar uang saku bulanan memiliki pengaruh pada kesadaran akan *cybersecurity* pada mahasiswa

**H2.5:** Jenjang pendidikan memiliki pengaruh pada kesadaran akan *cybersecurity* pada mahasiswa

**H2.6:** Jenis Perguruan Tinggi memiliki pengaruh pada kesadaran akan *cybersecurity* pada mahasiswa

**H2.7:** Jurusan yang ditempuh memiliki pengaruh pada kesadaran akan *cybersecurity* pada mahasiswa

**H3.1:** Kesadaran tentang *cybersecurity* memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.2:** Pengetahuan tentang *cybersecurity* memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.3:** Usia memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.4:** Jenis kelamin memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.5:** Domisili memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.6:** Besar uang saku bulanan memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.7:** Jenjang pendidikan memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.8:** Jenis Perguruan Tinggi memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

**H3.9:** Jurusan yang ditempuh memiliki pengaruh pada kebiasaan akan *cybersecurity* pada mahasiswa

### 3.7 Uji Validitas dan Reliabilitas Data

#### 1. Uji Validitas

Uji validitas digunakan untuk mengetahui sejauh mana alat ukur yang digunakan mampu untuk memberikan hasil yang sesuai dengan apa yang ingin dicapai dan menghasilkan data dengan tingkat relevansi yang tinggi (Wiyono, 2011).

Ada nilai *loading* dari masing-masing variabel yang harus dipenuhi. Semua nilai *loading* dari tiap variabel laten, baik itu pengetahuan dan kesadaran semuanya sudah memenuhi kriteria “*very beneficial*” yang berarti semua nilai *loading* pada setiap variabel sudah di atas 0.35 (Sugiyono, 2008).

#### 2. Uji Reliabilitas

Uji reliabilitas digunakan untuk mengetahui jika variabel dari data yang akan digunakan dalam penelitian memiliki presisi yang tinggi dan dapat dipercaya (Thoifah, 2015).

Dalam melakukan pengujian reliabilitas suatu data, sebuah data harus dapat memenuhi sebuah standar ukuran internal yang telah ditetapkan, ukuran nilai tersebut adalah *Cronbach's alpha* yang harus dipenuhi agar suatu data dapat disebut reliabel.

Nilai yang harus dipenuhi yaitu sebuah kriteria “*excellent*” yang bernilai  $\geq 0,60$  (Sugiyono, 2008).

### 3.8 Metode Analisis Data

#### 3.8.1 Analisis Statistik Deskriptif

Adalah sebuah analisis yang digunakan untuk menganalisis data dengan cara mendeskripsikan atau menggambarkan data yang ada tanpa bermaksud membuat kesimpulan yang berlaku untuk umum atau generalisasi.

Analisis ini biasanya digunakan dalam penelitian-penelitian yang bersifat eksplorasi (Muhson, 2006), misalnya seperti penelitian yang sedang dilakukan sekarang ini yaitu penelitian yang bertujuan untuk melihat bagaimana tingkat kesadaran tentang *cybersecurity* pada kalangan mahasiswa yang ada di Indonesia

### **3.8.2 Analisis Kuantitatif**

Adalah suatu proses analisis yang bertujuan untuk menemukan suatu pengetahuan dari sekumpulan data berupa angka. Dalam penelitian ini alat analisis yang digunakan adalah regresi linear.

Teknik yang dipakai dalam melakukan analisis regresi linear adalah teknik *Structural Equation Modeling* (SEM) dengan menggunakan Bahasa R. Dengan teknik SEM, peneliti dapat melakukan teknik analisis *multivariable* yang digunakan untuk menganalisis hubungan struktural pada suatu variabel yang terdapat pada data yang akan dianalisis, dan dengan menggunakan teknik SEM peneliti juga dapat menguji hubungan sebab akibat antara dua atau lebih variabel



## BAB IV

### HASIL DAN PEMBAHASAN

#### 4.1 Pengujian Kuesioner

Setelah semua data yang diperlukan sudah terkumpul, maka langkah selanjutnya yang dilakukan adalah melihat seberapa tinggi validitas dan reliabilitas yang dimiliki pada data yang sudah terkumpul sebelumnya. Hasil ini nanti akan digunakan untuk analisis selanjutnya.

##### 4.1.1 Uji Validitas

Ada nilai *loading* dari masing-masing variabel yang harus dipenuhi. Semua nilai *loading* dari tiap variabel laten, baik itu pengetahuan dan kesadaran semuanya sudah memenuhi kriteria “*very beneficial*” yang berarti semua nilai *loading* pada setiap variabel sudah di atas 0.35 (Sugiyono, 2008:178-179). Menurut Garson (2009) Nilai *loading* adalah sebuah bobot regresi yang menyatakan relasi setiap indikator terhadap variabel yang dibangun. Hasil lebih lengkap bisa dilihat pada tabel 4.1 di bawah ini:

Tabel 4. 1 Hasil Uji Validitas

| Kelompok Variabel | Variabel asli  | <i>Loading</i> | Hasil |
|-------------------|--|----------------|-------|
| Pengetahuan       | Saya tahu <i>password</i> yang kuat itu seperti apa  | 0.8201094      | Valid |
|                   | Saya tahu apa yang dimaksud dengan <i>password</i> yang unik                                 | 0.7929025      | Valid |
|                   | Saya tahu tentang pembaharuan <i>password</i> secara berkala                                 | 0.7539748      | Valid |
|                   | Saya tahu jaringan publik mana yang tidak aman   | 0.6423142      | Valid |
|                   | Saya tahu risiko-risiko yang ada pada transaksi finansial dan perbankan secara <i>online</i> | 0.7295932      | Valid |
|                   | Saya tahu apa itu Virtual Private Network(VPN)   | 0.7695173      | Valid |
|                   | Saya tahu VPN yang bisa dipercaya atau tidak terpercaya                                      | 0.6477576      | Valid |
|                   | Saya tahu apa itu SSL dan HTTPS  | 0.6269591      | Valid |
|                   | Saya tahu apa itu Two-Factor Authentications (2FA)   | 0.6663891      | Valid |

|           |   |           |       |
|-----------|---|-----------|-------|
|           | Saya tahu apa itu <i>software</i> bajakan (crack, keygen, dll)  | 0.8229524 | Valid |
|           | Saya tahu apa itu konten video ilegal/bajakan   | 0.8247332 | Valid |
|           | Saya tahu apa itu konten pornografi   | 0.7846924 | Valid |
| Kesadaran | Saya sadar bahwa <i>password</i> yang kuat bisa mengurangi risiko pembobolan akun                                 | 0.8376645 | Valid |
|           | Saya sadar bahwa <i>password</i> yang unik pada setiap akun bisa mengurangi risiko pembobolan akun                | 0.8289577 | Valid |
|           | Saya sadar jika memperbarui <i>password</i> secara berkala bisa mengurangi risiko pembobolan akun                 | 0.8579260 | Valid |
|           | Saya sadar menggunakan jaringan publik yang tidak aman bisa meningkatkan risiko keamanan akun                     | 0.7655478 | Valid |
|           | Saya sadar bahwa melakukan transaksi finansial atau perbankan saat menggunakan jaringan publik sangat tidak aman  | 0.7404650 | Valid |
|           | Saya sadar fungsi dan manfaat VPN pada saat terhubung di jaringan publik  | 0.6975356 | Valid |
|           | Saya sadar bahwa tidak semua VPN bisa dipercaya   | 0.6819891 | Valid |
|           | Saya sadar fungsi dan manfaat SSL dan HTTPS pada <i>website</i> di Internet                                       | 0.5353300 | Valid |
|           | Saya sadar jika menggunakan Two-Factor Authentications (2FA) saat login akun bisa mengurangi risiko keamanan akun | 0.6771881 | Valid |
|           | Saya sadar bahwa menggunakan <i>software</i> bajakan akan berbahaya bagi keamanan perangkat dan data              | 0.7889301 | Valid |
|           | Saya sadar risiko dari mengakses situs-situs penyedia konten video ilegal/bajakan                                 | 0.8401156 | Valid |
|           | Saya sadar risiko dari mengakses situs-situs penyedia konten pornografi   | 0.7927835 | Valid |
| Kebiasaan | Saya menggunakan <i>password</i> yang kuat pada setiap akun   | 0.5869055 | Valid |

|  |           |       |
|--|-----------|-------|
| Saya menggunakan <i>password</i> yang unik untuk setiap akun                                 | 0.6137221 | Valid |
| Saya memperbarui <i>password</i> akun secara berkala   | 0.5906322 | Valid |
| Saya hanya menggunakan VPN yang bisa dipercaya saja  | 0.6595601 | Valid |
| Saya hanya mengunjungi <i>website</i> yang mendukung SSL dan HTTPS                           | 0.6661006 | Valid |
| Saya menggunakan Two-Factor Authentications (2FA) untuk login di setiap akun saya            | 0.7009880 | Valid |
| Saya menggunakan <i>software</i> bajakan pada perangkat saya                                 | 0.5748744 | Valid |
| Saya mengakses situs-situs penyedia konten video ilegal                                      | 0.5478586 | Valid |
| Saya mengakses situs-situs penyedia konten pornografi  | 0.4840688 | Valid |
| Saya menggunakan VPN saat terhubung di jaringan publik                                       | 0.6033308 | Valid |
| Saya menggunakan jaringan publik untuk berinteraksi di dunia siber                           | 0.5055109 | Valid |
| Saya menggunakan jaringan publik saat transaksi finansial dan perbankan secara <i>online</i> | 0.3063399 | Valid |

#### 4.1.2 Uji Reliabilitas

Dalam melakukan pengujian reliabilitas suatu data, sebuah data harus dapat memenuhi sebuah standar ukuran internal yang telah ditetapkan, ukuran nilai tersebut adalah *Cronbach's alpha* yang harus dipenuhi agar suatu data dapat disebut reliabel.

Nilai yang harus dipenuhi yaitu variabel yang memiliki nilai  $\geq 0,60$  (Sugiyono, 2008:178-179). Hasil dari uji reliabilitas pada analisis ini bisa dilihat pada tabel 4.2 berikut:

Tabel 4. 2 Hasil Uji Reliabilitas

| Variabel  | <i>Cronbach's alpha</i> | Hasil            |
|-----------|-------------------------|------------------|
| Kesadaran | 0.94                    | <i>Excellent</i> |
| Kebiasaan | 0.85                    | <i>Excellent</i> |

|             |     |                  |
|-------------|-----|------------------|
| Pengetahuan | 094 | <i>Excellent</i> |
|-------------|-----|------------------|

Dari tabel 4.2 di atas bisa dilihat jika nilai *Cronbach's alpha* yang dihasilkan dari variabel kesadaran, kebiasaan dan pengetahuan, semua sudah memenuhi standar nilai yang sudah ditetapkan sebelumnya. Ini menunjukkan jika variabel tersebut sudah reliabel untuk digunakan pada analisis selanjutnya.

## 4.2 Uji Hipotesis

### 4.2.1 Hasil Analisis deskriptif

Adalah sebuah analisis yang digunakan untuk menganalisis data, dengan cara mendeskripsikan atau menggambarkan data yang ada tanpa bermaksud membuat kesimpulan yang berlaku untuk umum atau generalisasi.

Analisis ini dilakukan agar peneliti bisa menemukan jawaban dari hipotesis 1 dan 2, di mana hipotesis tersebut berisi tentang bagaimana tingkat kesadaran dan pengetahuan tentang *cybersecurity* yang dimiliki oleh mahasiswa yang ada di Indonesia.

Jenis skala yang digunakan pada variabel kesadaran dan pengetahuan adalah skala likert yang bernilai dari 1 sampai 5, di mana 1 adalah nilai yang memiliki bobot terendah dan 5 adalah nilai yang memiliki bobot paling tinggi. Oleh karena itu untuk melihat bagaimana tingkat kesadaran dan pengetahuan tentang *cybersecurity* yang dimiliki oleh mahasiswa di Indonesia, peneliti mencari nilai *mean* atau rata-rata yang dimiliki pada masing-masing variabel tersebut.

Kemudian nilai rata-rata yang dihasilkan dari variabel tersebut, akan dibulatkan sesuai dengan aturan pembulatan angka yang berlaku, yang mana angka 5 atau lebih akan dibulatkan ke atas dan angka yang kurang dari 5 akan dibulatkan ke bawah. Pembulatan ini dilakukan dengan tujuan untuk mempermudah peneliti dalam memilih atau menentukan kelompok dari nilai tersebut. Yang mana kelompok tersebut bisa dilihat pada tabel 4.3 berikut:

Tabel 4. 3 Tabel Pengelompokan Skala Likert

| No | Jawaban             | Kode | Bobot |
|----|---------------------|------|-------|
| 1  | Sangat Tidak Setuju | STS  | 1     |
| 2  | Tidak Setuju        | TS   | 2     |
| 3  | Netral              | N    | 3     |
| 4  | Setuju              | S    | 4     |
| 5  | Sangat Setuju       | SS   | 5     |

#### 4.2.2 Kesadaran

Hasil dari analisis deskriptif pada variabel kesadaran bisa dilihat pada tabel 4.4. pada tabel tersebut bisa dilihat jika tingkat kesadaran tentang *cybersecurity* yang dimiliki oleh mahasiswa di Indonesia sudah cukup baik, karena rata-rata nilai yang dihasilkan pada variabel tersebut adalah 4 (setuju), yang mana nilai 4 tersebut sudah menjadi nilai yang memiliki bobot tertinggi kedua setelah nilai 5 (sangat setuju). Hasil lebih jelas bisa dilihat pada tabel 4.4 berikut:

Tabel 4. 4 Hasil Analisis Deskriptif Kesadaran

| No | Variabel   | Nilai | Keterangan |
|----|--|-------|------------|
| 1  | Saya sadar bahwa <i>password</i> yang kuat bisa mengurangi risiko pembobolan akun                                | 4     | Setuju     |
| 2  | Saya sadar bahwa <i>password</i> yang unik pada setiap akun bisa mengurangi risiko pembobolan akun               | 4     | Setuju     |
| 3  | Saya sadar jika memperbarui <i>password</i> secara berkala bisa mengurangi risiko pembobolan akun                | 4     | Setuju     |
| 4  | Saya sadar menggunakan jaringan publik yang tidak aman bisa meningkatkan risiko keamanan akun                    | 4     | Setuju     |
| 5  | Saya sadar bahwa melakukan transaksi finansial atau perbankan saat menggunakan jaringan publik sangat tidak aman | 4     | Setuju     |
| 6  | Saya sadar fungsi dan manfaat VPN pada saat terhubung di jaringan publik   | 3     | Netral     |

|           |   |   |        |
|-----------|---|---|--------|
| 7         | Saya sadar bahwa tidak semua VPN bisa dipercaya   | 4 | Setuju |
| 8         | Saya sadar fungsi dan manfaat SSL dan HTTPS pada <i>website</i> di Internet                                       | 3 | Netral |
| 9         | Saya sadar jika menggunakan Two-Factor Authentications (2FA) saat login akun bisa mengurangi risiko keamanan akun | 3 | Netral |
| 10        | Saya sadar bahwa menggunakan <i>software</i> bajakan akan berbahaya bagi keamanan perangkat dan data              | 4 | Setuju |
| 11        | Saya sadar risiko dari mengakses situs-situs penyedia konten video ilegal/bajakan                                 | 4 | Setuju |
| 12        | Saya sadar risiko dari mengakses situs-situs penyedia konten pornografi   | 4 | Setuju |
| Rata-rata |   | 4 | Setuju |

#### 4.2.3 Pengetahuan

Hasil yang ditunjukkan pada variabel pengetahuan ini tidak jauh berbeda dengan hasil yang ditunjukkan pada variabel kesadaran sebelumnya, hasil nilai rata-rata pada variabel pengetahuan sama dengan nilai rata-rata dari variabel kesadaran. Hal ini menunjukkan jika pengetahuan tentang cybersecurity yang dimiliki oleh mahasiswa yang ada di Indonesia sudah cukup tinggi, karena nilai rata-rata yang dihasilkan pada variabel ini adalah 4 (setuju). Hasil lebih jelasnya bisa dilihat pada tabel 4.5 berikut:

Tabel 4. 5 Hasil Analisis Deskriptif Pengetahuan

| No        | Variabel   | Nilai | Keterangan |
|-----------|--|-------|------------|
| 1         | Saya tahu <i>password</i> yang kuat itu seperti apa  | 4     | Setuju     |
| 2         | Saya tahu apa yang dimaksud dengan <i>password</i> yang unik                                 | 4     | Setuju     |
| 3         | Saya tahu tentang pembaharuan <i>password</i> secara berkala                                 | 4     | Setuju     |
| 4         | Saya tahu jaringan publik mana yang tidak aman   | 3     | Setuju     |
| 5         | Saya tahu risiko-risiko yang ada pada transaksi finansial dan perbankan secara <i>online</i> | 4     | Setuju     |
| 6         | Saya tahu apa itu Virtual Private Network(VPN)   | 4     | Setuju     |
| 7         | Saya tahu VPN yang bisa dipercaya atau tidak terpercaya                                      | 3     | Netral     |
| 8         | Saya tahu apa itu SSL dan HTTPS  | 3     | Netral     |
| 9         | Saya tahu apa itu Two-Factor Autentications (2FA)  | 3     | Netral     |
| 10        | Saya tahu apa itu <i>software</i> bajakan (crack, keygen, dll)                               | 3     | Netral     |
| 11        | Saya tahu apa itu konten video ilegal/bajakan  | 4     | Setuju     |
| 12        | Saya tahu apa itu konten pornografi  | 4     | Setuju     |
| Rata-rata |  | 4     | Setuju     |

#### 4.2.4 Hasil Uji *Goodness of Fit*

Uji coba ini bertujuan untuk melihat seberapa tinggi tingkat kecocokan model yang digunakan pada data yang dianalisis. Ada beberapa ketentuan nilai yang menjadi standar dalam melakukan pengukuran *goodness of fit*. Jika nilai dari variabel yang diuji sudah dinyatakan Fit maka model yang digunakan sudah mampu secara realistis mempresentasikan data yang ada (Chandio, 2011). Nilai standar yang digunakan untuk uji coba ini akan ditampilkan pada tabel 4.6 di bawah ini, begitu pula dengan nilai yang dihasilkan oleh data yang dianalisis bisa dilihat pada tabel 4.7, 4.8 dan 4.9.

Tabel 4. 6 Kriteria *Goodness of Fit*

| <b>Indikator</b> | <b>Rekomendasi Nilai</b>       |
|------------------|--------------------------------|
| CMIN/DF          | $\leq 5.0$ (Wheaton, 1977)     |
| SRMR             | $\leq 0.08$ (Hu, 1999)         |
| RMSEA            | $\leq 0.10$ (MacCallum, 1996)  |
| CFI              | $\geq 0.90$ (Bagozzi, 1988)    |
| TLI              | $\geq 0.90$ (Bentler PM, 1980) |

Tabel 4. 7 Hasil *Goodness of Fit* Model Pengetahuan

| <b>Indikator</b> | <b>Nilai</b> | <b>Keterangan</b> |
|------------------|--------------|-------------------|
| CMIN/DF          | 2.881        | Fit               |
| SRMR             | 0.042        | Fit               |
| RMSEA            | 0.07         | Fit               |
| CFI              | 0.93         | Fit               |
| TLI              | 0.918        | Fit               |

Tabel 4. 8 Hasil *Goodness of Fit* Model Kesadaran

| <b>Indikator</b> | <b>Nilai</b> | <b>Keterangan</b> |
|------------------|--------------|-------------------|
| CMIN/DF          | 3.661        | Fit               |
| SRMR             | 0.051        | Fit               |
| RMSEA            | 0.083        | Fit               |
| CFI              | 0.915        | Fit               |
| TLI              | 0.9          | Fit               |

Tabel 4. 9 Hasil Goodness of Fit Model Kebiasaan

| Indikator | Nilai | Keterangan     |
|-----------|-------|----------------|
| CMIN/DF   | 3.415 | Fit            |
| SRMR      | 0.087 | Acceptable Fit |
| RMSEA     | 0.079 | Fit            |
| CFI       | 0.828 | Marginal Fit   |
| TLI       | 0.815 | Marginal Fit   |

Dari hasil uji *goodness of fit* pada tabel di atas, bisa kita lihat jika semua indikator sudah terpenuhi pada variabel pengetahuan dan kesadaran, hal ini menunjukkan jika model yang dipakai pada variabel pengetahuan dan kesadaran sudah cocok dan bisa dipakai untuk melakukan analisis SEM selanjutnya.

Sementara itu, untuk variabel kebiasaan, masih ada beberapa indikator seperti SRMR, CFI dan TLI yang belum memenuhi syarat nilai yang harus dipenuhi, tetapi masih ada juga 2 indikator yang berhasil memenuhi syarat nilai yang telah ditetapkan sebelumnya. Untuk hal itu maka model yang digunakan pada variabel kebiasaan masih bisa digunakan karena masih ada indikator yang masih terpenuhi.

#### 4.2.5 Uji Struktural Model

Hal yang paling penting yang perlu disiapkan untuk melakukan uji structural model pada suatu data ialah nilai dari parameter *estimate coefficient* (Chandio, 2011), yang mana nilai tersebut digunakan untuk menguji dan mengevaluasi dari hipotesis yang telah dimodelkan. Ada suatu nilai yang harus dipenuhi saat melakukan pengujian agar suatu hipotesis dapat diterima, yang mana nilai tersebut yaitu, nilai *critical ratio (CR)* > 1.96 (JJ Hox, 1998) dan *p-value* < 0.05 (Kock, 2016).

Tabel 4. 10 Hasil Pengujian Struktural Model Pengetahuan

| Index   | Estimate | CR     | P     |
|---------|----------|--------|-------|
| age     | -0.012   | -0.682 | 0.495 |
| sex     | 0.552    | 5.440  | 0.000 |
| jawa    | 0.369    | 3.614  | 0.000 |
| income  | 0.208    | 3.197  | 0.001 |
| sarjana | -0.240   | 1.709  | 0.087 |
| ptn     | 0.055    | 0.565  | 0.572 |

|         |       |       |       |
|---------|-------|-------|-------|
| compsci | 0.415 | 3.237 | 0.001 |
|---------|-------|-------|-------|

Tabel 4. 11 Hasil Pengujian Struktural Model Kesadaran

| Index   | Estimate | CR     | P     |
|---------|----------|--------|-------|
| age     | 0.042    | 2.650  | 0.008 |
| sex     | 0.205    | 2.250  | 0.024 |
| jawa    | 0.273    | 2.938  | 0.003 |
| income  | 0.147    | 2.487  | 0.013 |
| sarjana | 0.024    | 0.188  | 0.851 |
| ptn     | -0.027   | -0.300 | 0.764 |
| compsci | 0.208    | 1.786  | 0.074 |

Tabel 4. 12 Hasil Pengujian Struktural Model Kebiasaan

| Index       | Estimate | CR     | P     |
|-------------|----------|--------|-------|
| Pengetahuan | 0.341    | 4.818  | 0.000 |
| Kesadaran   | 0.128    | 1.717  | 0.086 |
| Age         | 0.002    | 0.322  | 0.747 |
| Sex         | 0.091    | 2.283  | 0.022 |
| Jawa        | -0.161   | -3.745 | 0.000 |
| Income      | 0.058    | 2.238  | 0.025 |
| Sarjana     | -0.071   | -1.280 | 0.201 |
| Ptn         | 0.025    | 0.668  | 0.504 |
| Compsci     | -0.001   | -0.022 | 0.983 |

Dari tabel 4.10, 4.11 dan 4.12 di atas, hasil yang ditemukan ialah, pengetahuan tentang *cybersecurity* yang dimiliki oleh mahasiswa di Indonesia dipengaruhi oleh faktor Jenis kelamin, Uang Saku, Domisili, dan Jurusan yang dipilih oleh mahasiswa tersebut., dan kesadaran yang dimiliki oleh mahasiswa di Indonesia juga dipengaruhi oleh Usia, Jenis Kelamin, Domisili, dan Uang Saku yang dimiliki oleh mahasiswa tersebut. Kebiasaan yang sering dilakukan ketika menggunakan Internet dipengaruhi oleh pengetahuan tentang *cybersecurity* yang dimiliki mahasiswa tersebut, jenis kelamin, dan uang saku perbulan yang diterima mahasiswa tersebut.

### 4.3 Pembahasan Hipotesis

Tabel 4. 13 Status Hipotesis

| <b>Hipotesis</b> | <b>Status</b>    |
|------------------|------------------|
| H1               | Signifikan       |
| H2               | Signifikan       |
| H1.1             | Tidak Signifikan |
| H1.2             | Signifikan       |
| H1.3             | Signifikan       |
| H1.4             | Signifikan       |
| H1.5             | Tidak Signifikan |
| H1.6             | Tidak Signifikan |
| H1.7             | Signifikan       |
| H2.1             | Signifikan       |
| H2.2             | Signifikan       |
| H2.3             | Signifikan       |
| H2.4             | Signifikan       |
| H2.5             | Tidak Signifikan |
| H2.6             | Tidak Signifikan |
| H2.7             | Tidak Signifikan |
| H3.1             | Signifikan       |
| H3.2             | Tidak Signifikan |
| H3.3             | Tidak Signifikan |
| H3.4             | Signifikan       |
| H3.5             | Tidak Signifikan |
| H3.6             | Signifikan       |
| H3.7             | Tidak Signifikan |
| H3.8             | Tidak Signifikan |
| H3.9             | Tidak Signifikan |

Setelah melakukan serangkaian analisis sebelumnya, pada subbab ini peneliti akan membahas hipotesis yang bisa dilihat pada tabel 4.13 di atas. Akan tetapi, hipotesis yang akan

dibahas di sini hanya hipotesis yang menunjukkan hasil positif atau dalam kata lain hipotesis tersebut berhasil diterima.

#### 4.3.1 H1

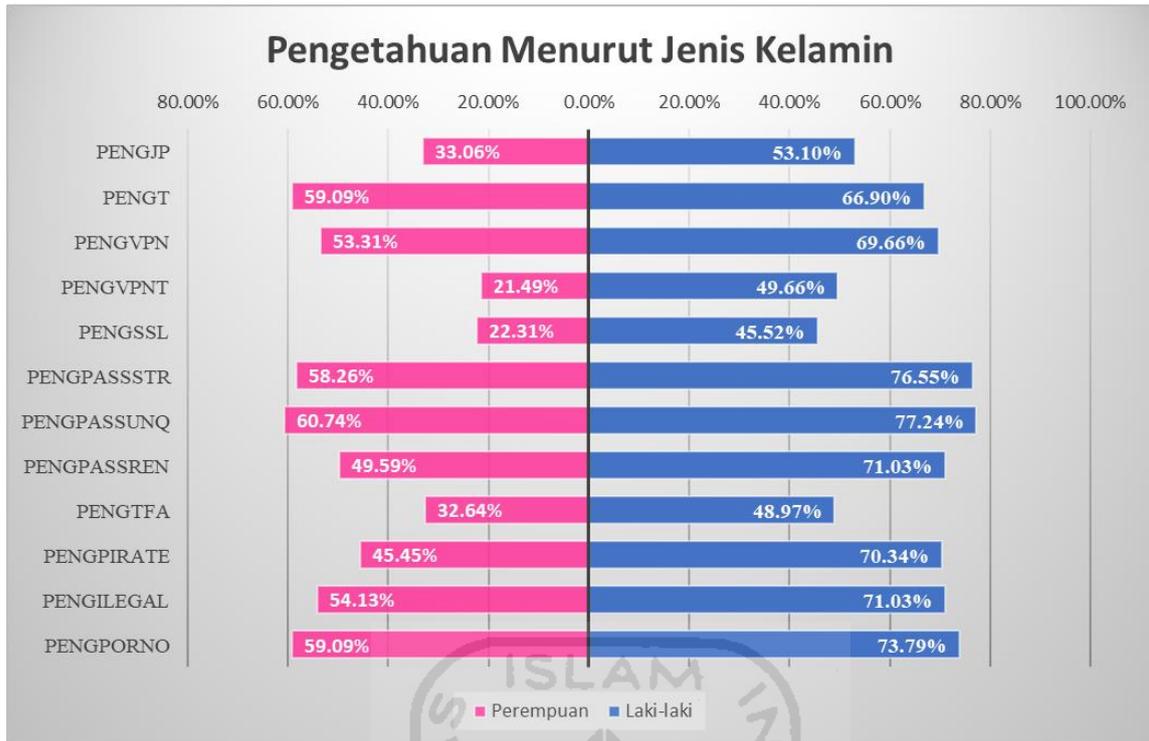
Setelah melakukan analisis deskriptif sebelumnya, hipotesis yang menyatakan jika mahasiswa di Indonesia sudah memiliki pengetahuan yang cukup tinggi dalam hal *cybersecurity*. Hipotesis ini dinyatakan bisa diterima, hal ini dikarenakan nilai rata-rata yang dihasilkan variabel pengetahuan tersebut menunjukkan angka 4 (tahu), hasil ini pun menunjukkan jika mahasiswa yang ada di Indonesia sudah memiliki pengetahuan tentang *cybersecurity* yang cukup tinggi. Hal ini akan membantu mereka dalam melindungi diri dari hal yang bisa merugikan mereka.

#### 4.3.2 H2

Setelah melakukan analisis deskriptif sebelumnya, hipotesis yang menyatakan jika mahasiswa di Indonesia sudah memiliki kesadaran yang cukup baik dalam hal *cybersecurity*. Hipotesis ini dinyatakan bisa diterima, hal ini dikarenakan nilai rata-rata yang dihasilkan variabel kesadaran tersebut menunjukkan angka 4 (sadar), angka tersebut menunjukkan jika mahasiswa di Indonesia sudah sadar akan bahaya yang mengintai jika mereka berinteraksi dengan dunia siber tersebut.

#### 4.3.3 H1.2

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Jenis kelamin memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa di Indonesia. Hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika pengetahuan tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan jenis kelamin para mahasiswa tersebut. Sebuah penelitian yang pernah dilakukan oleh X Liu (2013) menunjukkan jika perempuan menjadi kalangan yang paling sering menjadi korban dari *cybercrime*, hal ini menunjukkan jika laki-laki memiliki pengetahuan tentang *cybersecurity* yang lebih baik dari pada perempuan. Pada gambar 4.1 di bawah akan diberikan sebuah diagram untuk melihat lebih jelas terhadap pengaruh yang diberikan.



Gambar 4. 1 Diagram Pengetahuan Menurut Jenis Kelamin

#### 4.3.4 H1.3

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Domisili memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa di Indonesia. Hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika pengetahuan tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan domisili para mahasiswa tersebut. Dari hal ini juga menunjukkan jika terdapat kesenjangan informasi yang bisa didapatkan antara mahasiswa yang berdomisili di Jawa dengan mahasiswa yang berdomisili di luar Jawa.

#### 4.3.5 H1.4

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Uang Saku yang diperoleh mahasiswa memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa di Indonesia, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika pengetahuan tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan uang saku yang diterima para mahasiswa tersebut. Hal ini menjadi cukup menarik, karena dari hal ini kita bisa melihat jika

perbedaan ekonomi juga bisa menjadi pembeda dalam hal perolehan informasi para mahasiswa tersebut.

#### **4.3.6 H1.7**

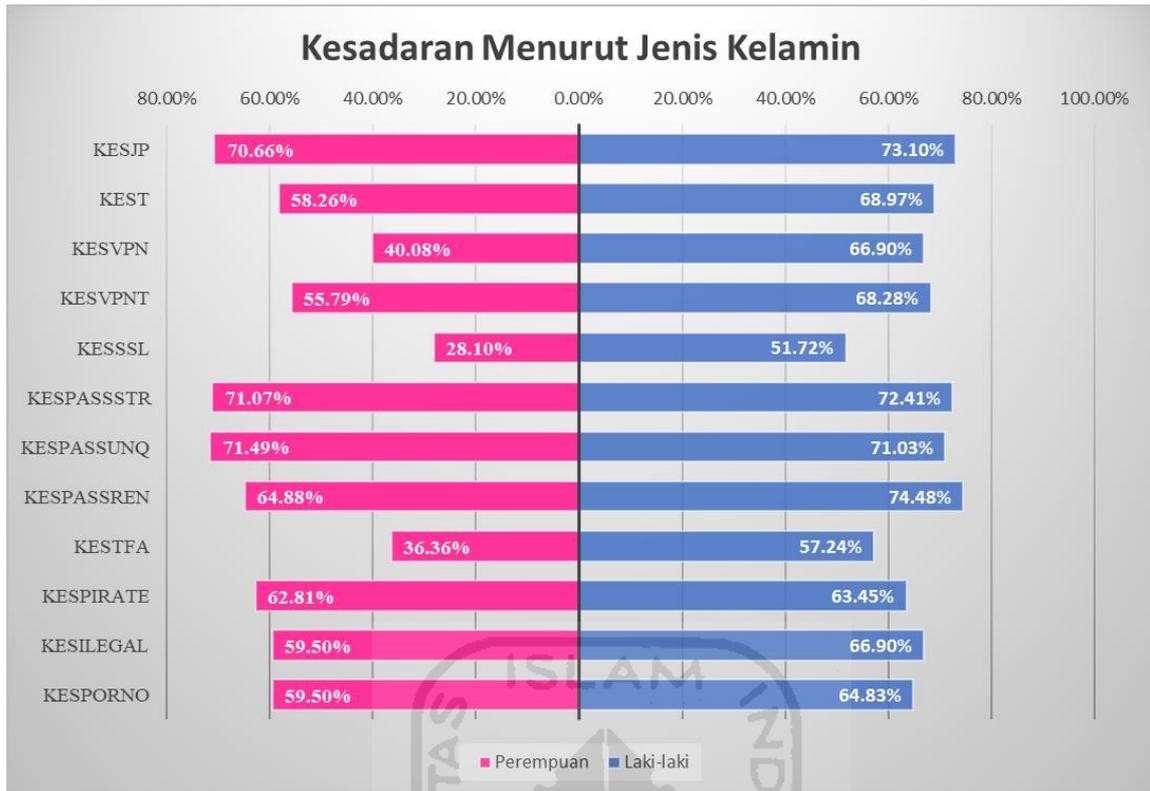
Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Jurusan yang dipilih mahasiswa memiliki pengaruh pada pengetahuan tentang *cybersecurity* pada mahasiswa di Indonesia, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika pengetahuan tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan jurusan yang dipilih para mahasiswa tersebut. Hal ini mungkin disebabkan karena adanya perbedaan bahan pembelajaran dari masing-masing jurusan tersebut, seperti contohnya jika jurusan ilmu formal khususnya ilmu komputer, pasti akan lebih sering mempelajari hal-hal yang bersangkutan dengan *cybersecurity* dari pada jurusan yang lainnya.

#### **4.3.7 H2.1**

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Usia mahasiswa memiliki pengaruh pada kesadaran tentang *cybersecurity* pada mahasiswa di Indonesia, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika kesadaran tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan usia para mahasiswa tersebut. Hal ini bisa juga berarti jika kesadaran tentang *cybersecurity* bisa dipengaruhi dari perbedaan generasi mahasiswa tersebut.

#### **4.3.8 H2.2**

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Jenis Kelamin mahasiswa memiliki pengaruh pada kesadaran tentang *cybersecurity* pada mahasiswa di Indonesia, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika kesadaran tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan jenis kelamin para mahasiswa tersebut. Dari hasil hipotesis ini bisa dilihat jika jenis kelamin menjadi hal yang berpengaruh terhadap kesadaran maupun pengetahuan tentang *cybersecurity* pada mahasiswa di Indonesia. Pada gambar 4.2 di bawah akan diberikan sebuah diagram untuk melihat lebih jelas terhadap pengaruh yang diberikan.



Gambar 4. 2 Diagram Kesadaran Menurut Jenis Kelamin

#### 4.3.9 H2.3

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Domisili mahasiswa memiliki pengaruh pada kesadaran tentang *cybersecurity* pada mahasiswa di Indonesia, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika kesadaran tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan domisili para mahasiswa tersebut. Sama halnya dengan jenis kelamin dan domisili juga berpengaruh terhadap pengetahuan maupun kesadaran tentang *cybersecurity* pada kalangan mahasiswa di Indonesia.

#### 4.3.10 H2.4

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Uang Saku mahasiswa memiliki pengaruh pada kesadaran tentang *cybersecurity* pada mahasiswa di Indonesia, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hal ini menunjukkan jika kesadaran tentang *cybersecurity* dari masing-masing mahasiswa di Indonesia sangat dipengaruhi oleh perbedaan uang saku para mahasiswa tersebut. Hal ini menjadi tambah menarik untuk di bahas, karena tidak hanya berpengaruh pada pengetahuan

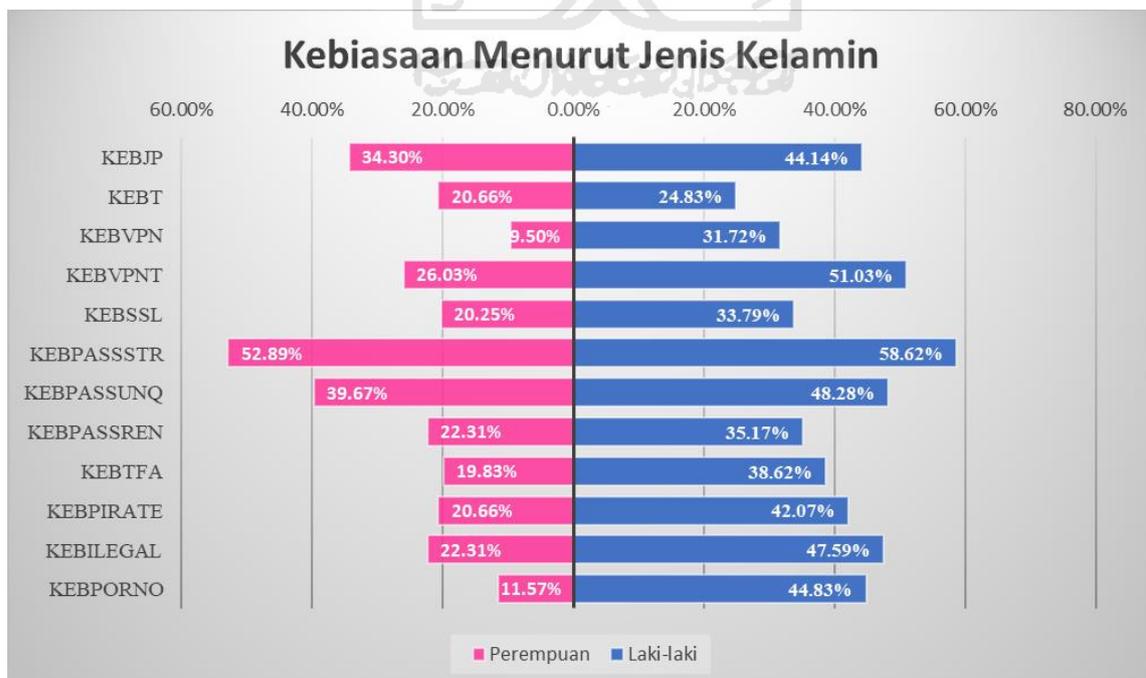
tetapi uang saku juga berpengaruh terhadap kesadaran tentang *cybersecurity* para mahasiswa yang ada di Indonesia.

#### 4.3.11 H3.1

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika pengetahuan tentang *cybersecurity* yang dimiliki mahasiswa di Indonesia memiliki pengaruh pada kebiasaan mereka akan *cybersecurity*, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Ini menunjukkan jika pengetahuan tentang *cybersecurity* yang dimiliki oleh mahasiswa di Indonesia memiliki pengaruh positif terhadap kebiasaan mereka dalam berinteraksi di dalam dunia siber tersebut.

#### 4.3.12 H3.4

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan jika Jenis Kelamin mahasiswa di Indonesia memiliki pengaruh pada kebiasaan mereka akan *cybersecurity*, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Dari hal ini bisa kita simpulkan jika jenis kelamin memiliki pengaruh positif terhadap bagaimana kebiasaan akan *cybersecurity* para mahasiswa di Indonesia. Pada gambar 4.3 dibawah akan diberikan sebuah diagram untuk melihat lebih jelas terhadap pengaruh yang diberikan.



Gambar 4. 3 Diagram Kebiasaan Menurut Jenis Kelamin

#### 4.3.13 H3.6

Berdasarkan hasil dari uji hipotesis yang sudah dilakukan, hipotesis yang menyatakan Uang Saku yang dimiliki mahasiswa di Indonesia memiliki pengaruh pada kebiasaan mereka akan cybersecurity, hipotesis ini dinyatakan bisa diterima karena nilai CR dan *p-value* yang dihasilkan pada variabel ini berhasil memenuhi standar nilai yang telah ditetapkan. Hipotesis ini juga membuktikan jika uang saku yang diterima mahasiswa berpengaruh kepada pengetahuan, kesadaran, dan kebiasaan akan *cybersecurity* pada mahasiswa yang ada di Indonesia.



## **BAB V**

### **KESIMPULAN DAN SARAN**

#### **5.1 Kesimpulan**

Setelah melakukan serangkaian analisis ini, kesimpulan yang bisa ditarik dari hasil analisis ini ialah sebagai berikut:

- Mahasiswa yang ada di Indonesia sudah memiliki pengetahuan dan kesadaran akan *cybersecurity* yang sudah cukup tinggi, akan tetapi tingkat pengetahuan dan kesadaran yang sudah cukup baik tersebut masih dipengaruhi oleh faktor demografis yang dimiliki oleh masing-masing mahasiswa di Indonesia.
- Faktor yang berpengaruh terhadap tingkat pengetahuan tentang *cybersecurity* yang dimiliki oleh mahasiswa Indonesia ialah Jenis Kelamin, Domisili, Uang Saku dan Jurusan masing-masing mahasiswa di Indonesia. Sementara itu, faktor yang berpengaruh terhadap kesadaran akan *cybersecurity* pada mahasiswa yang ada di Indonesia ialah faktor Usia, Jenis Kelamin, Uang Saku dan Domisili dari masing-masing mahasiswa tersebut. Juga faktor Jenjang Pendidikan dan Jenis Perguruan Tinggi, tidak ada pengaruh apapun terhadap pengetahuan dan kesadaran akan *cybersecurity* para mahasiswa di Indonesia.
- Pengetahuan, Jenis Kelamin dan Uang Saku juga memiliki pengaruh yang signifikan terhadap kebiasaan akan *cybersecurity* yang dimiliki mahasiswa di Indonesia, akan tetapi kesadaran akan *cybersecurity* yang dimiliki mahasiswa di Indonesia, tidak memiliki pengaruh apapun terhadap kebiasaan akan *cybersecurity* pada mahasiswa di Indonesia.

Dalam penelitian ini, peneliti juga menemukan jika tingkat pengetahuan, kesadaran dan kebiasaan akan *cybersecurity* pada mahasiswa di Indonesia, sangat dipengaruhi oleh Uang Saku yang diterima oleh masing-masing mahasiswa di Indonesia. Dari hal tersebut bisa ditarik kesimpulan jika perbedaan ekonomi seorang mahasiswa bisa memengaruhi tingkat pengetahuan, kesadaran dan kebiasaan akan *cybersecurity* yang dimiliki mahasiswa tersebut.

#### **5.2 Saran**

Berikut beberapa saran yang bisa diberikan untuk melakukan pengembangan lebih lanjut untuk penelitian ini yang bisa dipertimbangkan:

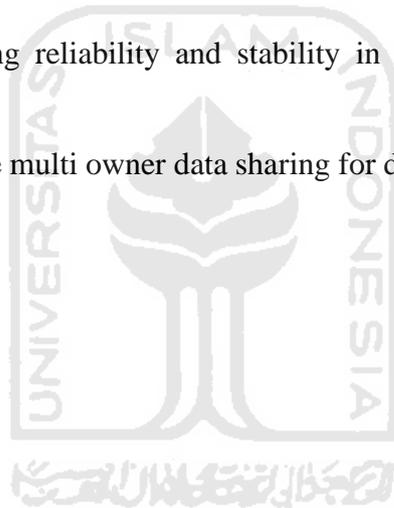
- Untuk penelitian berikutnya peneliti menyarankan untuk memperbaiki *path model* yang digunakan pada penelitian saat ini, karena peneliti menilai jika model yang digunakan pada penelitian ini masih kurang efektif terutama model yang dipakai pada variabel kebiasaan.
- Peneliti menyarankan jika penelitian berikutnya bisa mengupas habis tentang bagaimana bisa uang saku yang diterima mahasiswa bisa sangat berpengaruh kepada tingkat pengetahuan, kesadaran dan kebiasaan akan *cybersecurity* pada mahasiswa di Indonesia.



## DAFTAR PUSTAKA

- Afandi, I. A. (2017). Analisis Hubungan Kesadaran Keamanan , Privasi Informasi , Perilaku Keamanan Pada Para Pengguna Media Sosial Line. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* .
- Amin, M. (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mceda). *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika*, 15-24.
- APJII. (2019, 05 16). *APJII: Jumlah Pengguna Internet di Indonesia Tembus 171 Juta Jiwa*. Retrieved from <https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa>
- Ardiyanti, H. (2014). CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA.
- Bagozzi, R. P. (1988). On the evaluation of struktural equation models. *Journal of the Academy of Marketing Science*.
- Bentler PM, B. D. (1980). Significance Tests and Goodness of Fit in the Analysis of Covariance Structures, *Psychol. Bull.*
- Chairisda, N. R. (2020). OPTIMALISASI SATGAS CYBER PATROL POLRES BANYUMAS DALAM MENGHADAPI PEMILU 2019.
- Chandio, F. (2011). “Studying Acceptance Of Online Banking.
- CNN. (2018, 10 18). *3,9 Miliar Orang di Dunia Telah Terhubung*. Retrieved from [www.cnnindonesia.com: https://www.cnnindonesia.com/teknologi/2018121](https://www.cnnindonesia.com/teknologi/2018121)
- Costello, A. B. (2005). Best practices in exploratory factor analysis: four.
- E. J. Wolf, K. M. (2013). Sample Size Requirements for Struktural Equation Models: An Evaluation of Power, Bias, and Solution Propriety.
- Hu, L. T. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Struktural Equation Modeling* .
- Indriantoro, N. d. (1999). *Metodologi Penelitian Bisnis untuk Akuntansi & Manajemen. Edisi Pertama*. Yogyakarta: BPFE.
- Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index.
- JJ Hox, T. B. (1998). An introduction to structural equation modeling.
- Joanna Buick, J. J. (1997). *Mengenal Cyberspace For Beginners*.

- Kock, N. (2016). Hypothesis testing with confidence intervals and P values in PLS-SEM.
- MacCallum, R. C. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods*.
- Muhson, A. (2006). *TEKNIK ANALISIS KUANTITATIF*. Yogyakarta: Universitas Negeri Yogyakarta.
- Senthilkumar, K. a. (2017). A Survey on Cybersecurity Awareness among College Students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering* .
- Stein, C. M. (2017). *Structural Equation Modeling*.
- Sugiyono. (2008). *Metode Penelitian Kuantitatif Kualitatif dan R&D*.
- Wang, A. Y. (2020). Power Analysis for Parameter Estimation in Structural Equation Modeling: A Discussion and Tutorial. *Advances in Methods and Practices in Psychological Science*.
- Wheaton, B. M. (1977). Assessing reliability and stability in panel models. *Sociological Methodology*.
- X. Liu, Y. Z. (2013). Mona: Secure multi owner data sharing for dynamic groups in the cloud.



## LAMPIRAN

### Kuesioner Penelitian

Assalamualaikum, hai saya Raja Rizky Riyandhika mahasiswa program studi Informatika - program Sarjana di Universitas Islam Indonesia.

Untuk memenuhi kelengkapan penyusunan skripsi saya yang berjudul "Analisis Kesadaran Cyber Security pada Kalangan Mahasiswa di Indonesia", maka dengan segala kerendahan hati saya mohon kesediaan Saudara/i untuk meluangkan waktu sekitar 5-10 menit untuk mengisi kuesioner berikut ini.

Atas segala bantuan dan partisipasi yang Saudara/i berikan, saya ucapkan terima kasih.

#### A. Bagian Pertama: Pertanyaan Umum

- Inisial
- Usia
- Jenis kelamin
  - Laki-laki
  - Perempuan
- Domisili
  1. Aceh
  2. Bali
  3. Banten
  4. Bengkulu
  5. Gorontalo
  6. Jakarta
  7. Jambi
  8. Jawa Barat
  9. Jawa Tengah
  10. Jawa Timur
  11. Kalimantan Barat
  12. Kalimantan Selatan
  13. Kalimantan Tengah
  14. Kalimantan Timur



15. Kalimantan Utara
16. Kepulauan Bangka Belitung
17. Kepulauan Riau
18. Lampung
19. Maluku
20. Maluku Utara
21. Nusa Tenggara Barat
22. Nusa Tenggara Timur
23. Papua
24. Papua Barat
25. Riau
26. Sulawesi Barat
27. Sulawesi Selatan
28. Sulawesi Tengah
29. Sulawesi Tenggara
30. Sulawesi Utara
31. Sumatra Barat
32. Sumatra Selatan
33. Sumatra Utara
34. D.I. Yogyakarta



- Tempat Kelahiran

1. Aceh
2. Bali
3. Banten
4. Bengkulu
5. Gorontalo
6. Jakarta
7. Jambi
8. Jawa Barat
9. Jawa Tengah
10. Jawa Timur
11. Kalimantan Barat
12. Kalimantan Selatan

13. Kalimantan Tengah
14. Kalimantan Timur
15. Kalimantan Utara
16. Kepulauan Bangka Belitung
17. Kepulauan Riau
18. Lampung
19. Maluku
20. Maluku Utara
21. Nusa Tenggara Barat
22. Nusa Tenggara Timur
23. Papua
24. Papua Barat
25. Riau
26. Sulawesi Barat
27. Sulawesi Selatan
28. Sulawesi Tengah
29. Sulawesi Tenggara
30. Sulawesi Utara
31. Sumatra Barat
32. Sumatra Selatan
33. Sumatra Utara
34. D.I. Yogyakarta



- Uang Saku (Per bulan)
  - < Rp 1.000.000
  - Rp 1.000.000 - 2.999.999
  - Rp 3.000.000 - 4.999.999
  - Rp 5.000.000 - 9.999.999
  - > Rp 10.000.000
- Jenjang Pendidikan yang Ditempuh Saat Ini
  - Diploma 1-4
  - S1
  - Profesi

- S2
- S3
- Jenis Perguruan Tinggi
  - Negeri
  - Swasta
- Jurusan
  - Ilmu Alam (Fisika, Kimia, Biologi, Kehutanan, Pertanian, dll)
  - Ilmu Formal (Matematika, Statistika, Ilmu Komputer, Informatika)
  - Ilmu Kesehatan (Kedokteran, Keperawatan, Farmasi, dll)
  - Ilmu Sosial dan Budaya (Ekonomi, Hukum, Sosiologi, Seni, Filsafat dll)
  - Ilmu Teknik dan Rekayasa (Arsitektur, Sipil, Industri, Mesin, Elektro, dll)

B. Bagian Kedua: Pengetahuan tentang Cyber Security\

| No | Pertanyaan   | Sangat Tidak Setuju (STS) | Tidak Setuju (TS) | Netral (N) | Setuju (S) | Sangat Setuju (SS) |
|----|--|---------------------------|-------------------|------------|------------|--------------------|
| 1  | Saya tahu <i>password</i> yang kuat itu seperti apa  |                           |                   |            |            |                    |
| 2  | Saya tahu apa yang dimaksud dengan <i>password</i> yang unik                                 |                           |                   |            |            |                    |
| 3  | Saya tahu tentang pembaharuan <i>password</i> secara berkala                                 |                           |                   |            |            |                    |
| 4  | Saya tahu jaringan publik mana yang tidak aman   |                           |                   |            |            |                    |
| 5  | Saya tahu risiko-risiko yang ada pada transaksi finansial dan perbankan secara <i>online</i> |                           |                   |            |            |                    |

|    |  |  |  |  |  |  |
|----|--|--|--|--|--|--|
| 6  | Saya tahu apa itu Virtual Private Network(VPN)                 |  |  |  |  |  |
| 7  | Saya tahu VPN yang bisa dipercaya atau tidak dipercaya         |  |  |  |  |  |
| 8  | Saya tahu apa itu SSL dan HTTPS                                |  |  |  |  |  |
| 9  | Saya tahu apa itu Two-Factor Autentications (2FA)              |  |  |  |  |  |
| 10 | Saya tahu apa itu <i>software</i> bajakan (crack, keygen, dll) |  |  |  |  |  |
| 11 | Saya tahu apa itu konten video ilegal/bajakan                  |  |  |  |  |  |
| 12 | Saya tahu apa itu konten pornografi                            |  |  |  |  |  |

C. Bagian Ketiga: Kesadaran akan Cyber Security

| No | Pertanyaan   | Sangat Tidak Setuju (STS) | Tidak Setuju (TS) | Netral (N) | Setuju (S) | Sangat Setuju (SS) |
|----|--|---------------------------|-------------------|------------|------------|--------------------|
| 1  | Saya sadar bahwa <i>password</i> yang kuat bisa mengurangi risiko pembobolan akun                  |                           |                   |            |            |                    |
| 2  | Saya sadar bahwa <i>password</i> yang unik pada setiap akun bisa mengurangi risiko pembobolan akun |                           |                   |            |            |                    |

|   |   |  |  |  |  |  |
|---|---|--|--|--|--|--|
| 3 | Saya sadar jika memperbarui <i>password</i> secara berkala bisa mengurangi risiko pembobolan akun                 |  |  |  |  |  |
| 4 | Saya sadar menggunakan jaringan publik yang tidak aman bisa meningkatkan risiko keamanan akun                     |  |  |  |  |  |
| 5 | Saya sadar bahwa melakukan transaksi finansial atau perbankan saat menggunakan jaringan publik sangat tidak aman  |  |  |  |  |  |
| 6 | Saya sadar fungsi dan manfaat VPN pada saat terhubung di jaringan publik  |  |  |  |  |  |
| 7 | Saya sadar bahwa tidak semua VPN bisa dipercaya   |  |  |  |  |  |
| 8 | Saya sadar fungsi dan manfaat SSL dan HTTPS pada <i>website</i> di Internet                                       |  |  |  |  |  |
| 9 | Saya sadar jika menggunakan Two-Factor Authentications (2FA) saat login akun bisa mengurangi risiko keamanan akun |  |  |  |  |  |

|    |  |  |  |  |  |  |
|----|--|--|--|--|--|--|
| 10 | Saya sadar bahwa menggunakan <i>software</i> bajakan akan berbahaya bagi keamanan perangkat dan data |  |  |  |  |  |
| 11 | Saya sadar risiko dari mengakses situs-situs penyedia konten video ilegal/bajakan                    |  |  |  |  |  |
| 12 | Saya sadar risiko dari mengakses situs-situs penyedia konten pornografi                              |  |  |  |  |  |

D. Bagian Keempat: Kebiasaan terkait Cyber Security

| No | Pertanyaan   | Sangat Tidak Setuju (STS) | Tidak Setuju (TS) | Netral (N) | Setuju (S) | Sangat Setuju (SS) |
|----|--|---------------------------|-------------------|------------|------------|--------------------|
| 1  | Saya menggunakan <i>password</i> yang kuat pada setiap akun  |                           |                   |            |            |                    |
| 2  | Saya menggunakan <i>password</i> yang unik untuk setiap akun |                           |                   |            |            |                    |
| 3  | Saya memperbarui <i>password</i> akun secara berkala         |                           |                   |            |            |                    |
| 4  | Saya hanya menggunakan VPN yang bisa dipercaya saja          |                           |                   |            |            |                    |

|    |  |  |  |  |  |  |
|----|--|--|--|--|--|--|
| 5  | Saya hanya mengunjungi <i>website</i> yang mendukung SSL dan HTTPS                           |  |  |  |  |  |
| 6  | Saya menggunakan Two-Factor Autentications (2FA) untuk login di setiap akun saya             |  |  |  |  |  |
| 7  | Saya menggunakan <i>software</i> bajakan pada perangkat saya                                 |  |  |  |  |  |
| 8  | Saya mengakses situs-situs penyedia konten video ilegal                                      |  |  |  |  |  |
| 9  | Saya mengakses situs-situs penyedia konten pornografi  |  |  |  |  |  |
| 10 | Saya menggunakan VPN saat terhubung di jaringan publik                                       |  |  |  |  |  |
| 11 | Saya menggunakan jaringan publik untuk berinteraksi di dunia siber                           |  |  |  |  |  |
| 12 | Saya menggunakan jaringan publik saat transaksi finansial dan perbankan secara <i>online</i> |  |  |  |  |  |