

Analisis Keamanan Data pada Sistem Informasi Pendidikan Berbasis Cloud Computing

Arbi Gunawan¹, Harmawanto²

¹arbigunawan321@gmail.com, ²harmawanto.hamid@gmail.com,

^{1,2} Institut Teknologi dan Sains Nahdlatul Ulama Lampung

Article Information:

Received August 29, 2025

Revised October 27, 2025

Accepted December 15, 2025

Keywords:

Analisis
Keamanan Data, Sistem
Informasi, Cloud
Computing

Abstract

The rapid development of information technology has encouraged educational institutions to adopt cloud computing-based information systems to improve the efficiency and flexibility of educational data management. This study aims to analyze data security in cloud computing-based educational information systems by examining three main aspects of information security, namely data confidentiality, data integrity, and data availability. The research method employed is a qualitative descriptive approach through system analysis, observation, and review of the security mechanisms implemented in educational information systems. The results indicate that data security implementation in cloud computing-based educational information systems has been carried out through user authentication and access control management; however, it has not been fully optimized. Weaknesses are still found in the implementation of data encryption, data change validation and auditing, as well as data backup and recovery mechanisms. In addition, human resource factors and information security policies also influence the level of data security. Therefore, strengthening technical aspects, security policies, and user awareness is necessary to enhance data security in cloud computing-based educational information systems in order to support secure, reliable, and sustainable educational services.

Abstrak

Perkembangan teknologi informasi mendorong lembaga pendidikan untuk mengadopsi sistem informasi berbasis *cloud computing* guna meningkatkan efisiensi dan fleksibilitas pengelolaan data pendidikan. Penelitian ini bertujuan untuk menganalisis keamanan data pada sistem informasi pendidikan berbasis cloud computing dengan meninjau tiga aspek utama keamanan informasi, yaitu kerahasiaan data (*confidentiality*), keutuhan data (*integrity*), dan ketersediaan data (*availability*). Metode penelitian yang digunakan adalah pendekatan deskriptif kualitatif melalui analisis sistem, observasi, dan kajian terhadap mekanisme keamanan yang diterapkan pada sistem informasi pendidikan. Hasil penelitian menunjukkan bahwa penerapan keamanan data pada sistem informasi pendidikan berbasis cloud computing telah dilakukan melalui autentikasi pengguna dan pengelolaan hak akses, namun belum sepenuhnya optimal. Masih ditemukan kelemahan dalam penerapan enkripsi data, validasi dan audit perubahan data, serta mekanisme pencadangan dan pemulihan data. Selain itu, faktor sumber daya manusia dan kebijakan keamanan informasi juga berpengaruh terhadap tingkat keamanan data. Oleh karena itu, diperlukan penguatan aspek teknis, kebijakan, dan kesadaran pengguna untuk meningkatkan keamanan data pada sistem informasi pendidikan berbasis cloud computing agar dapat mendukung layanan pendidikan yang aman, andal, dan berkelanjutan.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) pada era globalisasi dan transformasi digital telah membawa perubahan yang sangat signifikan dalam berbagai sektor kehidupan, termasuk sektor pendidikan. Pemanfaatan teknologi informasi dalam dunia pendidikan tidak lagi bersifat pilihan, melainkan telah menjadi kebutuhan strategis untuk meningkatkan efektivitas, efisiensi, dan kualitas layanan pendidikan. Lembaga pendidikan dituntut untuk mampu mengelola informasi secara cepat, akurat, dan terintegrasi guna mendukung proses akademik, administrasi, serta pengambilan keputusan manajerial. Salah satu bentuk pemanfaatan teknologi informasi yang berkembang pesat dalam beberapa tahun terakhir adalah penerapan sistem informasi berbasis *cloud computing*. Teknologi cloud computing memungkinkan penyediaan sumber daya komputasi seperti penyimpanan data, server, aplikasi, dan layanan jaringan secara dinamis melalui internet. Dengan model ini, institusi pendidikan tidak perlu lagi mengelola infrastruktur teknologi informasi secara mandiri dengan biaya tinggi, melainkan dapat memanfaatkan layanan berbasis cloud yang lebih fleksibel, skalabel, dan efisien.

Dalam lingkungan pendidikan, sistem informasi berbasis cloud computing digunakan untuk mendukung berbagai aktivitas akademik dan non-akademik, seperti Sistem Informasi Akademik (SIKAD), Learning Management System (LMS), penyimpanan dokumen akademik, pengelolaan data peserta didik dan pendidik, serta layanan administrasi keuangan dan kepegawaian. Penggunaan sistem informasi berbasis cloud memungkinkan akses data secara real-time oleh berbagai pemangku kepentingan, baik pihak manajemen, pendidik, tenaga kependidikan, maupun peserta didik, tanpa terikat oleh batasan waktu dan lokasi.

Meskipun demikian, kemudahan dan efisiensi yang ditawarkan oleh cloud computing juga diiringi dengan meningkatnya risiko terhadap keamanan data. Data yang dikelola oleh sistem informasi pendidikan umumnya bersifat sangat sensitif dan bernilai tinggi, seperti data identitas pribadi, nilai akademik, riwayat pendidikan, data keuangan, serta dokumen institusional yang bersifat rahasia. Apabila data tersebut tidak dikelola dengan sistem keamanan yang memadai, maka berpotensi menimbulkan berbagai permasalahan, seperti kebocoran data (*data breach*), penyalahgunaan informasi, pencurian identitas, hingga kerugian institusional dan menurunnya kepercayaan publik terhadap lembaga pendidikan.

Keamanan data dalam sistem informasi berbasis cloud menjadi isu yang sangat krusial karena data tidak lagi sepenuhnya berada di bawah kendali langsung institusi pengguna, melainkan dikelola oleh pihak penyedia layanan cloud. Hal ini menimbulkan tantangan tersendiri, terutama terkait aspek kontrol data, kebijakan privasi, mekanisme perlindungan data, serta kepatuhan terhadap regulasi perlindungan data. Ketergantungan terhadap pihak ketiga dalam pengelolaan data menuntut institusi pendidikan untuk memiliki pemahaman yang komprehensif mengenai sistem keamanan cloud computing yang digunakan. Ancaman terhadap keamanan data dalam sistem informasi pendidikan berbasis cloud dapat berasal dari berbagai sumber, baik dari luar maupun dari dalam sistem. Ancaman eksternal dapat berupa serangan siber seperti *hacking*, *malware*, *phishing*, dan *ransomware*, sedangkan ancaman internal dapat berupa kesalahan pengguna, penyalahgunaan hak akses, serta lemahnya pengelolaan autentikasi dan otorisasi. Selain itu, risiko kehilangan data akibat kegagalan sistem, gangguan jaringan, atau bencana juga menjadi perhatian serius dalam pengelolaan sistem informasi berbasis cloud.

Di sisi lain, masih banyak lembaga pendidikan yang mengadopsi teknologi cloud computing tanpa diimbangi dengan penerapan kebijakan dan standar keamanan data yang memadai. Beberapa institusi pendidikan belum memiliki sistem manajemen keamanan informasi yang terstruktur, seperti penerapan enkripsi data, mekanisme *backup* dan *recovery*, manajemen akses pengguna, serta pemantauan dan audit keamanan secara berkala. Kurangnya sumber daya manusia yang kompeten di bidang keamanan informasi serta minimnya kesadaran akan pentingnya keamanan data turut memperbesar potensi terjadinya pelanggaran keamanan informasi.

Selain aspek teknis, faktor non-teknis juga berperan besar dalam keamanan data sistem informasi pendidikan. Kebijakan organisasi, budaya keamanan informasi, serta tingkat kesadaran pengguna sistem menjadi elemen penting dalam menjaga keamanan data. Tanpa adanya kebijakan yang jelas dan sosialisasi yang memadai, pengguna sistem cenderung mengabaikan aspek keamanan, seperti penggunaan kata sandi yang lemah, berbagi akun, atau mengakses sistem melalui jaringan yang tidak aman. Kondisi ini menunjukkan bahwa keamanan data tidak hanya bergantung pada teknologi, tetapi juga pada pengelolaan dan perilaku manusia yang terlibat di dalamnya.

Oleh karena itu, diperlukan suatu analisis yang komprehensif terhadap keamanan data pada sistem informasi pendidikan berbasis cloud computing. Analisis ini bertujuan untuk mengidentifikasi potensi ancaman dan kerentanan sistem, mengevaluasi mekanisme keamanan yang telah diterapkan, serta menilai kesesuaian sistem dengan prinsip-prinsip dasar keamanan informasi, seperti kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Dengan adanya analisis keamanan data yang sistematis, lembaga pendidikan dapat mengetahui tingkat keamanan sistem informasi yang digunakan serta langkah-langkah perbaikan yang perlu dilakukan.

Penelitian mengenai analisis keamanan data pada sistem informasi pendidikan berbasis cloud computing menjadi sangat relevan dan penting dilakukan, khususnya dalam konteks meningkatnya ketergantungan institusi pendidikan terhadap teknologi informasi. Hasil penelitian ini diharapkan dapat memberikan kontribusi akademik dalam pengembangan kajian keamanan informasi, sekaligus memberikan manfaat praktis bagi lembaga pendidikan dalam meningkatkan kualitas pengelolaan sistem informasi berbasis cloud. Selain itu, penelitian ini juga diharapkan dapat menjadi dasar bagi pengambilan kebijakan dalam merancang strategi keamanan data yang efektif, berkelanjutan, dan sesuai dengan kebutuhan institusi pendidikan di era digital.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa keamanan data merupakan aspek yang tidak terpisahkan dari penerapan sistem informasi pendidikan berbasis cloud computing. Oleh karena itu, penelitian dengan judul “Analisis Keamanan Data pada Sistem Informasi Pendidikan Berbasis Cloud Computing” dipandang penting untuk dilakukan guna memastikan bahwa pemanfaatan teknologi cloud computing dalam pendidikan dapat berjalan secara aman, andal, dan mendukung tercapainya tujuan pendidikan yang berkualitas.

PEMBAHASAN

Keamanan Data pada Sistem Informasi Pendidikan Berbasis Cloud Computing

Penerapan *cloud computing* dalam sistem informasi pendidikan memberikan berbagai keuntungan, seperti efisiensi biaya, fleksibilitas akses, dan kemudahan pengelolaan data. Namun, di balik manfaat tersebut terdapat tantangan besar terkait keamanan data. Keamanan data dalam konteks cloud computing mencakup serangkaian mekanisme teknis dan kebijakan organisasi yang bertujuan melindungi data dari akses tidak sah, perubahan yang tidak diinginkan, serta gangguan layanan. Analisis keamanan data pada sistem informasi pendidikan berbasis cloud umumnya mengacu pada tiga prinsip utama keamanan informasi, yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). (Aji, 2025)

Keamanan data merupakan aspek fundamental dalam penerapan sistem informasi pendidikan berbasis cloud computing. Sistem informasi pendidikan mengelola berbagai jenis data yang bersifat penting dan sensitif, seperti data identitas peserta didik, data pendidik dan tenaga kependidikan, nilai akademik, riwayat pendidikan, data keuangan, serta dokumen institusional lainnya. Pengelolaan data tersebut melalui teknologi cloud computing memberikan kemudahan dalam hal aksesibilitas dan efisiensi, namun sekaligus menimbulkan tantangan yang serius dalam menjaga keamanan dan perlindungan data.

Cloud computing memungkinkan data disimpan dan diproses pada infrastruktur pihak ketiga yang diakses

melalui jaringan internet. Kondisi ini menyebabkan data tidak sepenuhnya berada di bawah kendali langsung institusi pendidikan, sehingga meningkatkan risiko terhadap berbagai ancaman keamanan informasi. Ancaman tersebut dapat berupa kebocoran data (data breach), akses tidak sah (unauthorized access), kehilangan data, maupun manipulasi data yang dapat berdampak pada keakuratan informasi dan kredibilitas lembaga pendidikan.

Keamanan data pada sistem informasi pendidikan berbasis cloud computing tidak hanya berkaitan dengan aspek teknis, tetapi juga mencakup aspek manajerial dan kebijakan. Secara teknis, keamanan data mencakup penerapan mekanisme perlindungan seperti autentikasi pengguna, pengelolaan hak akses, enkripsi data, pencatatan aktivitas sistem, serta mekanisme pencadangan dan pemulihan data. Sementara itu, dari sisi manajerial, keamanan data berkaitan dengan penyusunan kebijakan keamanan informasi, pembagian tanggung jawab, serta peningkatan kesadaran dan kompetensi sumber daya manusia yang terlibat dalam pengelolaan sistem informasi.

Dalam konteks sistem informasi pendidikan berbasis cloud, prinsip dasar keamanan informasi yang harus diperhatikan adalah Confidentiality, Integrity, dan Availability (CIA Triad). Prinsip kerahasiaan (confidentiality) menekankan bahwa data pendidikan hanya boleh diakses oleh pihak yang berwenang sesuai dengan peran dan tanggung jawabnya. Prinsip keutuhan (integrity) memastikan bahwa data yang tersimpan dalam sistem tidak mengalami perubahan secara tidak sah, baik disengaja maupun tidak disengaja. Sementara itu, prinsip ketersediaan (availability) menjamin bahwa data dan layanan sistem informasi dapat diakses secara tepat waktu ketika dibutuhkan oleh pengguna.

Berdasarkan hasil analisis, penerapan keamanan data pada sistem informasi pendidikan berbasis cloud computing umumnya telah mencakup mekanisme autentikasi pengguna melalui akun dan kata sandi. Namun, masih ditemukan kelemahan dalam pengelolaan autentikasi dan otorisasi, seperti penggunaan kata sandi yang lemah, tidak adanya autentikasi ganda (multi-factor authentication), serta pembagian akun antar pengguna. Kondisi ini berpotensi membuka celah bagi pihak yang tidak berwenang untuk mengakses sistem dan data yang tersimpan di dalamnya.

Selain itu, penerapan enkripsi data belum sepenuhnya dilakukan secara menyeluruh. Beberapa sistem hanya menerapkan enkripsi pada saat pengiriman data (data in transit), sementara data yang tersimpan (data at rest) belum dienkripsi dengan baik. Padahal, enkripsi data merupakan salah satu mekanisme penting dalam melindungi informasi dari ancaman pencurian dan penyalahgunaan data, terutama ketika terjadi kebocoran atau akses ilegal terhadap sistem cloud.

Dari sisi keutuhan data, sistem informasi pendidikan berbasis cloud telah menerapkan pembatasan hak akses berdasarkan peran pengguna, seperti administrator, guru, dan peserta didik. Namun, mekanisme pengawasan dan audit terhadap perubahan data masih terbatas. Kurangnya pencatatan aktivitas pengguna secara detail (audit trail) menyulitkan proses pelacakan apabila terjadi perubahan data yang tidak sesuai prosedur. Hal ini berpotensi menurunkan tingkat kepercayaan terhadap keakuratan data akademik yang dikelola oleh sistem informasi.

Aspek ketersediaan data dalam sistem informasi pendidikan berbasis cloud computing relatif lebih baik dibandingkan dengan sistem berbasis lokal. Cloud computing memungkinkan sistem diakses secara fleksibel dan mendukung pembelajaran serta layanan akademik berbasis daring. Namun, ketersediaan data masih sangat bergantung pada kualitas jaringan internet dan keandalan penyedia layanan cloud. Gangguan jaringan, pemeliharaan sistem, atau kegagalan layanan cloud dapat menyebabkan sistem tidak dapat diakses dalam waktu tertentu, yang berdampak pada aktivitas akademik dan administrasi.

Selain aspek teknis, faktor sumber daya manusia juga memegang peranan penting dalam keamanan data sistem informasi pendidikan berbasis cloud. Tingkat kesadaran pengguna terhadap pentingnya keamanan data

masih tergolong rendah. Beberapa pengguna belum memahami risiko keamanan informasi, seperti bahaya penggunaan perangkat umum, jaringan tidak aman, serta praktik pengelolaan kata sandi yang tidak sesuai standar. Kondisi ini menunjukkan bahwa keamanan data tidak dapat hanya mengandalkan teknologi, tetapi juga memerlukan pendekatan edukatif dan kebijakan organisasi yang kuat.

1. Aspek Kerahasiaan Data (Confidentiality)

Kerahasiaan data merupakan aspek fundamental dalam keamanan sistem informasi pendidikan berbasis cloud computing. Data yang dikelola oleh institusi pendidikan mencakup informasi pribadi peserta didik, dosen, dan tenaga kependidikan, seperti identitas diri, riwayat akademik, nilai, serta data keuangan. Informasi tersebut bersifat sensitif dan dilindungi oleh etika serta regulasi perlindungan data, sehingga tidak boleh diakses oleh pihak yang tidak memiliki kewenangan. (Iskandar et al., 2025)

Dalam konteks pendidikan, pelanggaran terhadap kerahasiaan data dapat menimbulkan dampak serius, mulai dari kerugian individu hingga menurunnya reputasi lembaga pendidikan. Kebocoran data pribadi peserta didik, misalnya, dapat menyebabkan penyalahgunaan identitas dan pelanggaran privasi. Oleh karena itu, perlindungan kerahasiaan data harus menjadi prioritas utama dalam penerapan sistem informasi berbasis cloud.

Penerapan mekanisme autentikasi dan otorisasi menjadi langkah awal dalam menjaga kerahasiaan data. Autentikasi bertujuan memastikan bahwa pengguna yang mengakses sistem benar-benar pihak yang sah, sedangkan otorisasi mengatur hak akses sesuai dengan peran pengguna. (Apriadi, 2025) Dengan pembagian hak akses yang jelas, data sensitif hanya dapat diakses oleh pihak yang berwenang.

Selain itu, penggunaan teknologi enkripsi data merupakan strategi penting dalam melindungi kerahasiaan informasi. Enkripsi diterapkan pada data yang tersimpan di server cloud (data at rest) maupun data yang ditransmisikan melalui jaringan (data in transit). Melalui enkripsi, data tetap aman meskipun terjadi penyadapan atau akses tidak sah oleh pihak ketiga.

Aspek kerahasiaan data juga sangat dipengaruhi oleh kesadaran dan perilaku pengguna sistem. Penggunaan kata sandi yang kuat, tidak berbagi akun, serta menghindari akses melalui jaringan publik yang tidak aman merupakan langkah sederhana namun efektif dalam menjaga kerahasiaan data. Dengan kombinasi antara teknologi, kebijakan, dan perilaku pengguna yang baik, kerahasiaan data dalam sistem informasi pendidikan berbasis cloud dapat terjaga secara optimal. (Pratama et al., 2024)

Kerahasiaan data (confidentiality) merupakan salah satu prinsip utama dalam keamanan informasi yang bertujuan untuk memastikan bahwa data hanya dapat diakses oleh pihak yang memiliki kewenangan sesuai dengan peran dan tanggung jawabnya. Dalam sistem informasi pendidikan berbasis cloud computing, aspek kerahasiaan data menjadi sangat krusial karena sistem tersebut mengelola berbagai informasi yang bersifat pribadi dan sensitif, seperti data identitas peserta didik, data pendidik dan tenaga kependidikan, nilai akademik, riwayat pendidikan, serta data administratif lainnya. Pelanggaran terhadap kerahasiaan data dapat menimbulkan dampak serius, baik bagi individu maupun bagi institusi pendidikan secara keseluruhan.

Berdasarkan hasil analisis, penerapan kerahasiaan data pada sistem informasi pendidikan berbasis cloud computing umumnya telah dilakukan melalui mekanisme autentikasi pengguna, seperti penggunaan akun dan kata sandi untuk mengakses sistem. Mekanisme ini bertujuan untuk membatasi akses sistem hanya kepada pengguna yang terdaftar. Namun demikian, efektivitas mekanisme autentikasi tersebut masih bergantung pada kebijakan pengelolaan akun dan tingkat kesadaran pengguna dalam menjaga kredensial akses. Penggunaan kata sandi yang lemah, penggunaan ulang kata sandi, serta kebiasaan berbagi akun masih menjadi permasalahan yang dapat melemahkan perlindungan kerahasiaan data.

Selain autentikasi, pengelolaan hak akses (access control) merupakan elemen penting dalam menjaga kerahasiaan data. Sistem informasi pendidikan berbasis cloud umumnya menerapkan pembagian hak akses berdasarkan peran pengguna, seperti administrator, guru, tenaga kependidikan, dan peserta didik. Pembagian peran ini bertujuan untuk memastikan bahwa setiap pengguna hanya dapat mengakses data yang relevan dengan tugas dan tanggung jawabnya. Namun, hasil analisis menunjukkan bahwa dalam beberapa kasus, pengaturan hak akses belum dilakukan secara rinci dan konsisten, sehingga membuka peluang bagi pengguna untuk mengakses data yang seharusnya tidak menjadi kewenangannya.

Aspek lain yang sangat penting dalam menjaga kerahasiaan data adalah penerapan enkripsi. Enkripsi data berfungsi untuk melindungi informasi agar tidak dapat dibaca oleh pihak yang tidak berwenang, baik ketika data disimpan dalam sistem cloud (data at rest) maupun ketika data dikirimkan melalui jaringan (data in transit). Hasil penelitian menunjukkan bahwa penerapan enkripsi pada sistem informasi pendidikan berbasis cloud masih belum merata. Beberapa sistem hanya menerapkan enkripsi pada proses transmisi data, sementara data yang tersimpan di server cloud belum seluruhnya dienkripsi. Kondisi ini meningkatkan risiko kebocoran data apabila terjadi akses ilegal terhadap infrastruktur penyimpanan cloud.

Selain aspek teknis, faktor manusia juga memiliki pengaruh besar terhadap kerahasiaan data. Tingkat literasi keamanan informasi pengguna sistem, baik pendidik, tenaga kependidikan, maupun peserta didik, masih tergolong beragam. Kurangnya pemahaman mengenai praktik keamanan informasi, seperti penggunaan perangkat pribadi yang aman, pemilihan jaringan internet yang terpercaya, serta kewaspadaan terhadap serangan phishing, dapat meningkatkan risiko pelanggaran kerahasiaan data. Oleh karena itu, penguatan aspek kerahasiaan data perlu diiringi dengan upaya peningkatan kesadaran dan edukasi keamanan informasi kepada seluruh pengguna sistem.

Dalam konteks cloud computing, kerahasiaan data juga berkaitan erat dengan kebijakan privasi dan perjanjian layanan dengan penyedia cloud. Institusi pendidikan perlu memastikan bahwa penyedia layanan cloud memiliki komitmen yang jelas terhadap perlindungan data, termasuk kebijakan akses data oleh pihak ketiga, lokasi penyimpanan data, serta mekanisme penanganan insiden keamanan. Kurangnya pemahaman terhadap kebijakan dan kontrak layanan cloud dapat menimbulkan risiko kebocoran data yang berada di luar kendali langsung institusi pendidikan.

Dengan demikian, aspek kerahasiaan data dalam sistem informasi pendidikan berbasis cloud computing memerlukan pendekatan yang menyeluruh dan terintegrasi. Penerapan mekanisme autentikasi dan otorisasi yang kuat, enkripsi data yang menyeluruh, kebijakan pengelolaan akun yang ketat, serta peningkatan kesadaran pengguna merupakan langkah-langkah penting dalam menjaga kerahasiaan data. Upaya tersebut diharapkan dapat meminimalkan risiko kebocoran data dan memastikan bahwa sistem informasi pendidikan berbasis cloud dapat digunakan secara aman dan terpercaya oleh seluruh pemangku kepentingan.

2. Aspek Keutuhan Data (Integrity)

Keutuhan data berkaitan dengan jaminan bahwa data dalam sistem informasi pendidikan berbasis cloud tetap akurat, lengkap, dan konsisten sepanjang siklus penggunaannya. Dalam dunia pendidikan, keakuratan data sangat penting karena berkaitan langsung dengan penilaian akademik, pengambilan keputusan, serta perencanaan institusi. (Judijanto et al., 2025)

Perubahan data yang tidak sah, baik disengaja maupun tidak disengaja, dapat menimbulkan kesalahan informasi yang berdampak luas. Misalnya, perubahan nilai akademik tanpa otorisasi dapat merugikan peserta didik dan menimbulkan konflik akademik. Oleh karena itu, perlindungan terhadap keutuhan data menjadi kebutuhan yang tidak dapat diabaikan.

Ancaman terhadap keutuhan data dapat berasal dari kesalahan pengguna, gangguan sistem, maupun serangan siber seperti malware yang memodifikasi data. Lingkungan cloud computing yang memungkinkan akses jarak jauh oleh banyak pengguna meningkatkan potensi terjadinya risiko tersebut. (Wulan et al., 2024)

Untuk menjaga keutuhan data, sistem informasi pendidikan perlu dilengkapi dengan mekanisme pengendalian perubahan data. Penerapan audit trail memungkinkan setiap aktivitas perubahan data dicatat secara sistematis, sehingga memudahkan proses pengawasan dan penelusuran apabila terjadi penyimpangan.

Selain itu, penggunaan checksum, validasi data, dan kontrol versi data dapat membantu memastikan bahwa data yang disimpan dan ditampilkan oleh sistem tetap sesuai dengan data asli. Dengan terjaganya keutuhan data, institusi pendidikan dapat memastikan bahwa informasi yang digunakan sebagai dasar pengambilan keputusan akademik maupun manajerial bersifat akurat dan dapat dipercaya. (Ashari, n.d.)

Keutuhan data (*integrity*) merupakan salah satu prinsip utama dalam keamanan informasi yang bertujuan untuk memastikan bahwa data yang tersimpan dan diproses dalam sistem informasi tetap akurat, konsisten, dan tidak mengalami perubahan secara tidak sah. Dalam sistem informasi pendidikan berbasis cloud computing, aspek keutuhan data menjadi sangat penting karena data yang dikelola digunakan sebagai dasar dalam pengambilan keputusan akademik dan administratif, seperti penentuan nilai peserta didik, kelulusan, pelaporan akademik, serta perencanaan kebijakan pendidikan.

Berdasarkan hasil analisis, sistem informasi pendidikan berbasis cloud computing umumnya telah menerapkan mekanisme pembatasan hak akses sebagai upaya awal untuk menjaga keutuhan data. Pembatasan hak akses ini bertujuan untuk memastikan bahwa hanya pengguna tertentu yang memiliki kewenangan untuk melakukan perubahan terhadap data. Namun demikian, efektivitas mekanisme tersebut masih sangat bergantung pada ketepatan pengaturan peran pengguna dan konsistensi dalam penerapannya. Apabila pengaturan hak akses tidak dilakukan secara ketat, maka potensi perubahan data yang tidak sah tetap dapat terjadi.

Selain pengelolaan hak akses, validasi data merupakan elemen penting dalam menjaga keutuhan data. Validasi data berfungsi untuk memastikan bahwa data yang dimasukkan ke dalam sistem telah sesuai dengan format, batasan, dan aturan yang ditetapkan. Hasil penelitian menunjukkan bahwa masih terdapat kelemahan dalam mekanisme validasi data pada beberapa proses input, seperti pengisian nilai dan data akademik lainnya. Kurangnya validasi yang memadai dapat menyebabkan terjadinya kesalahan input data, baik yang disebabkan oleh kesalahan pengguna maupun kelemahan sistem, yang pada akhirnya berdampak pada menurunnya kualitas dan keakuratan data.

Aspek keutuhan data juga berkaitan erat dengan mekanisme pencatatan aktivitas sistem (*audit trail*). Pencatatan aktivitas pengguna bertujuan untuk merekam setiap tindakan yang dilakukan dalam sistem, termasuk penambahan, perubahan, dan penghapusan data. Berdasarkan hasil analisis, penerapan *audit trail* pada sistem informasi pendidikan berbasis cloud computing belum sepenuhnya optimal. Keterbatasan dalam pencatatan dan pemantauan aktivitas sistem menyulitkan proses pelacakan apabila terjadi perubahan data yang tidak sesuai prosedur atau indikasi penyalahgunaan sistem.

Selain itu, keutuhan data dalam sistem informasi berbasis cloud juga dipengaruhi oleh proses sinkronisasi dan integrasi data antar modul sistem. Sistem informasi pendidikan umumnya terdiri dari beberapa modul yang saling terhubung, seperti modul akademik, keuangan, dan kepegawaian. Apabila proses integrasi dan sinkronisasi data tidak dikelola dengan baik, maka dapat terjadi inkonsistensi data antar modul, yang berdampak pada ketidakakuratan informasi yang dihasilkan oleh sistem.

Dalam konteks cloud computing, ancaman terhadap keutuhan data tidak hanya berasal dari kesalahan pengguna atau kelemahan sistem internal, tetapi juga dari ancaman eksternal seperti serangan siber. Serangan yang bertujuan untuk memodifikasi data secara tidak sah dapat merusak keakuratan data dan menurunkan tingkat kepercayaan terhadap sistem informasi pendidikan. Oleh karena itu, diperlukan mekanisme pengamanan tambahan, seperti penggunaan *hashing*, tanda tangan digital, serta sistem deteksi intrusi untuk memastikan bahwa data tidak mengalami perubahan yang tidak sah.

Faktor sumber daya manusia juga berperan penting dalam menjaga keutuhan data. Kurangnya pemahaman pengguna terhadap prosedur pengelolaan data dan keamanan informasi dapat meningkatkan risiko terjadinya kesalahan atau penyalahgunaan sistem. Oleh karena itu, peningkatan kompetensi dan kesadaran pengguna mengenai pentingnya menjaga keutuhan data perlu menjadi bagian dari strategi keamanan informasi institusi pendidikan.

3. Aspek Ketersediaan Data (Availability)

Ketersediaan data merupakan aspek keamanan yang memastikan bahwa sistem informasi pendidikan berbasis cloud dapat diakses oleh pengguna kapan pun dan di mana pun dibutuhkan. Ketersediaan layanan sistem informasi sangat berpengaruh terhadap kelancaran proses pembelajaran, administrasi akademik, dan layanan institusi secara keseluruhan. (Anugrah et al., 2025)

Gangguan terhadap ketersediaan data dapat menyebabkan terhambatnya aktivitas akademik, seperti pengisian KRS, akses materi pembelajaran, maupun pengolahan nilai. Dalam jangka panjang, kondisi ini dapat menurunkan tingkat kepuasan pengguna dan kepercayaan terhadap sistem informasi yang digunakan.

Ancaman terhadap ketersediaan data dapat disebabkan oleh berbagai faktor, antara lain kegagalan perangkat keras, gangguan jaringan internet, bencana alam, serta serangan siber seperti Distributed Denial of Service (DDoS). Tanpa sistem pengamanan yang baik, gangguan tersebut dapat menyebabkan layanan sistem informasi tidak dapat diakses dalam waktu yang lama. (Agustin et al., 2026)

Untuk menjamin ketersediaan data, institusi pendidikan perlu menerapkan sistem backup data secara berkala dan terjadwal. Backup data berfungsi sebagai cadangan apabila terjadi kehilangan data akibat kegagalan sistem atau serangan siber.

Selain itu, penerapan redundansi server, pemantauan sistem secara berkelanjutan, serta penyusunan rencana pemulihan bencana (disaster recovery plan) menjadi langkah strategis dalam menjaga ketersediaan sistem. Dengan upaya tersebut, sistem informasi pendidikan berbasis cloud dapat tetap beroperasi secara andal dan mendukung keberlangsungan aktivitas akademik. (Dewanti & Permana, 2026)

Berdasarkan hasil analisis, penerapan sistem informasi pendidikan berbasis cloud computing secara umum memberikan tingkat ketersediaan layanan yang lebih baik dibandingkan dengan sistem informasi berbasis lokal (*on-premise*). Cloud computing memungkinkan sistem diakses kapan saja dan dari berbagai lokasi selama tersedia koneksi internet. Selain itu, penyedia layanan cloud umumnya menyediakan infrastruktur dengan tingkat *uptime* yang tinggi, sehingga sistem informasi pendidikan dapat beroperasi secara lebih stabil dan berkelanjutan.

Namun demikian, ketersediaan data dalam sistem informasi pendidikan berbasis cloud masih menghadapi berbagai tantangan. Salah satu faktor utama yang memengaruhi ketersediaan sistem adalah ketergantungan pada jaringan internet. Gangguan jaringan, keterbatasan bandwidth, serta kualitas koneksi internet yang tidak stabil dapat menghambat akses pengguna terhadap sistem informasi. Kondisi

ini sering terjadi pada wilayah dengan infrastruktur jaringan yang belum memadai, sehingga berdampak pada kelancaran proses pembelajaran dan layanan akademik berbasis digital.

Selain faktor jaringan, ketergantungan pada penyedia layanan cloud juga menjadi tantangan dalam menjaga ketersediaan data. Apabila terjadi gangguan pada layanan cloud, seperti pemeliharaan sistem, gangguan teknis, atau kegagalan layanan (*service outage*), maka akses terhadap sistem informasi pendidikan dapat terhenti sementara. Hal ini menunjukkan bahwa meskipun cloud computing menawarkan keandalan yang tinggi, risiko gangguan layanan tetap perlu diantisipasi melalui perencanaan yang matang.

Aspek ketersediaan data juga sangat berkaitan dengan mekanisme pencadangan data (*backup*) dan pemulihan data (*disaster recovery*). Hasil penelitian menunjukkan bahwa belum semua institusi pendidikan menerapkan kebijakan pencadangan data secara rutin dan terstruktur. Kurangnya dokumentasi dan pengujian terhadap prosedur pemulihan data dapat meningkatkan risiko kehilangan data apabila terjadi kegagalan sistem, serangan siber, atau bencana alam. Oleh karena itu, strategi *backup* dan *disaster recovery* yang jelas dan teruji menjadi elemen penting dalam menjaga ketersediaan data.

Dalam konteks cloud computing, penerapan sistem redundansi dan replikasi data juga berperan dalam meningkatkan ketersediaan layanan. Replikasi data pada beberapa lokasi atau server memungkinkan sistem tetap dapat diakses meskipun terjadi gangguan pada salah satu komponen infrastruktur. Namun, penerapan mekanisme ini memerlukan perencanaan yang matang dan pemahaman yang baik terhadap arsitektur sistem cloud yang digunakan.

Selain aspek teknis, faktor manajerial dan kebijakan juga memengaruhi ketersediaan data. Kurangnya perencanaan kapasitas sistem (*capacity planning*) dan manajemen beban kerja (*load management*) dapat menyebabkan penurunan kinerja sistem pada periode penggunaan tinggi, seperti saat pengisian nilai atau pendaftaran peserta didik. Oleh karena itu, institusi pendidikan perlu melakukan evaluasi kebutuhan kapasitas sistem secara berkala agar layanan sistem informasi dapat tetap tersedia dan optimal.

SIMPULAN

Berdasarkan hasil penelitian dan pembahasan mengenai Analisis Keamanan Data pada Sistem Informasi Pendidikan Berbasis Cloud Computing, dapat disimpulkan bahwa penerapan cloud computing dalam sistem informasi pendidikan memberikan kemudahan dan efisiensi dalam pengelolaan serta akses data, namun sekaligus menimbulkan tantangan yang serius dalam aspek keamanan data. Sistem informasi pendidikan mengelola data yang bersifat sensitif dan bernilai tinggi sehingga memerlukan pengelolaan keamanan yang terencana dan berkelanjutan agar terhindar dari risiko kebocoran, penyalahgunaan, dan kehilangan data.

Aspek kerahasiaan data (*confidentiality*) pada sistem informasi pendidikan berbasis cloud computing telah diterapkan melalui mekanisme autentikasi dan pengaturan hak akses pengguna, namun pelaksanaannya belum sepenuhnya optimal. Masih terdapat kelemahan dalam penggunaan kata sandi, belum diterapkannya autentikasi ganda, serta belum meratanya penerapan enkripsi data, baik saat penyimpanan maupun pengiriman data. Kondisi ini berpotensi membuka peluang akses tidak sah terhadap data pendidikan yang dikelola oleh sistem.

Aspek keutuhan data (*integrity*) menunjukkan bahwa sistem telah menerapkan pembatasan hak akses dan pengelolaan peran pengguna, tetapi masih terdapat keterbatasan dalam validasi data, pencatatan aktivitas pengguna, dan mekanisme audit perubahan data. Kelemahan tersebut dapat menyebabkan terjadinya kesalahan atau perubahan data yang tidak sesuai prosedur, sehingga berpotensi menurunkan tingkat

keakuratan dan keandalan data sebagai dasar pengambilan keputusan akademik dan administratif.

Aspek ketersediaan data (availability) pada sistem informasi pendidikan berbasis cloud computing secara umum lebih baik dibandingkan dengan sistem berbasis lokal karena memungkinkan akses data secara fleksibel dan berkelanjutan. Namun, ketersediaan data masih sangat bergantung pada kualitas jaringan internet, keandalan penyedia layanan cloud, serta penerapan mekanisme pencadangan dan pemulihan data. Oleh karena itu, penguatan infrastruktur jaringan, perencanaan kapasitas sistem, serta kebijakan *backup* dan *disaster recovery* yang terstruktur menjadi hal yang penting untuk menjamin keberlangsungan layanan sistem informasi pendidikan.

DAFTAR PUSTAKA

- Agustin, R., Achmadi, R. A. P., & Rahman, R. (2026). Analisis Risiko Keamanan Data pada Penyimpanan Cloud Computing. *INOMATEC: Jurnal Inovasi Dan Kajian Multidisipliner Kontemporer*, 1(03).
- Aji, P. (2025). Cloud Computing Fundamental. *Irfan Pandu Aji*.
- Anugrah, D., Ananda, R., & Wahyuni, E. I. (2025). Evaluasi Keandalan Infrastruktur Cloud Computing Di Politeknik Belitung Untuk Mendukung Layanan Kampus Digital. *Journal Of Informatics And Busisnes*, 3(1), 1–8.
- Apriadi, E. A. (2025). BAB 4 AUTENTIKASI DAN OTORISASI. *Keamanan Jaringan Komputer*, 44.
- Ashari, D. R. W. (n.d.). BAB 3 MANAJEMEN DATA DAN DATABASE. *SISTEM INFORMASI SISTEM INFORMASI AKUNTANSI DAN BISNIS AKUNTANSI DAN BISNIS*, 29.
- Dewanti, P., & Permana, P. A. G. (2026). *Disaster Recovery Plan*. Deepublish.
- Iskandar, I., Putra, D. D., Yasin, A. I., & Khairan, K. (2025). *Cyber Smart Campus: Cakap Digital & Aman Siber*. PT. Sonpedia Publishing Indonesia.
- Judijanto, L., Pasrun, Y. P., Rohman, T. B., Sudipa, I. G. I., Selviana, R., Pandawana, I. D. G. A., Listartha, I. M. E., Rusdianto, D., Salsabila, Z., & Nirsal, N. (2025). *Sistem Informasi: Teori dan Penerapannya di Berbagai Bidang*. PT. Sonpedia Publishing Indonesia.
- Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). *Keamanan Data dan Informasi*. Kaizen Media Publishing.
- Wulan, W., Hadita, H., Fauzi, A., Putri, A. M., Fitriyani, F., Astriyani, R., Arisana, V., & Cahyani, Y. I. (2024). Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis. *Jurnal Kewirausahaan Dan Multi Talenta*, 2(2), 126–137.