Journal on Education
Volume 06, No. 02, Januari-Februari 2024, pp. 14227-14236
E-ISSN: 2654-5497, P-ISSN: 2655-1365
Website: http://jonedu.org/index.php/joe

Analisis *Cyber Awareness* terhadap Keamanan Data Pribadi dari Serangan Siber menggunakan Metode AHP

Ayu Astridefi[1], Rudy A.G. Gultom[2], Yudistira Dwi Wardhana Asnar[3]

[1,2]Universitas Pertahanan Republik Indonesia, Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kab. Bogor, Jawa Barat
[3]Institut Teknologi Bandung, Jl. Ganesa No.10, Lb. Siliwangi, Kecamatan Coblong, Kota Bandung, Jawa Barat
ayuastridefi@gmail.com

Abstract

With the increasing number of cyber-attacks and data breaches, individuals and organizations must be proactive in protecting their sensitive personal data and information. Personal data security is a critical concern as individuals and organizations face increasing threats from cyber-attacks. One effective way to evaluate and improve personal data security is through the use of the Analytic Hierarchy Process (AHP) method. This paper presents a study that utilizes AHP to analyze the level of cyber awareness among individuals and the effect it has on the security of their personal data. A survey was conducted to gather data from a sample group of individuals, and the results were analyzed using AHP. The results of the study showed that there is a positive correlation between an individual's level of cyber awareness and the security of their personal data. The study also identified areas where individuals can improve their cyber awareness and, in turn, increase the security of their personal data. This research contributes to the field of personal data security by providing a practical and effective method for evaluating and improving an individual's cyber awareness.
Keywords: AHP Method, Cyber Awareness, Personal Data Security, Data Breach, Cyber-Attacks

Abstrak

Dengan meningkatnya jumlah serangan siber dan pelanggaran data, individu dan organisasi harus proaktif dalam melindungi data pribadi dan informasi sensitif mereka. Keamanan data pribadi adalah kekhawatiran kritis karena individu dan organisasi menghadapi ancaman yang meningkat dari serangan siber. Salah satu cara efektif untuk mengevaluasi dan meningkatkan keamanan data pribadi adalah melalui penggunaan metode Proses Hirarki Analitik (AHP). Makalah ini menyajikan sebuah studi yang memanfaatkan AHP untuk menganalisis tingkat kesadaran siber di kalangan individu dan efeknya terhadap keamanan data pribadi mereka. Sebuah survei dilakukan untuk mengumpulkan data dari kelompok sampel individu, dan hasilnya dianalisis menggunakan AHP. Hasil studi menunjukkan bahwa ada korelasi positif antara tingkat kesadaran siber seseorang dan keamanan data pribadi mereka. Studi ini juga mengidentifikasi area di mana individu dapat meningkatkan kesadaran siber mereka dan, pada gilirannya, meningkatkan keamanan data pribadi mereka. Penelitian ini memberikan kontribusi pada bidang keamanan data pribadi dengan menyediakan metode praktis dan efektif untuk mengevaluasi dan meningkatkan kesadaran siber seseorang.
Kata kunci: Metode AHP, Cyber Awareness, Keamanan Data Pribadi, Pencurian Data, Serangan Siber

Copyright (c) 2024 Ayu Astridefi, Rudy A.G. Gultom, Yudistira Dwi Wardhana Asnar

✉Corresponding author: Ayu Astridefi
Email Address: ayuastridefi@gmail.com (Kawasan IPSC Sentul, Kec. Citeureup, Kab.Bogor, Jawa Barat)
Received 26 January 2024, Accepted 30 January 2024, Published 5 February 2024

PENDAHULUAN

Keamanan siber telah menjadi komponen integral dari sistem yang terhubung internet dalam hal perlindungan sistem tersebut. Keamanan siber menyediakan pendekatan proaktif terhadap mitigasi serangan siber pada data akademis dan informasi pribadi, yang mengakibatkan pelanggaran data dan pencurian identitas (Alzighaibi, 2021). Keamanan siber diterapkan sebagai respons terhadap serangan siber yang terus menerus menargetkan dan mencuri informasi pribadi orang. Serangan siber adalah upaya jahat dan sengaja oleh seseorang atau organisasi untuk melanggar sistem informasi orang atau organisasi lain. Biasanya, penyerang berharap mendapatkan sesuatu dari mengganggu jaringan korban (Cisco, dsb). Biasanya, penyerang menggunakan berbagai metode untuk melakukan serangan siber,

tetapi salah satu yang paling umum adalah pelanggaran data.

Pelanggaran data adalah akses tidak sah ke data sensitif dan mengungkapkannya ke seluruh dunia. Ini adalah salah satu masalah paling penting dan serius dalam dekade ini. Peneliti ingin memberikan pemahaman yang jelas tentang pelanggaran data, masalah keamanan, dan pengelolaan ancaman siber. Pelanggaran data adalah tindakan menyebarkan data sangat sensitif yang dimaksudkan untuk dirahasiakan. Mengungkapkan data ke domain yang tidak aman baik dengan motif atau tidak sengaja. Hal ini terjadi ketika pihak ketiga atau individu yang tidak sah mencoba mencuri atau mengakses data yang mungkin mencakup rahasia puncak, saham perusahaan, rincian transaksi, atau informasi hukum. Ada berbagai jenis pelanggaran data yang meliputi phishing, serangan penolakan layanan, malware, dan ekstraksi. Dari waktu ke waktu, kita mendengar tentang beberapa perusahaan dan industri mengumumkan bahwa sistem mereka telah diretas. Hal ini mungkin terjadi melalui aktivitas ilegal penyusup. Atau juga oleh individu di dalam organisasi (Dr. Veena.S, 2018).

Menurut spicework.com pada Oktober 2022, Toyota mengalami pelanggaran data setelah peretas memperoleh kredensial untuk salah satu servernya dari kode sumber yang dipublikasikan di GitHub oleh subkontraktor pengembangan web. Pihak ketiga "secara tidak sengaja mengunggah sebagian kode sumber ke akun GitHub mereka sementara itu diatur menjadi publik," menurut perusahaan. Akibatnya, perusahaan menyatakan bahwa sebanyak 296,019 alamat email pelanggan dan nomor manajemen pelanggan bocor (Wadhwani, 2022).

Seiring kita mengetahui pertumbuhan serangan siber, terutama dalam pelanggaran data, data menjadi lebih kritis dan relevan dari sebelumnya. Kemajuan teknologi dan aplikasi baru, seperti sensor, sistem siber-fisik, perangkat seluler pintar, sistem cloud, analitik data, jejaring sosial, Internet of Things (IoT), dan kesehatan pintar dan terhubung, memungkinkan pengumpulan, penyimpanan, dan pemrosesan jumlah data yang sangat besar, yang disebut big data, tentang segala hal dari mana saja dan kapan saja. Ada tiga kebutuhan keamanan data dasar yang diidentifikasi: Kerahasiaan, mengacu pada perlindungan data dari akses yang tidak sah; Integritas, mengacu pada perlindungan data dari modifikasi yang tidak sah; dan Ketersediaan, mengacu pada memastikan bahwa data tersedia untuk pengguna yang sah. Ketiga kebutuhan ini masih sangat kritis hari ini. Namun, memenuhi kebutuhan tersebut saat ini jauh lebih menantang karena serangan data lebih canggih dan permukaan serangan data telah berkembang, karena meningkatnya aktivitas pengumpulan data dari berbagai sumber yang berbeda dan berbagi data. Selain tiga kebutuhan ini, privasi telah muncul sebagai kebutuhan kritis baru. Sering kali privasi data dilihat sebagai kebutuhan yang sama dengan kerahasiaan data. Privasi data membutuhkan memastikan kerahasiaan data karena jika data tidak dilindungi dengan baik terhadap akses yang tidak sah, privasi tidak dapat dijamin. Privasi memiliki masalah tambahan yang berasal dari kebutuhan untuk mempertimbangkan persyaratan dari peraturan privasi hukum serta preferensi privasi individu (Bertino, 2016).

Dengan pentingnya privasi data, setiap orang harus menyadari keamanan informasi data mereka sendiri. Kesadaran keamanan informasi dipengaruhi oleh pengetahuan, sikap, dan perilaku. Faktor

utama dalam risiko keamanan informasi adalah tingkat kesadaran keamanan siber individu, yang dapat digambarkan secara berguna sebagai rendah, sedang, atau tinggi. Perilaku kesadaran rendah termasuk tidak memperhatikan atau mengabaikan peringatan keamanan, yang dalam kebanyakan kasus disediakan secara otomatis oleh aplikasi, seperti saat mengakses jaringan terbuka gratis (seperti Wi-Fi) dengan perangkat seluler dan laptop. Tingkat kesadaran sedang mungkin ditandai oleh kelalaian yang diekspresikan dalam operasi teknologi yang tidak tepat. Akhirnya, kesadaran tinggi melibatkan pengetahuan tentang ancaman siber dan tindakan yang mampu diambil dalam pencegahannya. Karena faktor manusia telah ditunjukkan sebagai penyebab utama pelanggaran siber, semakin banyak program pelatihan kesadaran siber yang ditawarkan oleh institusi akademis dan perusahaan swasta, dengan tujuan meningkatkan kesadaran kejahatan siber individu (Moti Zwilling, 2020).

Talal Alharbi mengatakan Keamanan informasi sangat penting bagi institusi akademis, di mana sebagian besar pengguna tidak memiliki pengetahuan tentang konsep dasar keamanan siber atau praktik terbaik tentang cara melindungi perangkat mereka dari malware, virus, dan penipuan. Dalam penelitian ini, mereka mengevaluasi pengetahuan keamanan siber di kalangan mahasiswa di Universitas Majmaah, yang berlokasi di Arab Saudi, melalui pendekatan penelitian kuantitatif. Secara keseluruhan, mereka secara matematis menunjukkan bahwa program kesadaran dan pelatihan keamanan siber untuk mahasiswa harus dimasukkan dalam rencana manajemen keamanan dan dipromosikan dengan kuat oleh eksekutif dan manajer puncak. Institusi akademis perlu menyelenggarakan sesi kesadaran dan pelatihan keamanan secara komprehensif secara rutin untuk memastikan bahwa semua pengguna tahu cara mengenali ancaman dan kerentanan keamanan siber yang paling umum (Talal Alharbi, 2021).

Luthfi Febriansyah mengatakan menangani kasus yang melibatkan penggunaan teknologi informasi seringkali memerlukan penggunaan forensik. Forensik adalah investigasi dan penentuan fakta dalam kasus pidana dan masalah hukum lainnya. Forensik digital adalah cabang ilmu forensik yang berurusan dengan penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (komputer, smartphone, tablet, PDA, perangkat jaringan, penyimpanan, dan sebagainya). Dia menggunakan Metode AHP (*Analytical Hierarchy Process*) untuk *Cyber-Terrorism*, Sebagai hasilnya, *Early Warning Systems* dapat digunakan untuk mendapatkan target baru dari kasus yang sedang berlangsung menggunakan metode AHP (*Analytical Hierarchy Process*) dengan mengikuti langkah-langkah ini: menentukan kriteria, menimbang yang proporsional dengan pentingnya, memilih alternatif, dan Berdasarkan hasil tes dan analisis pada sebelumnya, ditentukan bahwa alternatif 3 adalah prioritas utama dan target baru untuk produk intelijen (informasi khusus) (Luthfi Febriansyah, 2018).

Balqis Rofiqoh Chasanah mengatakan berdasarkan survei mereka, mereka menemukan bahwa kesadaran keamanan siber mahasiswa universitas Indonesia memenuhi standar yang baik (80%). Ada beberapa area fokus yang harus ditangani untuk perbaikan potensial. Di sisi pengetahuan, Anda dapat

mencapai persentase yang lebih tinggi dengan menangani dan memperbaiki malware. Di sisi perilaku, bagaimanapun, kita memiliki keamanan kata sandi, phishing, malware, dan akhirnya mengunduh, berbagi, dan menggunakan perangkat lunak bajakan. Berdasarkan temuan kami, ada beberapa hal yang dapat dilakukan pemerintah dan komunitas, terutama mahasiswa, untuk meningkatkan kesadaran dan memastikan keselamatan saat menggunakan Internet, termasuk informasi pribadi. Penelitian ini memiliki beberapa keterbatasan. Seperti penelitian lainnya, responden yang terlibat tidak selalu lebih mewakili populasi. Juga, survei ini tidak selalu mewakili topik keamanan siber yang lebih luas. Oleh karena itu, kami berharap metode dan kerangka kerja akan ditingkatkan melalui berbagai perkembangan dalam studi berikutnya. Survei kesadaran keamanan siber kualitatif yang lebih mendalam dengan fokus rinci, seperti berbagai set objek yang beragam (Balqis Rofiqoh Chasanah, 2020).

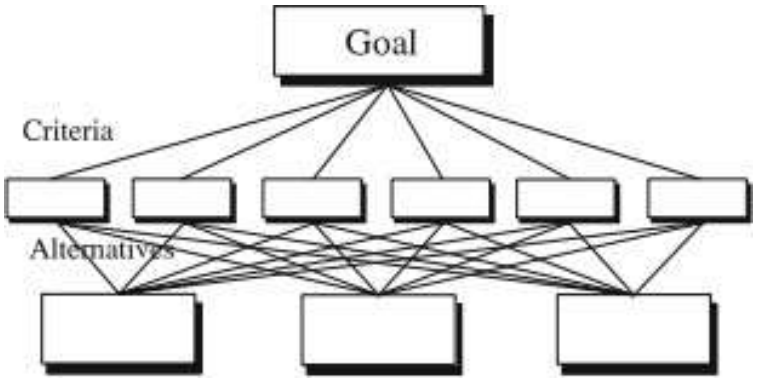
Irfan Syamsuddin mengatakan penelitian ini membenarkan penggunaan metodologi AHP untuk menyelesaikan penilaian keamanan informasi. Seperti yang diungkapkan oleh penelitian ini, AHP memberikan perlakuan yang kuat dan komprehensif baik secara kualitatif maupun kuantitatif kepada pengambil keputusan. Mereka menggunakan model AHP untuk menunjukkan bagaimana itu dapat membantu pengambil keputusan mengevaluasi implementasi kebijakan keamanan informasi mereka. Dari sudut pandang keamanan informasi, dibandingkan dengan aspek ekonomi dan budaya, aspek administratif dan teknis adalah yang paling menjadi perhatian. Kerahasiaan dan integritas mengikuti. Rekomendasi utama yang diambil dari penelitian ini adalah untuk mempromosikan kesadaran keamanan informasi melalui pendidikan keamanan dan tata kelola organisasi. Kami ingin memperluas pada kelompok responden lainnya, seperti industri dan universitas, untuk menjelajahi lebih lanjut. Pendekatan ini memungkinkan untuk melakukan studi komparatif untuk menganalisis kesamaan atau perbedaan antar kelompok yang berbeda (Irfan Syamsuddin, 2009).

Subramanian Vaithyasubramanian menjelaskan dalam jurnalnya, otentikasi dua faktor meningkatkan tingkat keamanan faktor otentikasi tunggal. Penelitian ini berfokus pada penerapan teknik otentikasi dua faktor yang menggunakan kata sandi alfanumerik grafis dan standar, yang ramah pengguna sebagai gerbang otentikasi. Otentikasi dua faktor telah dicoba, dan dalam pekerjaan ini, mereka membahas desain sistem dan implementasi desain untuk otentikasi dua faktor. Memiliki kata sandi kedua yang tersedia menawarkan lapisan keamanan lain (Subramanian, A, & Dhanavel, 2015).

Berdasarkan latar belakang dan dari penelitian sebelumnya yang telah dijelaskan sebelumnya, formulasi penelitian kami difokuskan pada apa faktor-faktor paling penting yang mempengaruhi tingkat kesadaran siber individu dan dampaknya terhadap keamanan data pribadi mereka. Selanjutnya, tujuan penelitian adalah untuk menunjukkan bahwa ada hubungan positif antara tingkat kesadaran siber seseorang dan keamanan data pribadi mereka. Penelitian ini juga telah mengidentifikasi area di mana orang dapat meningkatkan kesadaran siber mereka dan, akibatnya, keamanan data pribadi mereka.

METODE

Dalam penelitian ini, peneliti menggunakan Proses Hirarki Analitik (AHP) yang merupakan pendekatan mendasar dalam pengambilan keputusan. Pendekatan ini dimaksudkan untuk menangani baik aspek rasional maupun intuitif dalam rangka memilih opsi terbaik dari sejumlah alternatif berdasarkan berbagai kriteria. Dalam proses ini, pembuat keputusan melakukan penilaian perbandingan berpasangan yang sederhana, yang kemudian digunakan untuk mengembangkan prioritas keseluruhan untuk meranking alternatif. AHP memungkinkan adanya inkonsistensi dalam penilaian sambil juga menyediakan cara untuk meningkatkan konsistensi. Struktur paling dasar untuk masalah keputusan adalah hierarki tiga tingkat, dengan tingkat atas yang terdiri dari tujuan keputusan, diikuti oleh tingkat kedua yang terdiri dari kriteria di mana alternatif, yang berada di tingkat ketiga, akan dievaluasi (Thomas L. Saaty, 2012).



Gambar 1. Hirarki Tiga Tingkat

Penelitian ini dilakukan sebagai bagian dari proses penentuan kriteria yang tepat untuk kesadaran siber pribadi. Kemudian, penelitian ini dilanjutkan dengan menggunakan proses pengumpulan data acak untuk menentukan tingkat urgensi dari setiap kriteria kesadaran siber pribadi. Proses ini kemudian dilanjutkan dengan menghitung setiap kriteria yang ada untuk membuat matriks. Setiap kriteria akan mendapatkan skala peringkat untuk menentukan pentingnya setiap kriteria. Penelitian ini menggunakan Excel sebagai alat dalam perhitungannya. Lembar kerja Excel ini digunakan untuk menganalisis setiap kriteria kesadaran siber yang paling penting.

Tabel 1. Skala Fundamental

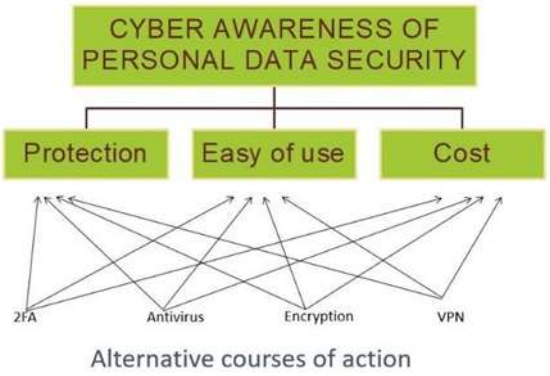
Intensitas Kepentingan	**Definisi**	**Penjelasan**
1	Equal Importance	Dua kegiatan berkontribusi sama besar terhadap tujuan
2	Weak	
3	Moderate Importance	Pengalaman dan penilaian sedikit mengutamakan satu aktivitas daripada aktivitas lainnya
4	Moderate plus	
5	Strong Importance	Pengalaman dan penilaian sangat mendukung satu aktivitas di atas yang lain

6	Strong Plus	
7	Very Strong or Demonstrated Importance	Suatu kegiatan sangat disukai sangat
8	Extreme Importance	
9	Extreme Importance	Bukti yang mendukung satu aktivitas atas yang lain adalah dari urutan tertinggi yang mungkin penegasan
Reciprocals of above	Jika aktivitas *i* memiliki salah satu angka bukan nol di atas yang diberikan kepadanya jika dibandingkan dengan aktivitas *j*, maka *j* memiliki nilai kebalikannya jika dibandingkan dengan *i*	Asumsi yang wajar
Rationals	Rasio yang timbul dari skala	Jika konsistensi dipaksakan dengan mendapatkan nilai numerik untuk menjangkau matriks

HASIL DAN DISKUSI

Hierarki

Tujuan dari penelitian ini adalah untuk mengevaluasi kesadaran siber akan keamanan data pribadi dengan menggunakan kriteria berikut: perlindungan, kemudahan penggunaan, dan biaya. Kriteria ini dibuat sesuai dengan masalah keamanan pribadi.



Gambar 2. Hirarki Desain AHP

Kriteria Berpikir

Tabel 2. memiliki matriks pemikiran kriteria yang mencakup perlindungan, kemudahan penggunaan, dan biaya sebagai kriteria.

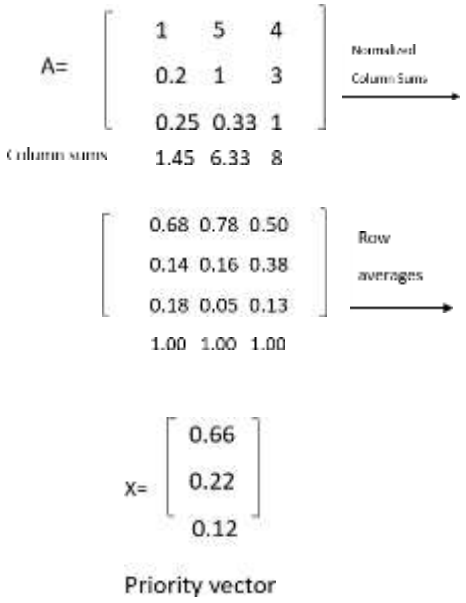
Tabel 2. Matrik Kriteria Berpikir

Criteria	Proteksi	Ease of Use	Cost
Proteksi	1	5	4
Ease of Use	1/5	1	3
Cost	1/4	1/3	1

Pemeringkatan Prioritas

Tabel 2 memberikan peringkat perhitungan prioritas, peringkat tertinggi berasal dari

perlindungan dengan nilai 0,66, hasil kedua adalah kegunaan dengan nilai 0,22, dan hasil terakhir adalah biaya dengan nilai 0,12. Terdiri dari matriks 3x3.



Eigen Value = 1.45x0.66 + 6.33x0.22 + 8x0.12

= 0.975+1.3926+0.96

= 3.3276

CI = 3.3276-3 / 3-1

= 0,1638

CR = 0.1638 / 3.3276

= 0.049225

Alternatif

Tabel 3 adalah tabel alternatif untuk AHP dengan sub-kriteria yang terdiri dari otentikasi dua faktor, perangkat lunak antivirus, enkripsi, dan VPN (virtual private network), serta memberikan skor antara kriteria perlindungan, kegunaan, dan biaya untuk dibandingkan.

Tabel 3.Tabel Alternatif AHP

Protection	**Two-factor authentication**	**Antivirus software**	**Encryption**	**Virtual private network (VPN)**	**Priority Vector**
Two-factor authentication	1,00	3,00	2,00	2,00	0,522977729
Antivirus software	0,33	1,00	3,00	0,25	0,221985973
Encryption	0,50	0,33	1,00	0,33	0,152806694
Virtual					

private network (VPN)	0,50	4,00	3,00	1,00	0,435562938
	2,33	8,33	9,00	3,58	
Eigen Value:	6,01	CI:	1,50	CR:	0,25

Ease of Use	**Two-factor authentication**	**Antivirus software**	**Encryption**	**Virtual private network (VPN)**	**Priority Vector**
Two-factor authentication	1,00	0,33	4,00	0,33	0,270729715
Antivirus software	3,00	1,00	2,00	0,50	0,370390202
Encryption	0,25	0,50	1,00	0,50	0,163438122
Virtual private network (VPN)	3,00	2	2	1,00	0,528775295
	7,25	3,83	9,00	2,33	
Eigen Value:	6,09	CI:	1,54	CR:	0,25

Cost	**Two-factor authentication**	**Antivirus software**	**Encryption**	**Virtual private network (VPN)**	**Priority Vector**
Two-factor authentication	1,00	5,00	2,00	5,00	0,67408113
Antivirus software	0,20	1,00	3,00	0,50	0,248541716
Encryption	0,50	0,33	1,00	2,00	0,230766055
Virtual private network (VPN)	0,20	2,00	0,50	1,00	0,179944431
	1,90	8,33	6,50	8,50	
Eigen Value:	6,38	CI:	1,69	CR:	0,26

Berat Komposit

Tabel 4 menunjukkan bobot sintetis untuk metode AHP. Metode ini merupakan varian dari Proses Hirarki Analitis (AHP), sebuah teknik terstruktur untuk mengevaluasi dan membandingkan alternatif yang kompleks. Bobot komposit kemudian dapat digunakan untuk mengevaluasi dan membandingkan alternatif, dengan bobot komposit yang lebih tinggi menunjukkan tingkat kepentingan yang lebih tinggi.

Tabel 4. Komposit

Composite Weight	**Protection**	**Ease of use**	**Cost**	**Overall Score**
Two-factor authentication	0,52	0,27	0,67	0,486

Antivirus software	0,22	0,37	0,25	0,258
Encryption	0,15	0,16	0,23	0,165
Virtual private network (VPN)	0,44	0,53	0,18	0,425
Weight	0,66	0,22	0,12	

KESIMPULAN

Penelitian ini memberikan kontribusi pada bidang keamanan data pribadi dengan menyediakan metode praktis dan efektif untuk mengevaluasi dan meningkatkan kesadaran siber individu. Eksperimen kami berhasil menunjukkan pentingnya otentikasi dua faktor dalam kesadaran siber data pribadi. Nilainya adalah 0,486. Kemudian, dengan nilai 0,425, tambahkan jaringan pribadi virtual (VPN), nilai 0,258 untuk perangkat lunak antivirus, dan nilai 0,165 untuk enkripsi. Eksperimen ini masih dapat diperluas dengan menggunakan nilai yang berbeda dalam metode AHP atau dengan menggunakan metode analisis perhitungan lainnya.

REFERENSI

Alzighaibi, A. R. (2021). Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment.. *Journal of Computer and Communications*, 77-90.

Balqis Rofiqoh Chasanah, C. (2020). Analysis of College Students' Cybersecurity Awareness In Indonesia. *SISFORMA: Journal of Information Systems* , 49- 57.

Bertino, E. (2016). Data Security and Privacy . *IEEE 40th Annual Computer Software and Applications Conference*, 400- 407.

Cisco. (n.d.). *What Is a Cyberattack?* Retrieved from CIsco: https://www.cisco.com/c/en/us/products/security/common- cyberattacks.html

Dr.Veena.S, D. M. (2018). STUDY OF CYBERSECURITY IN DATA BREACHING. *Scientific Journal of Impact Factor*, 1513-1516.

Irfan Syamsuddin, J. H. (2009). The Application of AHP to Evaluate The Application of AHP to Evaluate. *IJSSST*.

Luthfi Febriansyah, I. R. (2018). ANALYSIS ON PREDICTING CYBER TERRORISM USING AHP (ANALYTICAL HIERARCHY PROCESS) METHOD. *Journal of Theoretical and Applied Information Technology*, 7563-7575.

Subramanian, V., A, C., & Dhanavel, S. (2015, January). Two factor authentications for secured login in support of effective information preservation and network security.

Talal Alharbi, A. T. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *MDPI Big Data and Cognitive Computing*.

Thomas L. Saaty, L. G. (2012). *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. U.S: Springer.

Wadhwani, S. (2022, October 11). *Toyota Suffers Data Breach from "Mistakenly" Exposed Access Key on GitHub*. Retrieved from spiceworks: https://www.spiceworks.com/it- security/data-security/news/toyota-data-breach/