Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.269

PERAN CIA TRIAD, PRIVASI, DAN TERMS AND CONDITIONS DALAM KEPERCAYAAN DIGITAL SISTEM INFORMASI

Evy Nurmiati[1], Ghein Karimah[2*],
[1,2]UIN Syarif Hidayatullah Jakarta, Indonesia
[1]evy.nurmiati@uinjkt.ac.id, [2*]ghein.karimah24@mhs.uinjkt.ac.id

ABSTRACT

Rapid advancements in information technology have increased the use of digital systems across various sectors, including business, education, and government. While information systems offer convenience in data management and operational efficiency, they also introduce new risks related to information security and data protection. This condition highlights that digital systems must not only be efficient but also capable of ensuring security and building user trust. This study aims to analyze the role of confidentiality, integrity, and availability as fundamental principles of information security, along with privacy and Terms and Conditions, in establishing digital trust within modern information systems. A qualitative approach was employed using a literature review method, where data were collected from relevant scientific journals and analyzed descriptively and analytically to identify relationships among key concepts. The findings indicate that security principles provide a strong technical foundation but are not sufficient to address challenges related to human behavior. Privacy plays a crucial role in protecting users' personal data, while Terms and Conditions contribute to transparency in digital service management. The integration of these aspects demonstrates a strong interconnection in building digital trust. This study emphasizes the importance of a comprehensive approach to enhancing user trust and provides insights for improving the reliability of digital systems in organizational contexts.

Keywords:
Information Systems, Information Security, Data Privacy, Terms and Conditions, Digital Trust.

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital yang signifikan dalam berbagai sektor, seperti bisnis, pendidikan, dan pemerintahan. Sistem informasi modern kini menjadi komponen utama dalam pengelolaan data dan operasional organisasi (Laudon & Laudon, 2020; Stair & Reynolds, 2018). Ketergantungan yang tinggi terhadap sistem digital memberikan berbagai keuntungan, seperti efisiensi dan kemudahan akses informasi, namun di sisi lain juga meningkatkan risiko terhadap keamanan informasi dan data (ENISA, 2022; Von Solms & Van Niekerk, 2013).

Seiring dengan meningkatnya penggunaan sistem digital, ancaman terhadap keamanan informasi juga berkembang menjadi lebih kompleks dan terstruktur. Berbagai bentuk serangan seperti ransomware, phishing, Distributed Denial of Service (DDoS), serta social engineering menunjukkan bahwa sistem informasi tidak hanya rentan terhadap kelemahan teknis, tetapi juga terhadap faktor manusia. Kondisi ini menegaskan bahwa keamanan informasi memerlukan pendekatan yang tidak hanya berbasis teknologi, tetapi juga memperhatikan aspek perilaku dan kesadaran pengguna.

Dalam upaya menjaga keamanan sistem informasi, konsep CIA Triad yang terdiri dari Confidentiality, Integrity, dan Availability telah menjadi fondasi utama dalam pengembangan kebijakan dan mekanisme keamanan. Confidentiality berfokus pada perlindungan kerahasiaan data dari akses yang tidak sah, Integrity memastikan keakuratan dan keutuhan data, sedangkan Availability menjamin ketersediaan informasi bagi pihak yang berwenang ketika dibutuhkan. Ketiga aspek ini saling berkaitan dan menjadi dasar dalam menjaga keandalan sistem informasi.

Namun demikian, penelitian sebelumnya menunjukkan bahwa penerapan CIA Triad dalam praktik masih menghadapi berbagai keterbatasan. Implementasi yang berfokus pada aspek teknis belum sepenuhnya mampu mengatasi permasalahan keamanan yang dipengaruhi oleh faktor manusia dan kurangnya kesadaran pengguna. Selain itu, sebagian besar penelitian masih menempatkan CIA Triad sebagai kerangka keamanan yang berdiri sendiri, tanpa mengkaji keterkaitannya dengan aspek lain seperti perlindungan privasi dan transparansi kebijakan layanan digital.

Di sisi lain, meningkatnya kesadaran terhadap perlindungan data pribadi menempatkan privasi sebagai faktor penting dalam penggunaan sistem informasi. Pengguna tidak hanya membutuhkan sistem yang aman, tetapi juga sistem yang mampu melindungi hak mereka atas data pribadi. Selain itu, keberadaan Terms and Conditions sebagai bentuk kesepakatan antara pengguna dan penyedia layanan sering kali tidak dipahami secara menyeluruh, sehingga berpotensi menimbulkan kesenjangan antara perlindungan yang diberikan dan yang dipersepsikan oleh pengguna.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.269

Berdasarkan kondisi tersebut, terdapat kesenjangan penelitian (research gap) dalam memahami bagaimana keamanan sistem informasi, perlindungan privasi, dan transparansi kebijakan layanan dapat secara bersama-sama membentuk kepercayaan pengguna terhadap sistem digital. Oleh karena itu, penelitian ini menawarkan pendekatan integratif dengan mengkaji keterkaitan antara CIA Triad, privasi, dan Terms and Conditions dalam membangun kepercayaan digital.

Penelitian ini bertujuan untuk menganalisis peran CIA Triad, privasi, dan Terms and Conditions secara komprehensif dalam membentuk kepercayaan digital pada sistem informasi modern. Kontribusi utama penelitian ini adalah memberikan kerangka konseptual yang mengintegrasikan aspek keamanan, perlindungan data, dan transparansi sebagai dasar dalam membangun sistem informasi yang tidak hanya aman, tetapi juga terpercaya.

Sejumlah penelitian sebelumnya telah mengkaji berbagai aspek yang berkaitan dengan keamanan sistem informasi dan kepercayaan pengguna dalam lingkungan digital. Kajian tersebut menunjukkan bahwa penerapan konsep *CIA Triad* mampu meningkatkan tingkat keamanan sistem, khususnya dalam menjaga kerahasiaan dan keutuhan data. Selain itu, tingkat keamanan siber yang baik terbukti memiliki pengaruh terhadap kepercayaan pengguna terhadap layanan digital. Dalam konteks tertentu seperti layanan keuangan digital, keamanan sistem juga berperan dalam meningkatkan keyakinan pengguna terhadap keandalan sistem. Meskipun demikian, sebagian besar penelitian tersebut masih berfokus pada aspek teknis keamanan dan belum sepenuhnya mempertimbangkan faktor non-teknis yang turut memengaruhi persepsi kepercayaan pengguna.

Selain aspek keamanan, penelitian lain juga menyoroti pentingnya perlindungan data pribadi dan transparansi dalam penggunaan sistem digital. Perlindungan data pribadi menjadi faktor penting dalam menciptakan rasa aman bagi pengguna, terutama dalam menghadapi risiko penyalahgunaan data. Di sisi lain, keberadaan *Terms and Conditions* sebagai bentuk kesepakatan antara pengguna dan penyedia layanan seharusnya mampu memberikan transparansi terkait penggunaan data dan layanan. Namun dalam praktiknya, banyak pengguna yang tidak memahami isi *Terms and Conditions* secara menyeluruh, sehingga mengurangi efektivitasnya dalam membangun kepercayaan. Meskipun berbagai penelitian telah membahas aspek keamanan, privasi, dan transparansi secara terpisah, masih terdapat keterbatasan dalam mengintegrasikan ketiga aspek tersebut dalam satu kerangka yang komprehensif untuk menjelaskan pembentukan *digital trust*.

Penelitian ini menawarkan pendekatan integratif dalam mengkaji hubungan antara *CIA Triad*, privasi, dan *Terms and Conditions* dalam membangun *digital trust*. Berdasarkan permasalahan tersebut, penelitian ini berupaya menjawab bagaimana integrasi aspek keamanan, privasi, dan transparansi dapat membentuk kepercayaan digital dalam sistem informasi modern.

KAJIAN LITERATUR

Keamanan Informasi dan *CIA Triad*

Keamanan informasi merupakan upaya untuk melindungi aset informasi dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data. Dalam konteks ini, CIA Triad yang terdiri dari *confidentiality*, *integrity*, dan *availability* menjadi kerangka dasar dalam pengelolaan keamanan sistem informasi (Hidayat et al., 2023; Whitman & Mattord, 2017; Von Solms & Van Niekerk, 2013). Penerapan konsep ini umumnya dilakukan melalui mekanisme autentikasi, pembatasan akses, serta pengelolaan ketersediaan sistem untuk menjaga stabilitas layanan.

Jika dibandingkan dengan konsep privasi, CIA Triad lebih berfokus pada aspek teknis keamanan sistem, sedangkan privasi mencakup dimensi perlindungan hak pengguna terhadap data pribadi. Namun, penelitian lain menunjukkan bahwa ancaman keamanan modern tidak hanya berasal dari kelemahan teknis, tetapi juga dari faktor manusia melalui serangan seperti *phishing* dan *social engineering* (Jum'an & Asyura, 2025). Hal ini menunjukkan bahwa CIA Triad sebagai pendekatan teknis masih memiliki keterbatasan, sehingga diperlukan pendekatan yang lebih komprehensif dalam menghadapi risiko keamanan sistem informasi.

Privasi dalam Sistem Informasi Digital

Privasi berkaitan dengan hak individu dalam mengendalikan data pribadi yang dimilikinya (Smith et al., 2011; Bélanger & Crossler, 2011), termasuk dalam proses pengumpulan, penggunaan, dan penyebaran data dalam sistem digital. Seiring dengan meningkatnya penggunaan teknologi, jumlah data pribadi yang tersimpan dalam sistem juga semakin besar, sehingga risiko pelanggaran privasi menjadi semakin tinggi.

Penelitian oleh Jum'an & Asyura (2025) menunjukkan bahwa pelanggaran privasi sering kali terjadi akibat kombinasi kelemahan sistem dan rendahnya kesadaran pengguna, terutama melalui teknik manipulasi seperti *social engineering*. Jika dibandingkan dengan *confidentiality* dalam CIA Triad, privasi memiliki cakupan yang lebih luas karena mencakup aspek transparansi dan tanggung jawab dalam pengelolaan data. Dengan demikian, privasi tidak hanya melengkapi aspek keamanan teknis, tetapi juga memperluas cakupan perlindungan dalam sistem informasi dengan mempertimbangkan perspektif pengguna. Namun, sebagian besar penelitian masih membahas privasi secara

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.269

terpisah, sehingga menunjukkan perlunya integrasi dengan konsep keamanan sistem.

***Terms and Conditions* dalam Layanan Digital**

Terms and Conditions (T&C) merupakan perjanjian antara pengguna dan penyedia layanan digital (McDonald & Cranor, 2008). T&C ini yang mengatur hak dan kewajiban dalam penggunaan sistem, serta menjadi bentuk transparansi dalam pengelolaan data pengguna. Namun, penelitian menunjukkan bahwa sebagian besar pengguna tidak membaca atau memahami isi T&C secara menyeluruh, sehingga menimbulkan kesenjangan antara kebijakan yang diterapkan dan persepsi pengguna terhadap risiko (Azzahra et al., 2024; Waliullah et al., 2025). Selain itu, studi sebelumnya lebih banyak berfokus pada aspek teknis keamanan, sementara aspek kebijakan seperti T&C masih relatif kurang mendapat perhatian dalam kajian sistem informasi. Berbeda dengan pendekatan keamanan teknis dan perlindungan data, *Terms and Conditions* berperan dalam aspek transparansi kebijakan yang mengatur hubungan antara pengguna dan penyedia layanan.

Kepercayaan Digital (*Digital trust*)

Kepercayaan digital merupakan tingkat keyakinan pengguna terhadap keamanan sistem digital (Gefen et al., 2003; Kim et al., 2008), yang menjadi faktor penting dalam adopsi layanan digital. Penelitian menunjukkan bahwa meningkatnya kasus kejahatan siber dan *fraud* dapat menurunkan kepercayaan pengguna terhadap sistem digital (Syahraeni et al., 2024; Jum'an & Asyura, 2025), sehingga kepercayaan tidak hanya dipengaruhi oleh keamanan sistem, tetapi juga oleh persepsi risiko, perlindungan data, dan transparansi layanan.

Sintesis dan Kesenjangan Penelitian

Berdasarkan kajian literatur, penelitian sebelumnya menunjukkan bahwa keamanan sistem informasi melalui CIA Triad (Whitman & Mattord, 2017; Hidayat et al., 2023), perlindungan data melalui privasi (Azzahra et al., 2024; Balaka et al., 2024), serta transparansi melalui kebijakan layanan (Waliullah et al., 2025) umumnya masih dikaji secara terpisah. Ketiga aspek tersebut menunjukkan bahwa keamanan sistem informasi tidak dapat dipandang secara parsial, melainkan sebagai suatu kesatuan yang saling melengkapi dalam membentuk kepercayaan digital. Selain itu, penelitian terkait keamanan siber juga menekankan bahwa ancaman modern tidak hanya bersifat teknis, tetapi juga melibatkan faktor manusia dan perilaku pengguna (Afifah et al., 2025; Jum'an & Asyura, 2025).

Kondisi tersebut menunjukkan adanya kesenjangan penelitian dalam mengintegrasikan ketiga aspek tersebut dalam satu kerangka yang utuh untuk membangun kepercayaan digital. Oleh karena itu, penelitian ini berupaya mengkaji keterkaitan antara CIA Triad, privasi, dan Terms and Conditions secara komprehensif sebagai dasar dalam membentuk kepercayaan digital pada sistem informasi modern.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode *literature review* untuk menganalisis permasalahan keamanan informasi dalam sistem digital, khususnya yang berkaitan dengan keterbatasan pendekatan teknis melalui CIA Triad. Objek penelitian dalam studi ini mencakup konsep keamanan informasi, perlindungan data pribadi, serta transparansi kebijakan layanan dalam sistem digital. Metode *literature review* dipilih karena memungkinkan peneliti untuk mengkaji berbagai hasil penelitian sebelumnya secara sistematis serta mengidentifikasi keterkaitan antara aspek keamanan, privasi, dan transparansi dalam membangun kepercayaan digital.

Pendekatan ini digunakan untuk memperoleh pemahaman yang komprehensif terhadap hubungan antara keamanan sistem, perlindungan data, dan transparansi kebijakan dalam membangun kepercayaan digital. Melalui metode *literature review*, penelitian ini tidak hanya mengumpulkan informasi dari berbagai sumber, tetapi juga melakukan analisis kritis terhadap hasil penelitian sebelumnya guna mengidentifikasi pola, keterbatasan, serta peluang pengembangan konsep. Dengan demikian, metode ini memungkinkan penyusunan kerangka konseptual yang lebih terintegrasi dalam menjelaskan keterkaitan antara *CIA Triad*, privasi, dan *Terms and Conditions* dalam sistem informasi modern.

Tahapan Penelitian

Tahapan penelitian yang dilakukan meliputi:

- **Pengumpulan Literatur**

Pada tahap ini dilakukan pengumpulan berbagai sumber literatur yang relevan, seperti jurnal ilmiah, buku, dan publikasi akademik yang membahas keamanan informasi, *CIA Triad*, privasi, serta kepercayaan digital. Literatur yang dipilih merupakan penelitian yang memiliki keterkaitan langsung dengan topik yang dikaji.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.269

- **Klasifikasi dan Seleksi Data**

Literatur yang telah dikumpulkan kemudian diklasifikasikan berdasarkan fokus pembahasan, yaitu aspek keamanan teknis (*CIA Triad*), perlindungan data (privasi), serta transparansi kebijakan (*Terms and Conditions*). Proses ini bertujuan untuk mempermudah analisis hubungan antar konsep yang diteliti.

- **Analisis dan Sintesis Literatur**

Pada tahap ini dilakukan analisis terhadap hasil penelitian sebelumnya dengan membandingkan persamaan, perbedaan, serta keterbatasan masing-masing studi. Analisis ini menghasilkan sintesis yang menunjukkan bahwa pendekatan keamanan yang ada masih bersifat parsial dan belum mengintegrasikan seluruh aspek yang mempengaruhi kepercayaan digital.

- **Perumusan Kerangka Konseptual**

Berdasarkan hasil analisis, penelitian ini merumuskan suatu kerangka konseptual yang mengintegrasikan *CIA Triad*, privasi, dan *Terms and Conditions* sebagai faktor yang saling berinteraksi dalam membentuk kepercayaan digital. Kerangka ini dikembangkan sebagai solusi terhadap keterbatasan pendekatan keamanan yang hanya berfokus pada aspek teknis.

Metode Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui studi pustaka dengan mengkaji berbagai sumber literatur yang relevan. Data diperoleh dari jurnal ilmiah nasional dan internasional yang membahas keamanan informasi, privasi, serta kepercayaan digital (Hidayat et al., 2023; Azzahra et al., 2024; Balaka et al., 2024; Jum'an & Asyura, 2025). Selain itu, referensi tambahan digunakan untuk memperkuat analisis terhadap hubungan antar konsep yang dikaji.

Teknik Analisis Data

Teknik analisis data dilakukan dengan pendekatan deskriptif-analitis, yaitu dengan mengkaji dan membandingkan berbagai hasil penelitian sebelumnya untuk mengidentifikasi pola dan hubungan antar variabel. Analisis ini difokuskan pada keterkaitan antara keamanan sistem (*CIA Triad*), perlindungan data (privasi), serta transparansi kebijakan layanan (*Terms and Conditions*) dalam membentuk kepercayaan digital. Hasil analisis kemudian digunakan untuk menyusun kerangka konseptual yang menjadi kontribusi utama penelitian ini.

Model Konseptual Penelitian

Sebagai kontribusi penelitian, penelitian ini mengusulkan model konseptual yang mengintegrasikan tiga aspek utama, yaitu *CIA Triad* sebagai dasar keamanan sistem, privasi sebagai perlindungan data pengguna, dan *Terms and Conditions* sebagai bentuk transparansi kebijakan layanan. Ketiga aspek tersebut dianalisis sebagai faktor yang saling berinteraksi dalam membentuk kepercayaan digital pada sistem informasi modern.

HASIL DAN PEMBAHASAN

Hasil penelitian ini menunjukkan bahwa keamanan sistem informasi tidak dapat hanya bergantung pada pendekatan teknis semata. Berdasarkan analisis literatur, konsep *Confidentiality*, *Integrity*, dan *Availability* sebagai bagian dari prinsip keamanan informasi memberikan fondasi utama dalam melindungi sistem digital dari berbagai ancaman. Namun, temuan juga menunjukkan bahwa pendekatan ini masih memiliki keterbatasan, terutama dalam mengakomodasi faktor perilaku pengguna.

Selain aspek keamanan teknis, perlindungan data pribadi menjadi komponen penting dalam membangun kepercayaan pengguna. Konsep privasi tidak hanya berkaitan dengan pengamanan data, tetapi juga menyangkut bagaimana data tersebut dikelola dan digunakan secara bertanggung jawab. Hal ini menunjukkan bahwa keamanan sistem informasi perlu diperluas dengan mempertimbangkan dimensi perlindungan hak pengguna.

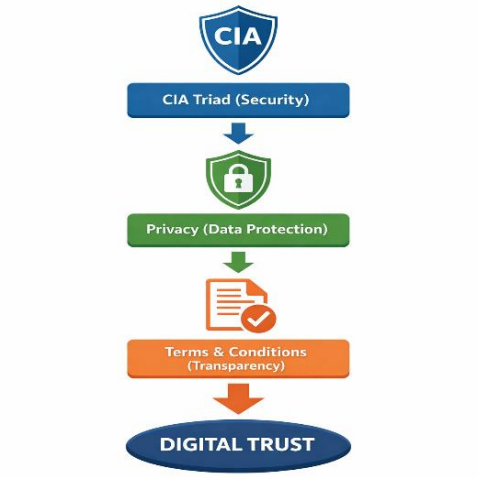
Di sisi lain, keberadaan *Terms and Conditions* berperan sebagai bentuk transparansi dalam layanan digital. Meskipun sering diabaikan oleh pengguna, kebijakan ini memiliki fungsi penting dalam menjelaskan hak dan kewajiban antara pengguna dan penyedia layanan. Temuan ini menunjukkan bahwa transparansi kebijakan merupakan faktor pendukung dalam meningkatkan kepercayaan terhadap sistem digital.

Jika dibandingkan, ketiga aspek tersebut memiliki peran yang saling melengkapi. Prinsip keamanan informasi berfokus pada perlindungan sistem secara teknis, privasi menitikberatkan pada perlindungan data pengguna, sedangkan *Terms and Conditions* berfungsi sebagai jembatan komunikasi antara sistem dan pengguna. Integrasi ketiga aspek ini membentuk suatu pendekatan yang lebih komprehensif dalam membangun kepercayaan digital.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.269

Dengan demikian, hasil penelitian ini menegaskan bahwa kepercayaan digital tidak hanya dibentuk oleh keamanan sistem, tetapi juga oleh perlindungan data dan transparansi kebijakan. Pendekatan yang terintegrasi menjadi kunci dalam meningkatkan keandalan sistem informasi serta memperkuat kepercayaan pengguna terhadap layanan digital.



Gambar 1. Model Keterkaitan Kepercayaan Digital

Temuan ini menunjukkan bahwa pendekatan keamanan sistem informasi yang hanya berfokus pada aspek teknis tidak lagi memadai dalam menghadapi kompleksitas sistem digital modern. Integrasi antara keamanan, privasi, dan transparansi menjadi semakin penting, terutama dalam meningkatkan kepercayaan pengguna terhadap layanan digital yang terus berkembang. Hal ini juga menunjukkan bahwa pengelolaan sistem informasi tidak hanya bergantung pada teknologi, tetapi juga pada bagaimana sistem tersebut dirancang untuk memenuhi kebutuhan dan ekspektasi pengguna.

KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa kepercayaan digital dalam sistem informasi modern tidak hanya dipengaruhi oleh aspek keamanan teknis, tetapi juga oleh perlindungan data dan transparansi kebijakan layanan. Prinsip *Confidentiality*, *Integrity*, dan *Availability* berperan sebagai fondasi dalam menjaga keamanan sistem, namun belum sepenuhnya mampu menjawab tantangan yang berkaitan dengan perilaku pengguna dan kompleksitas interaksi dalam lingkungan digital.

Privasi menjadi faktor penting yang melengkapi aspek keamanan dengan memberikan perlindungan terhadap hak pengguna atas data pribadi. Selain itu, *Terms and Conditions* berperan sebagai bentuk transparansi yang menjelaskan hubungan antara pengguna dan penyedia layanan, meskipun dalam praktiknya masih terdapat keterbatasan dalam tingkat pemahaman pengguna terhadap isi kebijakan tersebut. Integrasi antara keamanan sistem, perlindungan data, dan transparansi kebijakan menunjukkan bahwa ketiga aspek tersebut saling melengkapi dalam membangun kepercayaan digital yang lebih kuat.

Penelitian ini memberikan kontribusi dalam bentuk kerangka konseptual yang mengintegrasikan ketiga aspek tersebut sebagai dasar dalam meningkatkan keandalan sistem informasi. Secara praktis, hasil penelitian ini dapat digunakan sebagai acuan dalam merancang sistem digital yang tidak hanya aman secara teknis, tetapi juga mampu membangun kepercayaan pengguna.

Namun demikian, penelitian ini memiliki keterbatasan karena menggunakan pendekatan konseptual berbasis kajian literatur tanpa melibatkan data empiris secara langsung. Oleh karena itu, penelitian selanjutnya disarankan untuk menguji model yang diusulkan melalui pendekatan kuantitatif atau studi kasus agar dapat memberikan hasil yang lebih terukur dan aplikatif. Selain itu, kajian lanjutan juga diperlukan untuk memahami peran faktor perilaku pengguna dalam membangun kepercayaan digital secara lebih mendalam.

REFERENSI

Afifah, N., Pratama, R., & Sari, D. (2025). Analisis ancaman keamanan siber pada sistem informasi digital. *Jurnal Teknologi Informasi dan Keamanan*, 7(1), 45–55.

Azzahra, F., Nugroho, A., & Ramadhan, M. (2024). Perlindungan data pribadi dalam sistem digital di Indonesia. *Jurnal Sistem Informasi*, 10(2), 120–130.

Balaka, M., Hidayat, T., & Putri, A. (2024). Evaluasi keamanan data pada sistem berbasis web menggunakan

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.269

pendekatan privasi. *Jurnal Informatika dan Keamanan*, 9(1), 33–42.
Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017–1041.
ENISA. (2022). *ENISA threat landscape 2022*. European Union Agency for Cybersecurity.
Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90.
Hidayat, R., Saputra, D., & Wibowo, A. (2023). Implementasi *CIA Triad* dalam keamanan sistem informasi akademik. *Jurnal Teknologi Informasi*, 8(2), 89–98.
Jum'an, M., & Asyura, R. (2025). Analisis pengaruh keamanan siber terhadap kepercayaan pengguna pada layanan digital. *Jurnal Keamanan Informasi*, 6(1), 15–25.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce. *Decision Support Systems*, 44(2), 544–564.
Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (16th ed.). Pearson.
McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543–568.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016.
Stair, R., & Reynolds, G. (2018). *Principles of information systems* (13th ed.). Cengage Learning.
Syahraeni, R., Putra, I., & Lestari, N. (2024). Pengaruh keamanan sistem terhadap kepercayaan pengguna pada layanan perbankan digital. *Jurnal Sistem Informasi dan Teknologi*, 11(1), 60–70.
Von Solms, B., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.
Waliullah, M., Rahman, A., & Hasan, M. (2025). Analisis *Terms and Conditions* dalam layanan digital dan implikasinya terhadap pengguna. *Jurnal Hukum dan Teknologi*, 5(1), 25–35.
Whitman, M. E., & Mattord, H. J. (2017). *Principles of information security* (6th ed.). Cengage Learning.