

Analisis Persepsi Mahasiswa Fakultas Ilmu Komputer Terhadap Keamanan Sistem Infomasi Akademik Di Universitas Bhayangkara Jakarta Raya

Aziz Salim Adlianto ¹, Daniel Kristiano Dali ^{1,*}, Fadilah Zahra ¹, Sheila Muhammad

¹Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya, Bekasi Utara Jawa Barat, 17143, (021) 88955882, e-mail: 202110715027@mhs.ubharajaya.ac.id, 202210715046@mhs.ubharajaya.ac.id, 202310717001@mhs.ubharajaya.ac.id, 202210715029@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715046@mhs.ubharajaya.ac.id

Diterima: 4 Jan 25; Review: 5 Jan 25; Disetujui: 7 Jan 25; Diterbitkan: 11 Jan 25

Abstract

This research aims to analyze the perceptions of students at the Faculty of Computer Science, Bhayangkara University, Greater Jakarta regarding the security of the academic information systems used. Academic information system security is a crucial aspect for protecting personal data, academic records and other important information from potential security threats. Using a quantitative approach, data was collected through a survey of a number of randomly selected students. The research results show that the majority of students have a positive perception of the security of academic information systems, although there are some concerns regarding potential data leaks and password security. Factors such as ease of use, system transparency, and the system provider's efforts to provide education about security are the main determinants of student perceptions. It is hoped that these findings can provide input for managers of academic information systems to improve their security and strengthen user trust in the system.
Keywords: Student Perceptions, Information System Security, Academic Information Systems, Bhayangkara University, Data Security.

Abstrak

Penelitian ini bertujuan untuk menganalisis persepsi mahasiswa Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya terhadap keamanan sistem informasi akademik yang digunakan. Keamanan sistem informasi akademik merupakan aspek krusial untuk melindungi data pribadi, catatan akademik, dan informasi penting lainnya dari potensi ancaman keamanan. Dengan menggunakan pendekatan kuantitatif, data dikumpulkan melalui survei terhadap sejumlah mahasiswa yang dipilih secara acak. Hasil penelitian menunjukkan bahwa sebagian besar mahasiswa memiliki persepsi positif terhadap keamanan sistem informasi akademik, meskipun terdapat beberapa kekhawatiran terkait potensi kebocoran data dan keamanan kata sandi. Faktor-faktor seperti kemudahan penggunaan, transparansi sistem, dan upaya penyedia sistem dalam memberikan edukasi tentang keamanan menjadi penentu utama dalam persepsi mahasiswa (Saefuloh et al., 2023). Temuan ini diharapkan dapat memberikan masukan bagi pengelola sistem informasi akademik untuk meningkatkan keamanannya dan memperkuat kepercayaan pengguna terhadap sistem tersebut.

Kata Kunci: Persepsi Mahasiswa, Keamanan Sistem Informasi, Sistem Informasi Akademik, Universitas Bhayangkara, Keamanan data.

1. Pendahuluan

Keamanan sistem informasi akademik menjadi salah satu aspek yang sangat penting dalam dunia pendidikan tinggi, terutama dengan semakin berkembangnya teknologi informasi. Sistem informasi akademik digunakan untuk mengelola berbagai data penting seperti informasi pribadi mahasiswa, catatan akademik, dan administrasi pendidikan lainnya. Di Universitas Bhayangkara Jakarta Raya, sistem ini menjadi fondasi utama dalam mendukung proses akademik secara digital. Oleh karena itu, keamanan sistem informasi tidak hanya berfungsi melindungi data, tetapi juga membangun kepercayaan pengguna terhadap teknologi tersebut.

Namun, seiring dengan meningkatnya digitalisasi, ancaman keamanan data juga semakin kompleks. Serangan siber seperti phishing, pencurian data, dan eksploitasi kerentanan sistem dapat membahayakan integritas sistem informasi akademik. Dalam konteks ini, universitas tidak hanya dituntut untuk menyediakan sistem yang canggih, tetapi juga harus memastikan bahwa setiap elemen keamanannya mampu menghadapi potensi ancaman tersebut. Hal ini menjadikan keamanan sistem sebagai salah satu prioritas utama bagi institusi pendidikan tinggi (Chairoel et al., 2020).

Selain itu, pengguna sistem informasi, khususnya mahasiswa, sering kali menjadi faktor yang menentukan keberhasilan pengelolaan keamanan sistem. Ketidaktahuan atau kurangnya pemahaman mahasiswa terhadap praktik keamanan, seperti manajemen kata sandi yang baik dan kewaspadaan terhadap ancaman siber, dapat meningkatkan risiko pelanggaran keamanan. Oleh karena itu, selain mengamankan infrastruktur teknis, edukasi kepada pengguna juga menjadi aspek penting yang perlu diperhatikan oleh pengelola sistem.

Penelitian ini dilakukan untuk menganalisis bagaimana mahasiswa Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya menilai keamanan sistem informasi akademik yang ada. Fokus penelitian tidak hanya pada identifikasi persepsi, tetapi juga pada faktor-faktor yang memengaruhi pandangan mahasiswa terhadap keamanan tersebut. Dengan memahami persepsi mereka, universitas dapat mengevaluasi kekurangan sistem, merumuskan strategi peningkatan keamanan, dan membangun sistem yang lebih tangguh dan terpercaya. Pendekatan kuantitatif dengan metode survei digunakan dalam penelitian ini, sehingga hasil yang diperoleh diharapkan dapat menjadi acuan bagi pengelola sistem untuk meningkatkan keamanan dan kualitas layanan.

1. Keamanan Sistem Informasi

Keamanan sistem informasi adalah upaya perlindungan terhadap aset informasi dari berbagai ancaman untuk memastikan keberlangsungan bisnis, yang mencakup tiga aspek utama yaitu kerahasiaan (*confidentiality*) untuk menjamin informasi hanya diakses oleh pihak berwenang, integritas (*integrity*) untuk memastikan akurasi data, serta ketersediaan (*availability*) untuk menjamin akses informasi saat dibutuhkan, yang semuanya diterapkan melalui kebijakan, prosedur, dan teknologi untuk melindungi data dan sistem dari ancaman seperti serangan siber, kebocoran data, atau bencana alam.

2. Persepsi mahasiswa terhadap keamanan sistem informasi akademik

Bagaimana mahasiswa menilai tingkat keamanan, keandalan, dan privasi yang diberikan oleh sistem. Persepsi ini dipengaruhi oleh beberapa faktor, antara lain pengalaman langsung dengan sistem, pengetahuan tentang keamanan informasi, informasi dari lingkungan sekitar (teman, dosen, atau media), serta tingkat kepercayaan terhadap pengelola sistem. Semakin baik pengalaman mahasiswa dan semakin tinggi kepercayaan mereka terhadap sistem, maka persepsi terhadap keamanan sistem informasi akan meningkat.

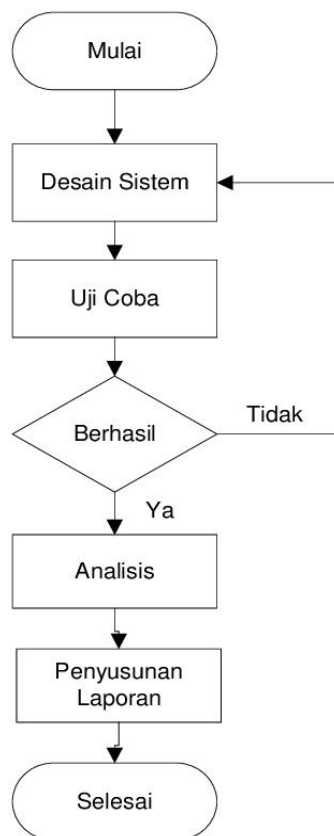
3. Sistem informasi akademik

Aplikasi berbasis teknologi informasi yang mendukung pengelolaan data akademik, seperti pendaftaran mata kuliah, pencatatan nilai, dan pengelolaan data mahasiswa. Sistem ini dirancang untuk meningkatkan efisiensi dan transparansi administrasi Pendidikan (Aldam Syaifuddin et al., 2024). Namun, dalam pengoperasiannya, sistem ini juga harus menghadapi ancaman keamanan, seperti serangan siber (hacking, phishing, atau malware) dan ancaman internal (insider threat) yang melibatkan kesalahan atau tindakan tidak etis dari staf pengelola.

Keamanan sistem informasi yang baik dapat memengaruhi tingkat kepercayaan dan kepuasan pengguna. Mahasiswa yang merasa bahwa sistem informasi akademik aman cenderung memiliki pengalaman yang lebih positif dan loyalitas yang lebih tinggi terhadap penggunaan sistem tersebut. Hal ini sejalan dengan *Technology Acceptance Model (TAM)*, yang menjelaskan bahwa penerimaan teknologi oleh pengguna dipengaruhi oleh persepsi kemudahan penggunaan (*perceived ease of use*) dan persepsi kegunaan (*perceived usefulness*). Jika mahasiswa merasa bahwa sistem informasi akademik aman, mereka akan lebih nyaman dan percaya menggunakan sistem tersebut. Selain itu, kepercayaan terhadap sistem juga dipengaruhi oleh transparansi, kejelasan kebijakan keamanan, dan pengalaman positif pengguna, sebagaimana dijelaskan dalam *Trust Model in Information Security*.

2. Metode Penelitian

Penelitian ini bertujuan untuk menganalisis persepsi mahasiswa Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya terhadap keamanan sistem informasi akademik. Penelitian ini dilakukan menggunakan pendekatan deskriptif kuantitatif, yang bertujuan untuk menggambarkan fenomena berdasarkan data yang diperoleh dari responden melalui pengisian kuesioner.



Sumber: Hasil Penelitian (2024)

Gambar 1. Flowchart Metodologi Penelitian

Pada gambar 1 menunjukkan Flowchar Metodoogi Penelitian yang terdiri dari :

1. Desain Sistem

Tahap awal dalam perancangan mencakup perancangan sistem yang akan dibuat, termasuk menentukan kebutuhan, spesifikasi, dan struktur sistem yang sesuai.

2. Uji Coba

Tahap ini, sistem yang telah dirancang diuji untuk memastikan apakah berfungsi sesuai dengan tujuan yang diinginkan.

3. Berhasil

Keputusan diambil berdasarkan hasil uji coba. Jika uji coba menunjukkan bahwa sistem berhasil memenuhi kriteria yang ditentukan, proses berlanjut. Jika tidak, sistem perlu didesain ulang atau diperbaiki.

4. Analisis

Melakukan analisis terhadap hasil dari uji cooba yang berhasil untuk mendapatkan data yang relevan sesuai tujuan penelitian.

5. Penyusunan Laporan

Menyusun laporan yang mendokumentasikan hasil analisis, termasuk metodologi, hasil, dan Kesimpulan dari proses yang telah dilakukan.

2.1. Desain Penelitian

Penelitian ini dirancang dengan metode survei menggunakan kuesioner sebagai instrumen utama. Metode survei dipilih karena memberikan fleksibilitas dalam menjangkau responden dalam jumlah besar secara efisien, terutama melalui penggunaan platform daring. Survei memungkinkan pengumpulan data secara terstruktur dengan pertanyaan yang dirancang untuk mengukur berbagai aspek persepsi mahasiswa terkait keamanan sistem informasi akademik (Yusa et al., 2021). Selain itu, survei memberikan responden kebebasan untuk menjawab dengan jujur tanpa tekanan eksternal, yang membantu meningkatkan validitas data.

Kuesioner dalam survei ini terdiri dari pertanyaan tertutup dengan skala Likert untuk kuantifikasi data, sehingga mempermudah analisis persepsi secara statistik. Pertanyaan tertutup dirancang untuk mengukur dimensi-dimensi spesifik, seperti pengalaman mahasiswa terhadap ancaman keamanan, persepsi mereka terhadap perlindungan data pribadi, dan penilaian terhadap mekanisme login. Di sisi lain, pertanyaan terbuka memungkinkan penggalian masukan atau saran dari mahasiswa, yang memberikan perspektif kualitatif sebagai pelengkap data kuantitatif.

Metode survei juga dianggap praktis karena dapat dilakukan dalam waktu yang relatif singkat dengan biaya rendah. Dengan menggunakan platform digital, data dapat langsung terekam secara otomatis, mengurangi kemungkinan kesalahan dalam pencatatan data. Pendekatan ini sangat sesuai dengan konteks penelitian yang melibatkan mahasiswa sebagai responden, mengingat akses mereka terhadap teknologi dan keterbiasaan dengan penggunaan perangkat daring.

2.2. Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh mahasiswa aktif Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya. Mahasiswa yang termasuk dalam populasi ini adalah mereka yang secara rutin menggunakan sistem informasi akademik untuk keperluan administrasi perkuliahan, seperti mengakses jadwal, nilai, pengisian Kartu Rencana Studi (KRS), dan fitur-fitur lain yang disediakan oleh sistem. Populasi ini dipilih karena keterlibatan langsung mereka dengan sistem, sehingga diharapkan memiliki persepsi yang relevan terhadap tingkat keamanannya (Aufan & Rosadi, n.d.).

Teknik pengambilan sampel yang digunakan adalah purposive sampling, yaitu memilih responden berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian. Dalam hal ini, kriteria yang digunakan adalah mahasiswa Fakultas Ilmu Komputer yang telah menggunakan sistem informasi akademik secara aktif. Sampel penelitian terdiri dari mahasiswa yang secara sukarela mengisi kuesioner daring yang telah disebarluaskan melalui platform survei online. Pendekatan ini dipilih untuk memastikan bahwa responden memiliki pengalaman langsung dengan sistem informasi akademik, sehingga data yang diperoleh memiliki validitas tinggi.

Jumlah sampel dalam penelitian ini disesuaikan dengan ketersediaan responden yang memenuhi kriteria tersebut, dengan mempertimbangkan tingkat respons serta kesesuaian jumlah sampel untuk analisis statistik yang memadai. Dengan metode ini, diharapkan penelitian dapat memperoleh data yang representatif dan relevan untuk menggambarkan persepsi mahasiswa secara keseluruhan terhadap keamanan sistem informasi akademik.

2.3. Lokasi dan Waktu Penelitian

Penelitian ini dilakukan di Universitas Bhayangkara Jakarta Raya, yang berlokasi di Bekasi, Jawa Barat. Universitas ini dipilih sebagai lokasi penelitian karena merupakan institusi tempat para responden, yaitu mahasiswa Fakultas Ilmu Komputer, menjalani aktivitas akademik sehari-hari. Sistem informasi akademik yang dianalisis dalam penelitian ini merupakan bagian integral dari layanan kampus yang digunakan oleh mahasiswa untuk berbagai keperluan, seperti pendaftaran mata kuliah, pengelolaan nilai, dan akses informasi akademik lainnya.

Pengumpulan data dilakukan pada bulan Desember 2024, menggunakan metode survei daring melalui platform online. Penggunaan platform daring dipilih untuk mempermudah penyebaran kuesioner kepada mahasiswa yang tersebar di berbagai wilayah, baik yang sedang mengikuti perkuliahan secara tatap muka maupun daring. Metode ini juga mempertimbangkan fleksibilitas waktu yang dimiliki mahasiswa, sehingga mereka dapat mengisi kuesioner kapan saja selama periode pengumpulan data.

Waktu pelaksanaan penelitian selama bulan Desember 2024 dipilih untuk memastikan responden dapat memberikan jawaban yang relevan, mengingat ini merupakan periode yang umumnya aktif dalam proses administrasi akademik, seperti pengisian Kartu Rencana Studi (KRS) untuk semester berikutnya. Hal ini diharapkan meningkatkan relevansi dan validitas data yang diperoleh terkait persepsi mahasiswa terhadap sistem informasi akademik yang digunakan.

2.4. Teknik Pengumpulan Data

Data dalam penelitian ini dikumpulkan secara daring melalui kuesioner yang dirancang menggunakan platform survei online, yang memungkinkan distribusi yang cepat dan efisien kepada responden. Setiap mahasiswa diminta untuk mengisi kuesioner berdasarkan pengalaman pribadi mereka serta persepsi terhadap sistem informasi akademik yang digunakan di institusi mereka. Kuesioner ini mencakup berbagai aspek, mulai dari kemudahan akses, fungsionalitas, keandalan, hingga tingkat kepuasan terhadap fitur-fitur yang disediakan oleh sistem tersebut. Mahasiswa diminta memberikan tanggapan yang jujur dan objektif, berdasarkan interaksi mereka dengan sistem informasi akademik dalam konteks kegiatan akademik sehari-hari. Survei ini bertujuan untuk mengidentifikasi kekuatan dan kelemahan yang ada dalam sistem, serta memberikan masukan yang berguna untuk perbaikan dan pengembangan sistem di masa depan.

2.5. Teknik Analisis Data

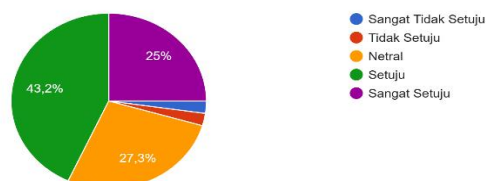
Data yang terkumpul dari kuesioner ini dianalisis menggunakan pendekatan kuantitatif dan kualitatif untuk memberikan gambaran yang komprehensif mengenai persepsi mahasiswa terhadap sistem informasi akademik (Septiani et al., n.d.). Analisis kuantitatif dilakukan dengan menghitung distribusi frekuensi, persentase, dan rata-rata dari jawaban pertanyaan tertutup. Hal ini bertujuan untuk menggambarkan pola umum persepsi mahasiswa, seperti apakah mayoritas responden merasa sistem informasi akademik sudah aman, efektif, dan mudah digunakan, atau apakah terdapat kelemahan tertentu yang perlu diperbaiki. Misalnya, analisis kuantitatif dapat menunjukkan apakah sebagian besar mahasiswa merasa nyaman dengan fitur keamanan sistem atau apakah mereka menemukan adanya celah yang perlu diperhatikan. Sementara itu, analisis kualitatif dilakukan dengan menganalisis jawaban dari pertanyaan terbuka untuk menggali lebih dalam masukan dan pengalaman mahasiswa yang tidak dapat tercakup dalam pilihan jawaban tertutup. Melalui pendekatan ini, dapat diidentifikasi tema atau pola masukan yang berulang, yang kemudian dapat dijadikan rekomendasi untuk perbaikan dan pengembangan lebih lanjut, terutama dalam aspek keamanan dan fungsionalitas sistem informasi akademik, guna meningkatkan kepuasan dan kenyamanan pengguna.

3. Hasil dan Pembahasan

3.1. Pelanggaran Percobaan Tidak Sah Terhadap SIA Ubharajaya

Pelanggaran percobaan tidak sah terhadap Sistem Informasi Akademik (SIA) Ubharajaya merupakan tindakan ilegal yang melibatkan upaya akses, manipulasi, atau penggunaan sistem tanpa izin resmi, dengan tujuan seperti meningkatkan nilai akademik secara curang, mencuri data sensitif, atau merusak sistem, yang dapat menyebabkan kerugian seperti hilangnya data, pelanggaran privasi, kerusakan reputasi universitas, dan kerugian finansial, sehingga memerlukan pencegahan melalui peningkatan keamanan sistem, edukasi pengguna, penerapan kebijakan tegas, serta penegakan hukum berdasarkan UU ITE yang mengatur sanksi berat bagi pelanggaran akses tidak sah, demi melindungi integritas sistem dan informasi universitas.

Saya tidak pernah mengalami percobaan akses tidak sah pada akun sistem informasi akademik saya.
44 jawaban



Sumber: Hasil Penelitian (2024)

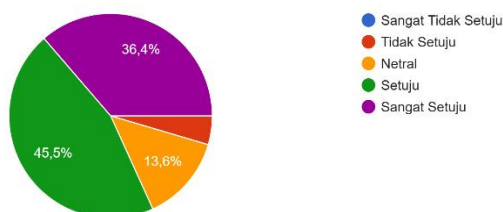
Gambar 2. Diagram Percobaan Akses Tidak Sah Terhadap Akun SIA

Pada Gambar 2 menunjukkan Hasil kuesioner menunjukkan bahwa mayoritas responden, yaitu 68,2%, merasa yakin atau cenderung yakin bahwa mereka tidak pernah mengalami percobaan akses tidak sah pada akun sistem informasi akademik mereka, dengan 43,2% memilih "Setuju" dan 25% "Sangat Setuju," sementara 27,3% responden bersikap netral, yang mungkin mencerminkan kurangnya kesadaran atau kepastian mengenai potensi ancaman keamanan, serta hanya sebagian kecil yang memilih "Tidak Setuju" atau "Sangat Tidak Setuju," sehingga secara keseluruhan menggambarkan tingkat keamanan yang cukup baik namun tetap membutuhkan peningkatan edukasi untuk memperkuat pemahaman pengguna terkait risiko keamanan dan perlindungannya.

3.2. Penggunaan SIA Ubharajaya Memiliki Mekanisme Login Yang Aman

Sistem Informasi Akademik (SIA) Universitas Bhayangkara Jakarta Raya mengimplementasikan mekanisme login yang aman dengan memanfaatkan kombinasi username dan password yang dilindungi oleh enkripsi untuk menjaga kerahasiaan data pengguna. Sistem ini juga dilengkapi dengan fitur keamanan tambahan, seperti verifikasi dua langkah (2FA), untuk mencegah akses tidak sah. Selain itu, firewall dan log aktivitas digunakan untuk memantau serta mendeteksi potensi ancaman terhadap sistem. Sebagai langkah pendukung, pengguna juga diberikan edukasi mengenai pentingnya menjaga kerahasiaan data pribadi untuk meningkatkan keamanan akun.

Sistem informasi akademik Universitas Bhayangkara Jakarta Raya memiliki mekanisme login yang aman (misalnya, penggunaan username dan password)
44 jawaban



Sumber: Hasil Penelitian (2024)

Gambar 3. Diagram Penggunaan SIA Ubharajaya Memiliki Mekanisme Login Yang Aman

Pada gambar 3 menunjukkan survei yang dilakukan terhadap 44 responden mengenai keamanan mekanisme login sistem informasi akademik Universitas Bhayangkara Jakarta Raya, mayoritas responden memberikan tanggapan positif. Lebih dari 80% responden (kombinasi dari 45,5% Setuju dan 36,4% Sangat Setuju) menyatakan bahwa sistem login yang menggunakan username dan password sudah memiliki tingkat keamanan yang baik. Hanya sebagian kecil

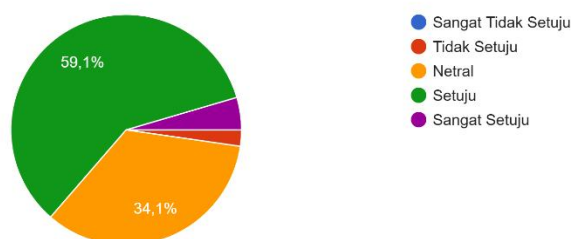
responden (13,6%) yang memilih untuk bersikap netral, dan tidak ada responden yang menyatakan ketidaksetujuan terhadap keamanan sistem tersebut.

3.3. Konsep Keamanan Internal SIA Ubharajaya

Perlindungan data pribadi dalam SIA Ubharajaya diimplementasikan melalui sistem keamanan berlapis yang komprehensif. Fondasi keamanan dimulai dari sistem autentikasi yang kuat, dilanjutkan dengan pengaturan hak akses yang ketat berdasarkan peran masing-masing pengguna. Kerahasiaan informasi dijaga melalui enkripsi database dan perlindungan firewall, sementara aktivitas pengguna dipantau secara sistematis melalui sistem pencatatan yang terstruktur. Pendekatan menyeluruh ini menciptakan lingkungan digital yang aman bagi seluruh civitas akademika dalam mengakses dan mengelola data pribadi mereka di dalam sistem (Keguruan et al., n.d.).

Saya merasa data pribadi saya, seperti nilai dan informasi akademik lainnya, terlindungi dengan baik dalam sistem informasi akademik.

44 jawaban



Sumber: Hasil Penelitian (2024)

Gambar 4. Diagram Konsep Keamanan Internal SIA Ubharajaya

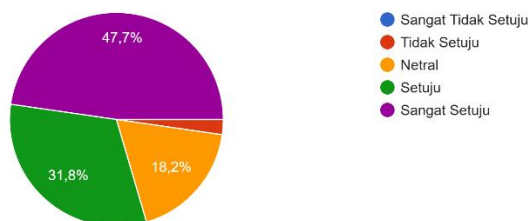
Pada Gambar 4 menunjukkan Mayoritas responden (59,1%) merasa data pribadi mereka, seperti nilai dan informasi akademik, terlindungi dengan baik dalam sistem informasi akademik. Sebagian lainnya (34,1%) bersikap netral, menandakan keraguan atau kurangnya keyakinan. Hanya sedikit yang memiliki pandangan negatif, yakni 2,3% menyatakan ketidaksetujuan, dan 4,5% sangat setuju terhadap perlindungan data tersebut. Hasil ini mencerminkan kepercayaan yang cukup tinggi terhadap sistem, meskipun masih ada ruang untuk peningkatan keamanan data.

3.4. Pentingnya Edukasi Terhadap Mahasiswa Mengenai SIA Ubharajaya

Edukasi mengenai Sistem Informasi Akademik (SIA) di Universitas Bhayangkara Jakarta Raya (Ubharajaya) sangat penting untuk memastikan mahasiswa dapat memanfaatkan sistem secara maksimal. Pemahaman yang baik memungkinkan mahasiswa mengakses informasi akademik, seperti jadwal, nilai, dan layanan administrasi, dengan efisien. Selain itu, edukasi ini juga meningkatkan kesadaran akan pentingnya menjaga keamanan data pribadi mereka,

sehingga mahasiswa dapat berkontribusi dalam menjaga kerahasiaan dan keamanan informasi yang ada. Dengan memberikan pelatihan atau panduan yang memadai, mahasiswa tidak hanya menjadi pengguna SIA yang aktif dan percaya diri, tetapi juga mampu meminimalkan kesalahan dan meningkatkan kepercayaan terhadap pengelolaan data kampus(Zakyah, 2019).

Saya merasa perlu adanya edukasi mengenai keamanan sistem informasi akademik untuk mahasiswa.
44 jawaban



Sumber: Hasil Penelitian (2024)

Gambar 5. Diagram Edukasi Keamanan SIA Ubharajaya

Pada Gambar 5 menunjukkan Mayoritas responden (79,5%) setuju atau sangat setuju bahwa edukasi mengenai keamanan sistem informasi akademik (SIA) sangat penting bagi mahasiswa. Hal ini menunjukkan adanya kebutuhan yang mendesak untuk memberikan pemahaman tentang keamanan data akademik di kalangan mahasiswa. Sebagian kecil (18,2%) bersikap netral, yang mungkin mencerminkan kurangnya pemahaman mereka tentang isu ini. Sementara itu, hanya sedikit yang tidak setuju, menunjukkan bahwa hampir semua responden mendukung inisiatif edukasi keamanan SIA. Hasil ini menegaskan bahwa universitas perlu segera mengimplementasikan program edukasi untuk meningkatkan kesadaran dan pemahaman mahasiswa terhadap pentingnya menjaga keamanan data akademik mereka(Yahya et al., 2020).

4. Kesimpulan

Penelitian ini menunjukkan bahwa mayoritas mahasiswa Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya memiliki persepsi positif terhadap keamanan Sistem Informasi Akademik (SIA). Mekanisme keamanan seperti penggunaan username, password terenkripsi, serta fitur tambahan seperti autentikasi dua faktor (2FA) dianggap cukup efektif dalam melindungi data pribadi pengguna. Meskipun demikian, terdapat beberapa perhatian yang perlu diperhatikan, seperti potensi kebocoran data dan kurangnya pemahaman sebagian mahasiswa mengenai ancaman keamanan digital.

Hasil survei juga mengungkapkan bahwa faktor transparansi sistem, kenyamanan penggunaan, dan edukasi tentang keamanan sangat berpengaruh terhadap tingkat kepercayaan mahasiswa terhadap SIA. Edukasi mengenai pentingnya menjaga data pribadi

dan penggunaan fitur keamanan secara bijak terbukti menjadi aspek yang penting untuk terus ditingkatkan (Fuad & Harisun, 2019).

Secara keseluruhan, Universitas Bhayangkara Jakarta Raya perlu terus meningkatkan langkah-langkah pengamanan, termasuk dengan mengintegrasikan teknologi yang lebih canggih, memperkuat kebijakan keamanan, dan memberikan edukasi yang memadai bagi seluruh pengguna sistem. Dengan demikian, kepercayaan pengguna terhadap SIA dapat terus dipertahankan dan ditingkatkan, sejalan dengan kebutuhan akademik dan tantangan era digital.

Daftar Pustaka

- Aldam Syaifuddin, F., Achmad Maulana, D., Faishol Amrulloh, M., Studi Informaika, P., Yudharta Pasuruan, U., & Artikel, H. (2024). *Analisis Keamanan Jaringan Menggunakan Firewall untuk Mencegah Serangan Brute Force dan Fraud*. 4(2). <https://doi.org/10.47709/digitech.v4i2.5003>
- Aufan, O. :, & Rosadi, I. (n.d.). *ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN WEB PENETRAION TESTING*.
- Chairoel, L., Eka Yan Fitri, M., & Yossi Hastini, L. (2020). Persepsi Mahasiswa tentang Sistem Informasi Akademik Perguruan Tinggi. *Andalas Management Review*, 4(1), 82–99. <https://sevima.com/>
- Fuad, A., & Harisun, E. (2019). ANALISIS TINGKAT KEPUASAN MAHASISWA TERHADAP KINERJA SISTEM INFORMASI AKADEMIK (SIMAK) DI PROGRAM STUDI INFORMATIKA. In *Jurnal Informatika dan Komputer Ternate* (Vol. 02, Issue 1). <http://if.unkhair.ac.id>;
- Keguruan, D., Raden, U., & Palembang, F. (n.d.). *ANALISIS PERSEPSI MAHASISWA TERHADAP KOMPETENSI DOSEN DALAM MENGAJAR PADA PROGRAM STUDI PAI FAKULTAS ILMU TARBIYAH*.
- Saefuloh, A., Aulia, I. P., Arief, R. F., Kusuma, W., Fakultas, I. /, Informasi, T., & Situ, J. A. (2023). *Analisis Persepsi dan Praktik Keamanan Teknologi di Kalangan Mahasiswa dan Umum: Studi Survei Mengenai Kesadaran dan Tindakan Keamanan dalam Penggunaan Teknologi*.
- Septiani, Y., Arribe, E., & Diansyah, R. (n.d.). *ANALISIS KUALITAS LAYANAN SISTEM INFORMASI AKADEMIK UNIVERSITAS ABDURRAB TERHADAP KEPUASAN PENGGUNA MENGGUNAKAN METODE SEVQUAL (Studi Kasus: Mahasiswa Universitas Abdurrab Pekanbaru)*.
- Yahya, M., Hasanuddin, T., & Abdullah, S. M. (2020). *Buletin Sistem Informasi dan Teknologi Islam Analisis dan Perancangan Sistem Pengaduan Mahasiswa Fakultas Ilmu Komputer Universitas Muslim Indonesia* INFORMASI ARTIKEL ABSTRAK. 1(3), 166–175.

Yusa, M., Sofwan Alqap, A. F., & Hidayati, N. (2021). *ANALISIS TINGKAT KEPUASAN MAHASISWA TERHADAP PELAYANAN AKADEMIK DI FAKULTAS TEKNIK UNIVERSITAS BENGKULU*. 18, 103. <https://doi.org/10.26487/jbmi.v18i2.14104>

Zakyah, A. M. (2019). Kualitas Pelayanan Sistem Informasi Akademik Pada Kepuasan Mahasiswa Menggunakan Metode Webqual 4.0. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, 4(1), 1. <https://doi.org/10.32528/justindo.v4i1.2416>