

Pengukuran Tingkat Kesadaran Keamanan Informasi Mahasiswa pada Pembelajaran Online

Devi Nurjanah^{a1}, Senie Destya^{a2}

^aProgram Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kab. Sleman, Daerah Istimewa Yogyakarta, Indonesia 55281

¹devinurjanah@students.amikom.ac.id

²seniedestya@amikom.ac.id

Abstrak

Tahun 2020 hingga sekarang menjadi tahun dimana teknologi semakin dibutuhkan karena adanya Corona Virus Disease yang mengharuskan seluruh instansi terkait pendidikan melakukan pembelajaran secara online. Penelitian ini dilakukan untuk mengukur tingkat kesadaran keamanan informasi mahasiswa yang melakukan aktifitas online menggunakan platform seperti zoom, google meet, dll dan mengedukasi mahasiswa melalui feedback kuisisioner secara online. Pengukuran masalah ini dilakukan melalui 3 dimensi kesadaran yaitu attitude, behavior, dan knowledge yang bertujuan untuk mengetahui tingkat kesadaran, dengan demikian dapat diformulasikan tindakan yang harus dilakukan agar mengedukasi yang kurang dan mempertahankan yang sudah baik dari hasil presentase akhir. Penelitian ini menggunakan metode Multiple Criteria Decision Analysis (MCDA) dan pengumpulan data menggunakan metode kuisisioner google form. Hasil dari penelitian ini menunjukkan bahwa tingkat kesadaran keamanan informasi mahasiswa berada pada level "sedang" dengan total nilai 66%. Perlu mempertahankan dimensi knowledge yang sudah baik dan memberikan perhatian khusus pada dimensi *attitude* dan *behavior*.

Kata kunci: Keamanan Informasi, MCDA, Kesadaran Keamanan, Dimensi Kesadaran, Daring

Measurement of Students Information Security Awareness Level in Online Learning

Abstract

The year 2020 until now will be the year that technology is increasingly needed due to the corona virus disease that requires all educational institutions to do online learning. This research was conducted to measure the level of information security awareness of students who engage in online activities using platform such as zoom, google meet, etc. and educate students through online questionnaire feedback. Measurement of this problem is done through 3 dimensions of consciousness namely attitude, behavior, and knowledge that aims to know the level of awareness, thus it can be focused actions that must be taken in order to educate the less and maintain the already good of the final percentage results. This research uses the Multiple Criteria Decision Analysis (MCDA) method and data collection using the google form questionnaire method. The results of this study showed that the level of information security awareness of students was at a "moderate" level with a total score of 66%. It is necessary to maintain a good knowledge dimension.

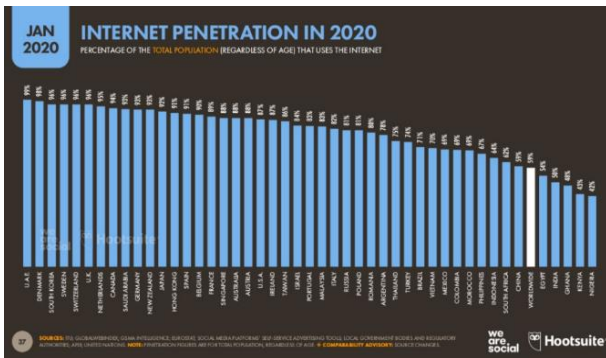
Keywords: Information Security, MCDA, Security Awareness, Dimensions of Consciousness, Online

I. PENDAHULUAN

Berdasarkan data statistik digital Indonesia yang dilansir dari wearesosial.com dapat dilihat pada gambar 1 pada tahun 2020 menunjukkan presentase penggunaan internet yang semakin meningkat pada tahun 2020. Indonesia merupakan salah satu negara yang mengakses internet tertinggi didunia dengan total penduduk mencapai 4,3 milyar yang setengah populasi sekitar 2,14 milyar sudah menggunakan social media. Pada masa pandemic covid19 penetrasi internet total 9,2 % salah satunya penggunaan

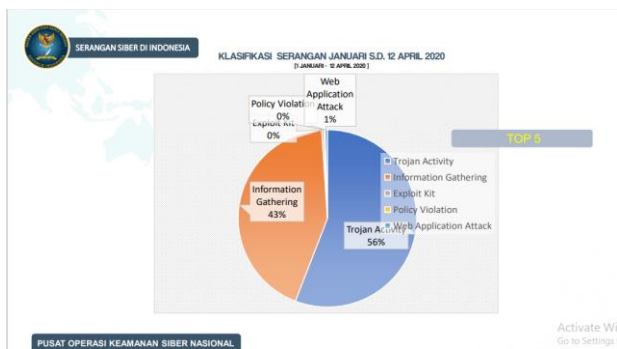
system pembelajaran online. Dari data penggunaan tersebut akan semakin banyak dan membesar celah keamanan yang dengan sendirinya akan terbuka untuk publik.

Dari semua sektor termasuk pendidikan salah satunya dikalangan mahasiswa yang melakukan pembelajaran jarak jauh, yang mewajibkan untuk mengolah dan menggunakan teknologi informasi yang ada untuk penunjang. Banyak sekali manfaat yang didapatkan dan akan berdampak lebih besar negatifnya dari pemanfaatan teknologi tersebut tanpa adanya pembekalan keamanan (*security*).



Gambar 1. Internet penetration 2020

Tidak sedikit contoh kasus-kasus yang terjadi pada kalangan mahasiswa, contoh sederhananya adalah sering kalinya data-data kuliah yang di laptop sering hilang tanpa sebab, karena tidak adanya pengamanan antivirus pada perangkat laptop maupun *smartphone* yang dapat menunjukkan secara *real-time* aktifitas pribadi, penipuan yang mengatas namakan sebuah Instansi melalui email atau SMS dengan tanpa difilter kita mempercayainya dengan mengirimkan beberapa jumlah uang sebagai transaksinya, laptop yang sering kali digunakan untuk pembelajaran online sering kali mendapatkan *top up* iklan yang menarik atau tanpa sengaja meng-klik iklan tersebut yang ternyata adalah sebuah *malware* bahkan memungkinkan untuk para hacker telah mengambil alih akses perangkat. Hal ini menunjukkan bahwa kesadaran terhadap kemandirian masih sangat rendah.



Gambar 2. Klasifikasi serangan pada bulan Januari – April 2020

Berdasarkan gambar 2 dari Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) juga telah melansir jumlah serangan siber mencapai 88.414.296 yang terhitung dari bulan Januari-April 2020 yang di latar belakang isu pandemi covid-19. Para *cyber threat actor* sering sekali memanfaatkan moment-moment tersebut untuk memperoleh keuntungan. Adapun pengelompokkan serangan yang paling tinggi adalah *trojan activity* yang mencapai 56 %.

Pencurian data privasi sangatlah berbahaya, oleh karena itu diperlukan adanya peningkatan pengetahuan dasar terkait *information security awareness* pada mahasiswa untuk mengurangi kasus-kasus tersebut. Peninjauan aspek keamanan informasi dasar yaitu *Confidentiality, Integrity, dan Availability (CIA)* merupakan tiga kesatuan dalam konsep *information protection*.

II. METODOLOGI

A. Konsep E-Learning

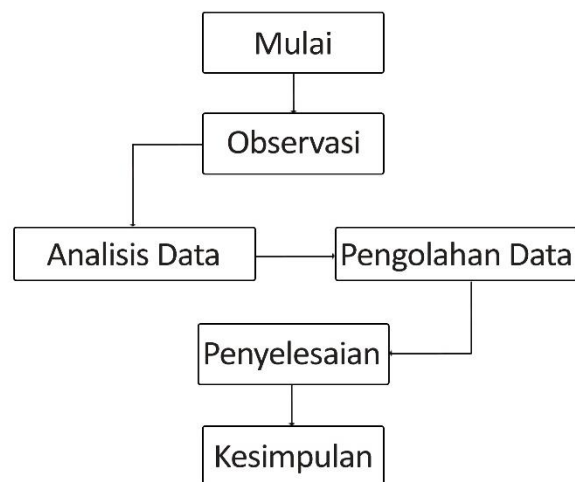
Konsep pendidikan untuk mendukung proses belajar dan mengajar sekarang adalah melalui online atau media pembelajaran yang sering dikenal dengan e-learning. *Learning Management System (LMS)* dilakukan pembaharuan terkait fitur-fitur standar yang akan digunakan dalam pembelajaran, seperti penugasan, fitur ujian online ataupun mandiri, dan lain-lain [1].

B. Keamanan Informasi

Konsep umum keamanan informasi menurut [2] [3] ada beberapa yang dijelaskan antara lain adalah *phising* merupakan usaha yang dilakukan untuk mencuri data atau identitas menggunakan email atau website palsu yang dengan sengaja dibuat hampir sama dengan yang asli, *spam* adalah surat atau pesan elektronik komersial yang tidak diinginkan oleh penerimanya, *social engineering* digunakan untuk mencuri data atau informasi secara pendekatan emosional ataupun visual, dan *strong password* merupakan kunci otentikasi pengguna dan untuk mencegah hal yang tidak diizinkan masuk kedalam hak akses.

C. Pentingnya Keamanan Informasi

Pentingnya kesadaran keamanan informasi menurut [4] mengungkapkan bahwa pengamanan informasi dilaukan bertujuan untuk mengamankan data-data yang sangat penting dan rahasia. Berdasarkan hal itu, pengamanan informasi harus dilakukan untuk menghindari dari ancaman-ancaman yang tidak sah atau kewenangan yang masuk dan menjaga dari kerusakan yang disebabkan oleh pihak luar yang buruk.



Gambar 3. Alur penelitian

Pada gambar 4 merupakan metode penelitian, metode ini akan melewati beberapa proses, yang pertama observasi yaitu melakukan *Kajian Literatur* yang berarti dalam hal ini melakukan pengumpulan referensi dari buku-buku, jurnal hingga penunjang lainnya yang berkaitan dengan penelitian ini contohnya pembuatan soal-soal untuk kuisisioner, penyebaran kuisisioner online (google form) melalui social media merupakan cara yang efektif dan

fleksibel pada masa pandemic covid-19 terkhusus kepada mahasiswa (responden) yang melakukan pembelajaran daring. Pada tahap selanjutnya sesuai dengan gambar 3, area yang diteliti meliputi internet & media pembelajaran online, e-mail dan password, device used, security incidents, dan consequences yang proses pengambilannya dengan metode yang digunakan adalah *Multi Criteria Decision Analysis* (MCDA) melalui beberapa multi choice yang banyak digunakan oleh penelitian sebelumnya dengan objek dan subjek yang sama.

$$v(a) = \sum_{i=0}^n vi(a)wi$$

Rumus diatas adalah rumus persamaan umum menggunakan metode MCDA ini dan metode ini sangat mewakili untuk pengukuran kesadaran keamanan informasi oleh [5] untuk perhitungan menentukan jumlah responden menggunakan rumus perhitungan dari Slovin (dengan nilai margin of error (e) sebesar 0.05) yang digunakan menurut [6] dengan rumus sebagai berikut:

Keterangan :

- n : Jumlah elemen/anggota sampel
- N : Jumlah elemen/anggota populasi
- e : Error Level (tingkat kesalahan pada umumnya)

$$n = \frac{N}{1 + Ne^2}$$

$$n = \frac{112}{1 + (112 * 0.052)} = 112$$

Tahapan selanjutnya dilakukan pengumpulan data dan menganalisis dari hasil kuisioner yang disebarkan dengan jangka waktu yang ditentukan, kuisioner ini terdiri dari 30 pertanyaan terkait keamanan informasi dan 20 pertanyaan terkait pengujian attitude, behavior dan knowledge dalam perspektif keamanan pembelajaran online. Menjadi point terpenting untuk memberikan edukasi mendasar terkait kesadaran keamanan informasi dan privasi adalah adanya feedback dan skor penilaian langsung pada kuisioner, sehingga responden akan mempelajari yang seharusnya dilakukan secara benar. Peneliti menggunakan populasi atau objek dalam penelitian ini adalah mahasiswa yang melakukan system pembelajaran online yang memungkinkan variasi dari latar belakang program studi hingga universitas. Setelah pengumpulan data melalui kuisioner, selanjutnya melakukan pengolahan data dengan menggunakan metode MCDA untuk memetakan penggolongan dalam penilaian per dimensi. Tahap akhir penelitian dengan memberikan kesimpulan dari semua proses yang sudah dilakukan.

Dalam penelitian ini mengadopsi model teori dari [5] merupakan teori psikologi social untuk mengukur 3 dimensi yaitu attitude (sikap para pengguna), knowledge (pengetahuan pengguna) dan behavior (perilaku atau hal yang dapat dilakukan pengguna) untuk setiap area berdasarkan gambar 3. Untuk pengujian yang dilakukan pada setiap pertanyaan kuisioner akan terbagi menjadi 3 skala yaitu benar, tidak tahu dan salah. Pertanyaan itu akan

digunakan untuk menentukan nilai vi(a). Contoh pertanyaan dari kuisioner adalah sebagai berikut :

TABEL I
PERTANYAAN UNTUK DIMENSI KNOWLEDGE

No	Pertanyaan
1	Internet merupakan system komunikasi global yang menghubungkan komputer dengan jaringannya di seluruh dunia.
2	Tidak mengikuti kebijakan atau pedoman keamanan standart merupakan salah satu yang membuat komputer rentan terkena serangan.
3	E-mail perlu digunakan untuk proses pembelajaran online.
4	UU ITE merupakan dasar pengaturan di bidang pemanfaatan teknologi informasi dan transaksi elektronik.
5	Backup data penting untuk mencegah kehilangan data.

TABEL II
PERTANYAAN UNTUK DIMENSI BEHAVIOR

No	Pertanyaan
1	Saya mengetahui adanya UU No 11 Tahun 2008 tentang informasi dan Transaksi Elektronik.
2	Saya menggunakan tanggal lahir dan tanggal special sebagai password.
3	Saya pernah menggandakan file (copy-paste) dari flashdisk yang membawa virus ke laptop.
4	Saya membatasi konten-konten yang saya akses menggunakan leptop atau hp.
5	Backup data yang saya lakukan menggunakan perangkat internet (dropbox, drive, dst)

TABEL III
PERTANYAAN UNTUK DIMENSI ATTITUDE

No	Pertanyaan
1	Saya mengetahui adanya UU No 11 Tahun 2008 tentang informasi dan Transaksi Elektronik.
2	Saya menggunakan tanggal lahir dan tanggal special sebagai password.
3	Saya pernah menggandakan file (copy-paste) dari flashdisk yang membawa virus ke laptop.
4	Saya membatasi konten-konten yang saya akses menggunakan leptop atau hp.
5	Backup data yang saya lakukan menggunakan perangkat internet (dropbox, drive, dst)

Pada tahap akhir perhitungan total yang sudah di proses, peneliti menggunakan penentuan level yang digunakan oleh [1] dalam pengukuran kesadaran keamanan informasi akan diperolehnya nilai yang sudah ditetapkan yaitu baik, sedang dan buruk. Masing-masing level memiliki nilai yang dapat dilihat berikut ini :

TABEL IV
LEVEL TINGKAT KESADARAN KEAMANAN INFORMASI

No	Level	Nilai (%)
1	Baik	80 – 100 %
2	Sedang	60 – 79 %
3	Buruk	0 – 59 %

III. HASIL DAN PEMBAHASAN

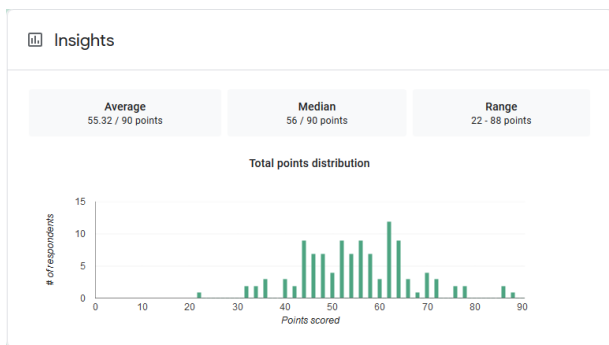
Berdasarkan metode penelitian, setelah menentukan nilai vi(a) selanjutnya melakukan perhitungan perkalian yang ditentukan menggunakan *Analytic Hierarchy Proses* (AHP) dengan cara kerjanya adalah mengidentifikasi masalah yang akan diukur (area pada gambar 1) dengan melakukan perbandingan sejumlah kombinasi elemen

berpasangan dan bergantung pada penilaian ahli untuk memperoleh skala prioritas dengan menggunakan angka pritoritas menurut [7] yang disesuaikan dengan permasalahan. Kemudian dekomposisi masalahnya atau memecah persoalan dengan menyusun struktur hirarki. Menurut [8] Pendekatan AHP memungkinkan kita melakukan pair comparasion terhadap masing-masing kriteria kesadaran keamanan informasi. Hasil dari penelitian ini akan lebih mudah disajikan dalam bentuk matriks *pairwise comparisons* yaitu skala perbandingan berpasangan yang memuat beberapa alternative pada setiap kriteria. Berdasarkan hasil penelitian, sampel penelitian ini melibatkan 112 responden atau mahasiswa dari semua jurusan yang berbeda seperti, Pendidikan Matematika, Agribisnis, Kewirausahaan, Pendidikan Agama Islam, dst. Kemudian peneliti mengelompokkan berdasarkan tahun angkatan serta jumlah responden agar mempermudah perhitungan, seperti tahun 2019, 2018, dan 2017. Berdasarkan tujuan dan metode pengumpulan data penelitian ini, dari 114 hanya menjadi 112 mahasiswa yang memenuhi syarat untuk pengambilan sampel objek. Dapat dilihat pada tabel berikut ini :

TABEL V
JUMLAH RESPONDEN

No	Tahun Semester	Jumlah Responden
1	2017	40
2	2018	49
3	2019	23
Total		112

Pada tabel 5 diatas dapat dijelaskan pendistribusian responden secara mentah atau belum diolah ke dalam metode dan sesuai dengan *google form* yang sudah disebarakan dapat dilihat pada gambar dibawah ini :



Gambar 4. *Insight* responden.

Berdasarkan responden penelitian, menunjukkan bahwa sebagian besar adalah responden berasal dari tahun 2018 atau semester 5 dan untuk skala preferensi yang digunakan yaitu skala 1 yang berarti pada tingkatan yang paling rendah (*equal importance*) sampai dengan skala 9 yang bererati pada tingkatan yang paling tinggi (*extreme importance*). Penentuan bobot nilai dilakukan perhitungan eigen value dari matrik. Pembobotan yang digunakan oleh [5] seperti tabel berikut ini :

TABEL VI
HASIL BOBOT DIMENSI

No	Dimensi	Bobot
1	Knowledge	30
2	Behavior	40
3	Attitude	20

Untuk langkah selanjutnya, perhitungan matriks *pairwise comparisons* sebagai penentuan akhir penelitian ini yang sudah dijelaskan sebelumnya, pada matriks ini pada setiap kolom tabelnya diisi dengan kriteria penilaian pada sesuai dengan skala yang sudah diberikan ($w_1/w_1, w_1/w_2, w_1/3, \text{dst}$), kemudian tahap selanjutnya untuk rumus proses perhitungan total skor nilai pada setiap dimensi per area yang digunakan oleh [6] dapat dituliskan pada tabel berikut ini :

TABEL VII
PERHITUNGAN TOTAL NILAI

Dimensi	Area					Total Nilai
	A1	A2	A3	A4	A5	
Knowledge	A11	A21	A31	A41	A51	
Attitude	A12	A22	A32	A42	A52	
Behavior	A13	A23	A33	A43	A53	
Total Nilai						

Pada tabel VII diatas dilakukan penjumlahan per area kemudian di bagi dengan 3 menurun atau $\sum_{i=1}^3 Ai/3$ dan untuk 6 mendatar $\sum_{i=1}^6 Ai/6$ begitu seterusnya hingga nilai total skor terpenuhi.

TABEL VIII
PERHITUNGAN TOTAL NILAI

Dimensi	Area					Total Nilai
	A1	A2	A3	A4	A5	
Knowledge	A11	A21	A31	A41	A51	
Attitude	A12	A22	A32	A42	A52	
Behavior	A13	A23	A33	A43	A53	
Total Nilai						

Dapat diketahui dari tabel 8 *local Priority (TPV)* yaitu total nilai keseluruhan menunjukkan nilai kesadaran keamanan informasi yang diperoleh dari semua area adalah sebesar 66 %. Berdasarkan tabel 5 menunjukkan bahwa level kesadaran keamanan informasi pada mahasiswa yang melakukan pembelajaran daring berada pada level “sedang”. Jika kita jabarkan pada setiap dimensi, dimensi *Knowledge* menunjukan total sebesar 86 % yang berarti dimensi ini berada pada level “baik” sehingga hanya perlu dipertahankan. Pada dimensi *Attitude* menunjukkan total sebesar 56 % yang berarti masih berada pada kategori “buruk”, hal ini dapat disimpulkan bahwa *attitude* pada mahasiswa yang melakukan pembelajaran online perlu banyak pembenahan atau perbaikan yang berupa sosialisasi atau himbauan terkait menjaga kesadaran keamanan informasi. Pada dimensi *Behavior* menunjukkan total sebesar 58 % yang dimana kategori ini masih berada pada level “buruk”, seperti hal nya pada dimensi sebelumnya yang perlu mendapatkan perhatian khusus untuk menindak lanjuti kekurangan tersebut.

IV. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan, secara umum level kesadaran keamanan informasi mahasiswa yang melakukan pembelajaran online sudah berada pada level “sedang” dengan total perhitungan nilai keseluruhan mencapai 66 %. Dengan demikian perlu dipertahankan yang baik dan perlu peningkatan pada mahasiswa yang berada pada level rendah. Perlu tindakan monitoring berkelanjutan setelah adanya *feedback* dari kuisioner untuk memastikan peningkatan yang terjadi setelah itu. Diperlukan juga adanya Kerjasama antara semua pihak yang terkait untuk peningkatan kesadaran keamanan informasi. Dari hasil penelitian, perlu ditingkatkan bagian dimensi *Behavior* dan *Attitude* dapat dilakukan peningkatan khusus pada dimensi ini serta upaya-upaya pembenahan kesadaran keamanan informasi seperti pihak lembaga perguruan tinggi perlu tindakan khusus untuk menangani hal tersebut, memberikan sosialisasi atau himbauan secara online dan memperingatkan untuk tetap berhati-hati dalam penggunaan perangkat yang digunakan dalam pembelajaran online, dengan mengikuti aturan dari pemerintah pada masa pandemi ini.

Saran yang diberikan dalam penelitian ini adalah melakukan penambahan responden segala jenjang pendidikan agar dapat menelaah secara *continue* permasalahan yang sering menjadi celah dalam kesadaran keamanan informasi dikarenakan semua jenjang pendidikan menggunakan perangkat yang terhubung dengan internet dan dapat mengedukasi *security awareness* pengguna internet.

DAFTAR PUSTAKA

- [1] A. Ratnasari, “Studi Pengaruh Penerapan E-Learning Terhadap Keaktifan Studi Kasus Universitas Mercu Buana Jakarta,” *Semin. Nas. Apl. Teknol. Inf.* 2012, vol. 2012, no. Snati, pp. 15–16, 2012.
- [2] S. Destya, “Model Pengukuran Tingkat Kesadaran Keamanan,” pp. 19–24, 2018.
- [3] P. Jati Sekar Agri, “Evaluasi Tingkat Kesadaran Keamanan Informasi Mahasiswa Akuntansi Universitas Sanata Dharma,” Universitas Sanata Dharma, 2019.
- [4] D. Ariyus, *Kemanan Multimedia*. Yogyakarta: ANDI, 2009.
- [5] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.
- [6] Dafid and Dorie, “Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 1, pp. 11–20, 2020.
- [7] M. Amin, “Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (McdA),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, p. 122371, 2014.
- [8] M. Amin, “Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (McdA),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, pp. 15–24, 2014.
- [9] D. C. Islami, K. B. I.H, and C. Candiwan, “Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia,” *J. INKOM*, vol. 10, no. 1, p. 19, Nov. 2016.
- [10] R. Akraman, C. Candiwan, and Y. Priyadi, “Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia,” *J. Sist. Inf. Bisnis*, vol. 8, no. 2, p. 115, 2018.
- [11] V. Tobing, “Insiden web defacement,” 2013. .
- [12] EC-Council, “Protecting Systems Using Antiviruses,” pp. 1–32.
- [13] EC-Council, “Securing Email Communications,” pp. 1–42.
- [14] EC-Council, “Internet security,” *Comput. Commun.*, vol. 29, no. 3, p. 279, 2006.
- [15] L. Laurentinus, H. A. Pradana, D. Y. Sylfania, and F. P. Juniawan, “Performance comparison of RSA and AES to SMS messages compression using Huffman algorithm,” *J. Teknol. dan Sist. Komput.*, vol. 8, no. 3, pp. 171–177, 2020.
- [16] EC-Council, *Fondasi Keamanan Skenario*.
- [17] M. Amin, “Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (McdA),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, pp. 15–24, 2014.