PAPER NAME

Isminarti_Bab15_Keamanan_dan_Privasi_dalam_Pendidikan_Digital.docx

WORD COUNT

5144 Words

CHARACTER COUNT

35424 Characters

PAGE COUNT

13 Pages

FILE SIZE

1023.3KB

SUBMISSION DATE

Aug 10, 2024 9:27 PM GMT+8

REPORT DATE

Aug 10, 2024 9:28 PM GMT+8

0% Overall Similarity

This submission did not match any of the content we compared it against.

- 0% Internet database
- 0% Publications database
- Crossref database
- Crossref Posted Content database
- 0% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 25 words)

BAB 15 KEAMANAN DAN PRIVASI DALAM PENDIDIKAN DIGITAL

Dr. Ir. Isminarti, S.T., M.T
Politeknik Bosowa

Pendahuluan

Pendidikan digital telah menjadi bagian integral dari dunia pendidikan modern. Dengan memanfaatkan teknologi, pendidikan digital menawarkan peluang untuk meningkatkan proses belajar-mengajar, meskipun juga menghadirkan tantangan baru. Studi-studi menunjukkan bagaimana digitalisasi telah mengubah pendidikan di berbagai belahan dunia. Sebagai contoh, program *Contemporary Teaching Skills for South Asia* (CONTESSA) di Kamboja dan Sri Lanka, yang didanai oleh Uni Eropa, telah menunjukkan bahwa pelatihan guru berbasis *e-learning* dapat meningkatkan kualitas pembelajaran meskipun dihadapkan dengan keterbatasan sumber daya (Hummel et al., 2024). Penelitian di Ukraina menyoroti pentingnya teknologi internet dalam membekali lulusan dengan kompetensi profesional yang tinggi, yang diperlukan dalam pasar tenaga kerja modern (Braslavska & Ozerova, 2024). Berikut ini adalah tabel 15.1 yang membahas lebih lanjut mengenai hasil dari penelitian tersebut:

Tabel 15.1. Studi Literatur dan Uraian

No.	Studi Literatur	Uraian
1.	*Modern Pedagogies in the Digital Era: Elevating Educational Standards in Teacher Education* (Hummel et al., 2024)	Program CONTESSA meningkatkan pelatihan guru melalui e-learning, berfokus pada adaptasi metodologi pengajaran abad ke-21, meningkatkan perencanaan pelajaran, dan kualitas pengajaran di Kamboja dan Sri Lanka.
2	*Digitalization of education a tribute of the time or the need of modern society, The Trend of Digitalization of Foreign Language Education in Modern Society, Development of the Education System in the Conditions of Digitalization of Modern Society* (Sarzhanova, 2024)(Sergeeva, 2019)(SY et al., 2018).	Digitalisasi pendidikan membawa tantangan seperti dehumanisasi tetapi juga menawarkan peluang besar dengan memperkenalkan teknologi jarak jauh dan pembelajaran online, yang meningkatkan kualitas pendidikan dan adaptasi terhadap teknologi modern.
3	*Digitalization of education a tribute of the time or the need of modern society* (Braslavska & Ozerova, 2024).	Teknologi internet menjadi komponen penting dalam memastikan kompetensi profesional yang tinggi dan daya saing lulusan di pasar tenaga kerja modern, dengan penekanan pada penggunaan

No.	Studi Literatur	Uraian
		teknologi modern dalam proses pelatihan profesional di Ukraina
4	*Digital socialization of personality in the educational environment* (Grevtseva, 2022)	Digitalisasi menjadi tren utama dalam pendidikan modern, dengan peran penting teknologi digital dalam pendidikan sekolah dan pelatihan spesialis masa depan, serta pentingnya platform teknologi untuk implementasi program pendidikan dan peningkatan kualitas pembelajaran jarak jauh.
5	*Digital technologies in education* (Khamza et al., 2024)	Teknologi digital memberikan fleksibilitas kepada siswa dalam memilih tempat dan metode belajar, serta memerlukan kemampuan adaptasi yang cepat dan pembelajaran keterampilan baru secara berkelanjutan untuk sukses dalam sistem pendidikan yang semakin digital.

Keamanan dan Privasi Digital dalam Pendidikan

Keamanan dan privasi digital merupakan aspek penting dalam penggunaan teknologi di era digital saat ini. Keamanan digital melibatkan berbagai tindakan pencegahan untuk melindungi pengguna dari risiko online seperti peretasan, *malware*, dan penipuan *online* dengan mengajarkan cara menghindarinya. Penggunaan kata sandi yang kuat dan unik untuk setiap akun juga sangat penting untuk menjaga kerahasiaan data. Selain itu, siswa diajarkan untuk tidak membagikan informasi pribadi sembarangan dan memahami risiko *oversharing* di media sosial. Di sisi lain, privasi digital melibatkan pemahaman tentang pengaturan privasi di platform digital agar siswa dapat mengontrol siapa yang dapat melihat informasi mereka. Etika digital juga ditekankan, seperti menghormati privasi orang lain dan menghindari tindakan *cyberbullying*. Edukasi tentang hak atas privasi dan bagaimana data pribadi dapat digunakan oleh pihak ketiga, termasuk pemahaman tentang kebijakan privasi, sangat penting untuk memastikan bahwa siswa memiliki literasi digital yang baik dan dapat menggunakan teknologi dengan aman dan bijaksana (Herawati et al., 2024). Edukasi digital tentang keselamatan dan privasi tidak hanya penting untuk penggunaan internet secara umum tetapi juga sangat relevan dan krusial dalam konteks penggunaan *metaverse*. Mempersiapkan siswa dengan literasi digital yang baik akan membantu mereka berinteraksi dengan lebih aman dan etis di lingkungan virtual yang semakin kompleks (Arrofi et al., 2024).

Tantangan dalam Pendidikan Digital

Digitalisasi pendidikan membawa serta tantangan yang harus dihadapi dengan serius. Salah satu tantangan terbesar adalah dehumanisasi hubungan pendidikan, di mana interaksi antara siswa dan guru dapat menjadi lebih pragmatis dan kurang personal. Di sisi lain, teknologi digital seperti *e-learning* dan pembelajaran *online* juga membuka peluang besar untuk meningkatkan kualitas pendidikan dan

adaptasi terhadap teknologi modern (Frolova, 2019). Pentingnya keamanan dan privasi dalam pendidikan digital sangat krusial, terutama di era globalisasi di mana teknologi memainkan peran sentral dalam proses belajar mengajar dan manajemen pemasaran pendidikan. Dengan adopsi teknologi digital yang semakin luas, institusi pendidikan mampu mencapai audiens yang lebih besar dan meningkatkan efisiensi serta efektivitas operasional mereka. Namun, manfaat ini juga disertai dengan tantangan besar terkait keamanan dan privasi data. Kesenjangan digital dan kurangnya keterampilan teknologi di kalangan staf pendidikan meningkatkan risiko kebocoran data dan serangan siber. Oleh karena itu, investasi dalam infrastruktur teknologi informasi dan komunikasi (TIK), pelatihan keterampilan teknologi, serta pengembangan kebijakan privasi yang kuat sangat penting untuk melindungi data sensitif dan memastikan informasi pribadi siswa tetap aman. Etika dalam literasi digital juga menjadi landasan penting untuk mencegah penyebaran informasi palsu, *cyberbullying*, dan menjaga privasi pengguna. Institusi pendidikan harus memberikan perhatian besar terhadap pengelolaan data dan kebijakan privasi untuk membangun reputasi sebagai entitas yang bertanggung jawab dan aman, menciptakan lingkungan belajar yang terpercaya dan terlindungi (Yandra et al., 2024)(Tanjung et al., 2024).

Pada tingkat Pendidikan Anak Usia Dini (PAUD), menjaga keamanan dan privasi menjadi sangat penting karena pendidikan digital sering kali melibatkan pengumpulan dan penyimpanan data pribadi anak-anak, seperti nama, foto, dan informasi sensitif lainnya. Melindungi data ini dari akses yang tidak sah adalah hal yang krusial untuk mencegah penyalahgunaan, seperti pencurian identitas atau pelecehan online. Anak-anak, sebagai kelompok yang rentan, membutuhkan perlindungan khusus untuk memastikan data mereka tidak disalahgunakan. Selain itu, mengedukasi anak-anak tentang keamanan digital sejak dini membantu mereka membentuk kebiasaan yang aman saat berinteraksi dengan teknologi. Mereka perlu memahami pentingnya menjaga informasi pribadi, menyadari risiko yang ada di dunia digital, dan bersikap aman saat menggunakan perangkat teknologi, yang pada akhirnya menciptakan generasi yang lebih sadar akan keamanan digital. Guru dan orang tua memegang peran penting dalam mengawasi dan membimbing anak-anak dalam penggunaan teknologi, memastikan bahwa mereka bisa memberikan pengawasan yang efektif dan melindungi anak-anak dari potensi ancaman di dunia digital. Lebih lanjut, anak-anak dapat menjadi target empuk untuk eksploitasi online jika tidak diberikan edukasi yang tepat, sehingga mengajarkan mereka tentang keamanan digital dapat membantu mencegah mereka menjadi korban kejahatan online, seperti eksploitasi seksual atau peretasan akun. Oleh karena itu, kesadaran akan privasi di dunia digital harus diajarkan sejak dini, termasuk bagaimana melindungi informasi pribadi, apa yang seharusnya tidak dibagikan secara online, serta pentingnya menjaga kata sandi dengan baik (Suryani et al., 2024).

Data seperti informasi identitas, catatan akademik, dan data kesehatan sering dikelola secara elektronik. Melindungi data ini dari akses tidak sah dan penyalahgunaan sangat penting untuk mencegah dampak negatif pada kehidupan pribadi dan masa depan siswa. Oleh karena itu, integrasi literasi digital dengan keamanan digital dianggap penting untuk membangun kecerdasan digital, sehingga semua pihak dalam pendidikan dapat mengenali dan mengatasi ancaman tersebut secara efektif. Selain itu, pentingnya membangun kesadaran dan tanggung jawab di kalangan siswa dan pendidik mengenai cara melindungi data pribadi dan menggunakan teknologi dengan aman, serta menekankan bahwa keamanan dan privasi harus didukung oleh kebijakan yang kuat dan penegakan hukum yang jelas, mengikuti standar internasional. Literasi digital yang kuat dianggap sebagai pondasi dari keamanan digital yang efektif, membantu membangun kecerdasan digital yang komprehensif dalam menghadapi berbagai risiko di dunia digital saat ini (Alamin et al., 2024).

Dalam konteks pertahanan dan keamanan data siber sejumlah tantangan keamanan yang signifikan perlu diatasi untuk melindungi data pribadi siswa, guru, dan staf administratif yang sangat berharga. Tantangan ini mencakup ancaman dari serangan siber seperti *phishing, malware,* dan *ransomware* yang dapat mengakibatkan pencurian atau kompromi data, serta kelemahan infrastruktur teknologi di banyak institusi yang masih menggunakan perangkat lunak usang, jaringan tidak aman, dan protokol keamanan yang lemah. Selain itu, penggunaan aplikasi dan platform pihak ketiga dalam pembelajaran online juga meningkatkan risiko jika standar keamanan yang tinggi tidak diterapkan. Kurangnya kesadaran dan literasi siber di kalangan pengguna, seperti pendidik dan siswa, menambah kerentanan terhadap serangan siber. Tantangan lain yang dihadapi adalah implementasi kebijakan keamanan yang sering terhambat oleh keterbatasan anggaran, sumber daya manusia yang kurang terlatih, serta resistensi terhadap perubahan. Dengan meningkatnya pembelajaran jarak jauh, perlindungan terhadap infrastruktur dan data kelas online menjadi semakin krusial, di samping ancaman serangan *Denial-of-Service* (DoS) yang dapat mengganggu akses ke platform pembelajaran (Azzahrah et al., 2024). Tantangan keamanan dalam pendidikan digital sangat kompleks dan memerlukan pendekatan yang multifaset. Pendidikan digital harus didukung oleh infrastruktur yang aman, kebijakan yang kuat, kesadaran pengguna yang tinggi, dan kepatuhan terhadap regulasi yang berlaku. Institusi pendidikan harus terus beradaptasi dengan perkembangan teknologi dan ancaman siber yang terus berkembang untuk memastikan lingkungan belajar yang aman dan efektif.

Tantangan keamanan dalam pendidikan digital mencakup ancaman siber, kerentanan sistem, dan penggunaan perangkat pribadi, yang semuanya berpotensi membahayakan data dan informasi sensitif. Ancaman siber, seperti peretasan dan serangan *malware*, mengancam integritas dan kerahasiaan data yang disimpan dan diproses oleh platform digital pendidikan. Dalam kasus sistem Penerimaan Peserta Didik Baru (PPDB) daring di Sekolah Menengah Kejuruan (SMK) dan *website* pendaftaran mahasiswa baru di Universitas Muhammadiyah Purwokerto, perlindungan terhadap data sensitif sangat penting. Penelitian menggunakan *Information System Security Assessment Framework* (ISAAF) dan metode *Vulnerability Assessment* mengungkap kerentanan sistem yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Kerentanan ini, seperti celah keamanan pada *server-side software* dan pengaturan *header* keamanan yang kurang optimal, menambah risiko terhadap keamanan data (Susanti & Sriyanto, 2024)(Hafsari, 2024). Selain itu, penggunaan perangkat pribadi oleh staf dan siswa dalam proses belajar mengajar dan administrasi meningkatkan risiko keamanan. Perangkat pribadi sering kali tidak memiliki tingkat perlindungan yang sama dengan sistem institusi, sehingga lebih rentan terhadap serangan siber dan akses tidak sah. Untuk mengatasi tantangan ini, institusi pendidikan perlu memperkuat kebijakan keamanan informasi, termasuk pelatihan keterampilan teknologi bagi staf dan siswa, serta implementasi langkah-langkah keamanan yang komprehensif. Investasi dalam infrastruktur teknologi informasi dan komunikasi (TIK) juga sangat penting untuk memastikan bahwa data tetap aman dan privasi pengguna terjaga, membangun kepercayaan dan reputasi institusi sebagai entitas yang bertanggung jawab dan aman dalam lingkungan digital yang semakin kompleks.

Pengawasan Digital dan Etika dalam Pendidikan

Sebuah artikel dengan judul *Digital Privacy in the Mainstream of Education* membahas implikasi pengawasan digital dalam pendidikan dan menyoroti kebutuhan untuk mengeksplorasi dampaknya terhadap analitik prediktif dan pengambilan keputusan di masyarakat demokratis. Pengawasan digital melibatkan pengumpulan dan analisis data siswa, yang mencakup informasi pribadi, akademis, dan perilaku. Risiko utama terkait dengan proses ini termasuk pelanggaran data, akses tidak sah, dan

penggunaan data yang tidak sesuai dengan tujuan awal. Artikel ini menggarisbawahi pentingnya kesadaran para pemangku kepentingan seperti orang tua, siswa, dan pemimpin pendidikan tentang cara kerja pengawasan digital dan dampaknya terhadap masa depan mereka. Hak atas privasi siswa dan staf adalah aspek kritis yang mencakup pengetahuan tentang data apa yang dikumpulkan, bagaimana data tersebut digunakan, serta hak untuk mengakses dan mengoreksi data. Kesenjangan kebijakan mengenai privasi digital dalam pendidikan perlu ditangani dengan pendekatan yang lebih kritis dan interdisipliner. Pendekatan ini harus dipandu oleh kerangka analisis kebijakan kritis yang mempertanyakan semua aspek kebijakan terkait masalah privasi digital yang berkembang. Selain itu, artikel ini menyoroti pentingnya kepatuhan terhadap regulasi privasi data seperti *General Data Protection Regulation* (GDPR) di Eropa dan *Children's Online Privacy Protection Act* (COPPA) di Amerika Serikat. GDPR mengharuskan persetujuan eksplisit sebelum pengumpulan data dan memberikan hak untuk menghapus data, sementara COPPA melindungi data anak-anak di bawah usia 13 tahun. Kepatuhan terhadap regulasi ini adalah kunci untuk melindungi data siswa dan memastikan keamanan serta kerahasiaan informasi mereka (Robertson & Muirhead, 2020).

Pengawasan digital dan teknologi kecerdasan buatan/*Artificial Inteligent* (AI) mempengaruhi pendidikan digital, serta implikasi etis dan sosial dari penerapan teknologi ini di lingkungan pendidikan. Pengawasan digital dalam pendidikan merujuk pada penggunaan teknologi untuk memantau aktivitas siswa, seperti perilaku online, penggunaan perangkat, dan interaksi digital. Pengawasan ini sering digunakan untuk berbagai tujuan, termasuk memastikan keamanan, mencegah kecurangan, dan memantau kinerja siswa. Pengawasan digital dalam pendidikan memungkinkan peningkatan keamanan dan perlindungan data siswa dari akses yang tidak sah, tetapi juga memunculkan kekhawatiran tentang privasi data, terutama jika teknologi seperti AI tidak dikelola dengan baik. Penerapan teknologi pengawasan, termasuk AI, sangat bergantung pada penerimaan dari siswa, guru, dan orang tua, yang dipengaruhi oleh manfaat fungsional serta kepercayaan dan persepsi etis. Pentingnya keseimbangan antara pengawasan dan privasi menjadi sorotan karena pengawasan berlebih dapat menciptakan rasa tidak nyaman dan menghambat kreativitas siswa, sementara kurangnya pengawasan dapat menimbulkan risiko keamanan. Selain itu, meskipun pengawasan digital dapat meningkatkan kualitas pendidikan melalui analisis data dan personalisasi pembelajaran, terlalu fokus pada teknologi ini dapat mengurangi interaksi manusia dan mengubah metode pengajaran tradisional. Penerapan AI dan pengawasan digital juga menimbulkan pertanyaan etis terkait penggunaan data, akses, dan potensi bias, yang bisa memperburuk ketidakadilan jika tidak diterapkan dengan hati-hati. Meskipun pengawasan digital dan AI memiliki potensi untuk meningkatkan keamanan dan efektivitas pendidikan digital, implementasinya harus dilakukan dengan mempertimbangkan implikasi etis dan sosial. Pendidikan digital perlu menyeimbangkan antara pemanfaatan teknologi untuk kemajuan pendidikan dan perlindungan hak-hak privasi siswa. Pengembangan kebijakan yang bijak dan inklusif diperlukan untuk memastikan bahwa teknologi ini digunakan secara adil dan bertanggung jawab (Park & Jones-Jang, 2023).

Pengawasan digital dalam pendidikan merujuk pada penggunaan teknologi dan data untuk memantau, mengelola, dan menilai aktivitas mahasiswa dan dosen di lingkungan pendidikan. Ini mencakup penggunaan *Learning Management Systems* (LMS), analitik pembelajaran (learning analytics), *proctoring online*, dan berbagai alat lain yang mengumpulkan dan menganalisis data pengguna. Adapun Implikasi Utama dari Pengawasan digital dalam pendidikan telah mengubah cara interaksi antara mahasiswa dan dosen, dimana mahasiswa tidak lagi hanya berperan sebagai peserta belajar, tetapi juga sebagai objek pengawasan melalui analisis data yang terus-menerus dikumpulkan. Hal ini menimbulkan kekhawatiran tentang otonomi dan privasi, karena mahasiswa mungkin merasa

kebebasan akademik dan kreativitas mereka terbatas akibat pengawasan yang konstan. Data yang dihasilkan dari aktivitas online mahasiswa sering digunakan sebagai alat pengendalian, baik untuk evaluasi kinerja, prediksi keberhasilan, maupun intervensi akademik, sehingga menimbulkan pertanyaan etis terkait penggunaan dan kontrol data tersebut. Pengawasan digital juga berpotensi memperkuat ketimpangan yang ada, dengan alat *proctoring online* yang mungkin mendiskriminasi mahasiswa berdasarkan latar belakang sosial-ekonomi atau lokasi geografis, serta algoritma yang mengandung bias yang dapat mempengaruhi hasil penilaian. Pendidikan tinggi juga semakin diperlakukan sebagai komoditas, dimana data mahasiswa menjadi aset yang dapat dieksploitasi oleh institusi atau pihak ketiga, yang berisiko menggeser fokus dari pembelajaran ke pengelolaan dan monetisasi data. Tantangan etis dan regulasi pun muncul, perlunya persetujuan, transparansi, dan akuntabilitas yang lebih dalam penggunaan data, serta regulasi yang memadai untuk menghadapi kompleksitas teknologi pengawasan baru ini (Szcyrek & Stewart, 2022).

Meskipun pengawasan digital dapat memberikan manfaat seperti peningkatan efisiensi dan personalisasi pendidikan, ada kebutuhan mendesak untuk refleksi kritis tentang bagaimana data digunakan dan dampaknya terhadap komunitas pendidikan. Pendekatan yang lebih beretika dan transparan dalam penggunaan data, termasuk melibatkan mahasiswa dan staf dalam diskusi tentang pengawasan digital dan mempromosikan kebijakan yang melindungi privasi dan otonomi individu. Pengawasan digital membawa perubahan signifikan dalam pendidikan tinggi, yang dapat memperkaya pengalaman belajar, tetapi juga berisiko menciptakan lingkungan yang lebih terkontrol dan kurang bebas. Oleh karena itu, diperlukan keseimbangan yang hati-hati antara inovasi teknologi dan perlindungan hak-hak individu.

Solusi Teknologi untuk Keamanan dan Privasi

Adapun *best practices* untuk keamanan dalam pendidikan digital berkaitan dengan penerapan langkah-langkah strategis untuk menjaga keamanan data dan jaringan di institusi pendidikan yang memanfaatkan teknologi digital.

1. Keamanan Jaringan: Praktik terbaik untuk melindungi jaringan sekolah/universitas adalah Keamanan Jaringan dalam pendidikan digital yang mengacu pada upaya melindungi infrastruktur jaringan dari ancaman seperti peretasan, *malware*, dan serangan siber lainnya. Institusi pendidikan harus menerapkan protokol keamanan yang ketat seperti *firewall*, enkripsi data, dan pemantauan jaringan secara *real-time* untuk mendeteksi aktivitas yang mencurigakan. Dalam konteks globalisasi dan digitalisasi pendidikan, keamanan jaringan menjadi esensial untuk melindungi data siswa, staf, dan institusi dari potensi kebocoran atau penyalahgunaan.
2. Manajemen Akses: Pengaturan akses yang tepat untuk siswa, staf, dan pihak ketiga adalah dengan melibatkan pengaturan hak akses yang tepat untuk berbagai kelompok pengguna di dalam institusi pendidikan, seperti siswa, staf, dan pihak ketiga (misalnya vendor atau konsultan teknologi). Pengaturan akses yang baik berarti memastikan bahwa setiap pengguna hanya memiliki akses ke data dan sistem yang relevan dengan peran mereka. Ini membantu mencegah akses tidak sah dan melindungi data sensitif dari penyalahgunaan. Sebagai contoh, siswa mungkin memiliki akses terbatas ke sumber daya pembelajaran, sementara staf pengajar dan administrasi memiliki akses lebih luas ke sistem akademik dan manajemen.
3. Kesadaran Keamanan: Program pelatihan dan kesadaran keamanan bagi siswa dan staf merujuk pada pentingnya program pelatihan yang dirancang untuk meningkatkan pemahaman siswa dan staf tentang ancaman keamanan digital dan cara menghindarinya. Mengingat tantangan yang muncul dari digitalisasi pendidikan, seperti risiko kebocoran data dan serangan siber, program

pelatihan ini bertujuan untuk membangun budaya keamanan di lingkungan pendidikan. Pelatihan tersebut mencakup topik seperti penggunaan kata sandi yang kuat, pengenalan *phishing*, serta cara melindungi informasi pribadi saat berinteraksi dengan teknologi digital.

Implementasi praktik-praktik terbaik ini sangat penting untuk memastikan bahwa pendidikan digital tidak hanya efektif dan inovatif, tetapi juga aman bagi semua pihak yang terlibat. Tanpa langkah-langkah keamanan yang tepat, risiko yang terkait dengan penggunaan teknologi digital dalam pendidikan dapat mengganggu proses belajar-mengajar dan merusak reputasi institusi pendidikan.

Solusi teknologi untuk keamanan dan privasi berfokus pada berbagai pendekatan dan teknologi yang digunakan untuk melindungi keamanan dan privasi adalah sebagai berikut:

1. Enkripsi, adalah salah satu metode utama yang digunakan untuk melindungi data di dunia digital. Dalam konteks pendidikan, enkripsi melibatkan proses mengubah data menjadi kode yang hanya dapat diakses oleh mereka yang memiliki kunci enkripsi. Ini sangat penting dalam melindungi informasi sensitif seperti data pribadi siswa, nilai, dan informasi keuangan dari akses yang tidak sah. Dengan menggunakan enkripsi, institusi pendidikan dapat memastikan bahwa data yang dikirimkan atau disimpan tetap aman meskipun terjadi pelanggaran keamanan. Manajemen kunci enkripsi adalah komponen penting dalam menjaga keamanan sistem. Pentingnya pengelolaan kunci yang aman untuk mencegah kebocoran kunci yang dapat mengkompromikan data yang dienkripsi (Isminarti et al., 2023).
2. Alat Keamanan, software dan alat keamanan merupakan komponen penting dalam infrastruktur teknologi pendidikan. Ini mencakup antivirus, firewall, dan sistem deteksi intrusi yang digunakan untuk melindungi sistem dari ancaman siber seperti malware, phishing, dan serangan peretasan. Alat-alat ini juga melibatkan manajemen identitas dan akses, yang memastikan hanya individu yang berwenang yang dapat mengakses data tertentu. Dengan menggunakan alat keamanan yang tepat, institusi pendidikan dapat mencegah kebocoran data dan menjaga integritas informasi mereka.
3. *Platform* pendidikan digital yang aman adalah kebutuhan penting di era pendidikan digital. Ini melibatkan evaluasi dan pemilihan platform yang tidak hanya mendukung pembelajaran tetapi juga memiliki fitur keamanan dan privasi yang kuat. Misalnya, platform yang mematuhi regulasi seperti GDPR atau COPPA memastikan bahwa data siswa dikelola dengan benar dan dilindungi dari penyalahgunaan. Platform ini juga harus menyediakan pengaturan privasi yang memungkinkan pengguna untuk mengontrol siapa yang dapat mengakses informasi mereka, serta fitur untuk mengenkripsi komunikasi antara siswa dan guru.

Studi kasus pada salah satu sekolah di Indonesia yang menerapkan metode *Caesar Cipher* untuk meningkatkan keamanan pada Sistem Informasi Akademik Sekolah berbasis Android. Adapun implementasi kebijakan keamanan dan privasi diuraikan sebagai berikut:

1. Pentingnya Keamanan Data: Sistem Informasi Akademik Sekolah melibatkan informasi penting dan sensitif seperti data siswa, nilai, dan catatan akademik. Menyadari pentingnya menjaga kerahasiaan dan integritas data ini, maka prioritas utama adalah meningkatkan keamanan data.
2. Metode *Caesar Cipher*: Metode *Caesar Cipher* adalah teknik enkripsi klasik yang menggantikan setiap huruf dalam teks dengan huruf lain berdasarkan pergeseran tertentu dalam alfabet. Meskipun sederhana, metode ini dipilih karena kemudahannya dalam implementasi pada platform Android. Sekolah memiliki keterbatasan dalam hal sumber daya atau kebutuhan akan solusi yang cepat dan mudah diimplementasikan untuk menjaga keamanan data.

3. Implementasi dalam Sistem Informasi Akademik: Implementasi Caesar Cipher dalam Sistem Informasi Akademik Sekolah bertujuan untuk mengenkripsi data sehingga lebih sulit diakses oleh pihak yang tidak berwenang. Meskipun metode ini dikenal sederhana dan tidak memberikan tingkat keamanan yang sangat tinggi, dalam konteks ini, *Caesar Cipher* digunakan sebagai bagian dari langkah awal atau komponen dari pendekatan keamanan yang lebih komprehensif.

Secara keseluruhan, implementasi kebijakan keamanan dan privasi mencerminkan pendekatan yang pragmatis dan bertahap, di mana langkah-langkah sederhana seperti *Caesar Cipher* digunakan sebagai pondasi yang dapat dikembangkan lebih lanjut untuk meningkatkan keamanan sistem secara keseluruhan (Amsyari & Gunawan, 2024).

Studi kasus di salah satu website perguruan tinggi yang digunakan untuk proses pendaftaran mahasiswa baru. Berikut adalah kebijakan keamanan dan privasi yang diimplementasikan serta dianalisis terkait keamanan *website* tersebut. *Website* pendaftaran mahasiswa baru merupakan salah satu sistem yang sangat penting di institusi pendidikan, karena menjadi pintu masuk bagi calon mahasiswa untuk mendaftar. Mengingat sensitivitas data pribadi yang dikumpulkan, seperti nama, alamat, nomor identitas, dan informasi kontak, *website* ini harus memiliki kebijakan keamanan yang kuat untuk melindungi data dari ancaman keamanan siber. Studi kasus menggunakan *Metode Vulnerability Assessment* untuk mengidentifikasi potensi kerentanan yang ada pada *website*. Proses ini melibatkan serangkaian pengujian untuk mendeteksi kelemahan dalam sistem, seperti celah keamanan yang bisa dieksploitasi oleh penyerang untuk mencuri atau merusak data.

Secara umum aspek keamanan diuji berdasarkan tingkat keamanannya sebagai berikut:

1. Keamanan Data Input: Pengujian dilakukan untuk memastikan bahwa data yang dimasukkan oleh pengguna (misalnya calon mahasiswa) tidak dapat disusupi melalui teknik seperti SQL *Injection* atau *Cross-Site Scripting* (XSS). Hasil pengujian menunjukkan bahwa ada beberapa input yang tidak sepenuhnya divalidasi, yang bisa menjadi celah bagi penyerang untuk memasukkan kode berbahaya.
2. Keamanan Data Transfer: *Website* diuji untuk memastikan bahwa data yang dikirimkan antara pengguna dan *server* dilindungi melalui enkripsi, misalnya menggunakan protokol HTTPS. Studi menemukan bahwa meskipun sebagian besar data ditransfer dengan aman, ada beberapa bagian dari website yang masih menggunakan koneksi HTTP yang tidak terenkripsi, sehingga data tersebut rentan terhadap serangan *man-in-the-middle*.
3. Keamanan Penyimpanan Data: Data pengguna yang disimpan di *server* diuji untuk melihat apakah dilindungi dengan baik, misalnya melalui enkripsi atau *hashing*. Studi menunjukkan bahwa ada kelemahan dalam metode penyimpanan data yang dapat dieksploitasi jika penyerang berhasil mengakses *server*.
4. Kebijakan Akses: Implementasi kebijakan akses diuji untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data sensitif. Studi menemukan bahwa ada beberapa kelemahan dalam manajemen akses, seperti akun admin yang tidak dilindungi dengan baik oleh kata sandi yang kuat.

Studi ini menekankan pentingnya penilaian kerentanan secara rutin untuk menjaga keamanan sistem informasi, terutama yang menangani data pribadi yang sensitif.

Kesimpulan dan Rekomendasi

Digitalisasi pendidikan telah memberikan dampak signifikan terhadap proses belajar-mengajar di era modern, menghadirkan berbagai manfaat seperti fleksibilitas pembelajaran, peningkatan akses terhadap pendidikan, dan peningkatan kompetensi profesional melalui penggunaan teknologi internet. Program-program seperti CONTESSA menunjukkan bagaimana *e-learning* dapat meningkatkan kualitas pelatihan guru, sementara studi di Ukraina menekankan pentingnya teknologi digital dalam meningkatkan daya saing lulusan. Meskipun demikian, digitalisasi juga menghadirkan tantangan, termasuk dehumanisasi hubungan pendidikan, peningkatan pragmatisme, serta ancaman terhadap keamanan dan privasi data.

Keamanan dan privasi digital menjadi aspek krusial yang perlu dikelola dengan serius. Ancaman siber, kerentanan sistem, dan penggunaan perangkat pribadi yang tidak dilindungi dengan baik meningkatkan risiko terhadap keamanan data. Selain itu, pengawasan digital dalam pendidikan menimbulkan risiko pelanggaran privasi, yang memerlukan kesadaran dan pengelolaan yang hati-hati oleh semua pemangku kepentingan. Pentingnya literasi digital dan etika dalam penggunaan teknologi menjadi semakin relevan untuk memastikan bahwa siswa dapat berinteraksi dengan aman dan etis di lingkungan digital. pentingnya juga merujuk kepatuhan terhadap regulasi privasi data seperti *General Data Protection Regulation* (GDPR) di Eropa dan *Children's Online Privacy Protection Act* (COPPA) di Amerika Serikat.

Solusi teknologi untuk keamanan dan privasi dalam pendidikan digital sangat penting untuk melindungi data sensitif dan menciptakan lingkungan belajar yang aman. Institusi pendidikan perlu berinvestasi dalam teknologi dan kebijakan yang memastikan data tetap terlindungi dari ancaman siber, serta mendidik siswa dan staf mengenai praktik keamanan digital yang baik. Ini bukan hanya soal memenuhi kebutuhan teknis, tetapi juga memastikan bahwa lingkungan pendidikan digital adalah tempat yang aman dan terpercaya bagi semua pengguna. Terbukti bahwa meskipun *Caesar Cipher* bukan solusi yang paling kuat, perancangannya dan implementasinya dapat dianggap sebagai langkah efektif awal dalam melindungi data dalam aplikasi berbasis Android. Ini relevan dalam konteks kebijakan keamanan yang lebih luas, di mana langkah-langkah dasar seperti ini dapat menjadi bagian dari strategi keamanan yang berlapis-lapis, yang kemudian dapat ditingkatkan dengan metode enkripsi yang lebih canggih atau langkah-langkah keamanan tambahan lainnya.

Adapun rekomendasi yang diberikan adalah:

1. Penguatan Kebijakan Keamanan dan Privasi: Institusi pendidikan perlu memperkuat kebijakan keamanan informasi dan privasi digital dengan mengadopsi standar yang ketat seperti GDPR dan COPPA. Implementasi langkah-langkah keamanan yang komprehensif, termasuk pelatihan keterampilan teknologi bagi staf dan siswa, sangat diperlukan untuk melindungi data sensitif.
2. Investasi dalam Infrastruktur Teknologi: Institusi pendidikan harus berinvestasi dalam infrastruktur TIK yang aman dan handal untuk mendukung lingkungan digital yang semakin kompleks. Penggunaan perangkat pribadi dalam proses pendidikan harus diatur dengan kebijakan yang jelas untuk mengurangi risiko keamanan.
3. Peningkatan Literasi Digital: Literasi digital harus menjadi bagian integral dari kurikulum pendidikan, dengan fokus pada keamanan digital, privasi, dan etika dalam penggunaan teknologi. Edukasi mengenai hak privasi dan cara melindungi data pribadi harus ditanamkan sejak dini kepada siswa.

4. Pengembangan Pendekatan Interdisipliner: Kesenjangan kebijakan terkait privasi digital perlu diatasi dengan pendekatan interdisipliner yang melibatkan analisis kebijakan kritis. Pemangku kepentingan harus dilibatkan secara aktif dalam proses pengambilan keputusan terkait dengan pengawasan digital dan dampaknya terhadap siswa.
5. Kepatuhan terhadap Regulasi: Institusi pendidikan harus memastikan kepatuhan terhadap regulasi privasi data, baik di tingkat nasional maupun internasional, untuk melindungi hak privasi siswa dan staf.
6. Mengimplementasikan validasi input yang lebih ketat untuk mencegah serangan injeksi dan XSS.
7. Memastikan bahwa semua komunikasi antara pengguna dan server menggunakan protokol HTTPS untuk melindungi data selama transfer.
8. Menguatkan kebijakan akses dengan menggunakan kata sandi yang lebih kuat dan pengaturan hak akses yang lebih ketat.

Dengan menerapkan rekomendasi ini, institusi pendidikan dapat memanfaatkan teknologi digital secara optimal sambil memastikan keamanan dan privasi data pengguna, menciptakan lingkungan belajar yang aman, etis, dan berkelanjutan.

Daftar Pustaka

Alamin, Z., Khairunnas, Teguh Ansyor Larosae, Ummu Rofikah, Randitha Missouri, Sutriawan, & Muh. Alimin. (2024). Membangun Kecerdasan Digital Melalui Integrasi Literasi Digital dan Keamanan Digital. *Journal of Excellence Humanities and Religiosity*, *2*(2), 59–70. https://doi.org/10.34304/joehr.v2i2.247

Amsyari, A. A., & Gunawan, B. (2024). Perancangan Dan Implementasi Caesar Chiper Untuk Meningkatkan Keamanan Sistem Informasi Akademik Sekolah Berbasis Android. *Saturnus : Jurnal Teknologi dan Sistem Informasi*, *3*, 151–161. https://journal.arteii.or.id/index.php/Saturnus/article/view/205

Arrofi, R. A., Ajie, R., Ananda Hersya, D., Sutabri, T., & Bina Darma, U. (2024). Metaverse dan Implikasinya pada Privasi dan Keamanan Data Pengguna. *IJM: Indonesian Journal of Multidisciplinary*, *2*(1), 84–90. https://journal.csspublishing/index.php/ijm

Azzahrah, B. T., Naufal, M., Hamdi, R., Raynee, R., & Layla, Z. (2024). Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi. *Jurnal Pendidikan Tambusai*, *8*(2), 23934–23943. https://jptam.org/index.php/jptam/article/view/15661

Braslavska, O., & Ozerova, L. (2024). Digitalization of Education a Tribute of the Time or the Need of Modern Society. *Problems of Modern Teacher Training*, *1*(1(29)), 74–82. https://doi.org/10.31499/2307-4914.1(29).2024.305098

Frolova, P. I. (2019). The problems of digitalization of education in the context of the transformation of modern society. In *Voprosy pedagogiki*.

Grevtseva, G. Y. (2022). Digital socialization of personality in the educational environment. In *Bulletin of SUSU. Series: Education. Pedagogical .*

Hafsari, S. A. (2024). Analisis Keamanan Website Pendaftaran Mahasiswa Baru Dengan Munggunakan Metode Vulnerability Assessment TIN : Terapan Informatika Nusantara. *TIN: Terapan Informatika Nusantara*, *4*(11), 698–708. http://ejurnal.seminar-id.com/index.php/tin/article/view/5060

Herawati, E. S. B., Mustofa, Z., Sari, M. N., Mirsa, N. R. P., Widiyan, A. P., & Astuti, Y. (2024). Edukasi Digital

Safety Dalam Meningkatkan Kecakapan Bermedia Digital Siswa. *Lamahu: Jurnal Pengabdian Masyarakat Terintegrasi*, *3*(1), 47–54. https://doi.org/10.37905/ljpmt.v3i1.24090

Hummel, S., Bohlinger, S., & Sheehan, B. (2024). Modern Pedagogies in the Digital Era: Elevating Educational Standards in*: Hummel, S. (eds) Empowering Education in Cambodia and Sri Lanka: Quality Improvement in Teaching and Learning in the 21st Centur. Doing Higher Education. Springer VS, Wiesbade*, 65–76. https://doi.org/10.1007/978-3-658-43306-2_5

Isminarti, Ilham, A. A., Arief, A., & Syafaruddin. (2023). Improved Data Security Using Advanced Encryption Standard Algorithm on Long-Range Communication System At Smart Grid. *ICIC Express Letters, Part B: Applications*, *14*(5), 499–508. https://doi.org/10.24507/icicelb.14.05.499

Khamza, A., Zhanguttin, B., Omarbekova, A., & Nurman, S. (2024). Digital technologies in education. *Scientific Herald of Uzhhorod University. Series Physics*, *0*(55), 1955–1964. https://doi.org/10.54919/physics/55.2024.195bw5

Park, Y. J., & Jones-Jang, S. M. (2023). Surveillance, security, and AI as technological acceptance. *AI and Society*, *38*(6), 2667–2678. https://doi.org/10.1007/s00146-021-01331-9

Robertson, L., & Muirhead, B. (2020). Digital Privacy in the Mainstream of Education. *The Journal of Systemics, Cybernetics & Systemics Journal*, *18*(7), 8. https://www.researchgate.net/profile/Lorayne-Robertson-2/publication/362701347_Digital_Privacy_in_the_Mainstream_of_Education/links/62fa93adaa4b1206fab33c4d/Digital-Privacy-in-the-Mainstream-of-Education.pdf

Sarzhanova, D. (2024). The Trend of Digitalization of Foreign Language Education in Modern Society. *Fergana State University Conference*. https://conf.fdu.uz/conf/article/view/3250

Sergeeva, M. G. (2019). Media education in the conditions of digitalization of modern society. In *Kazan Pedagogical Journal*.

Suryani, V., Erfianto, B., & Cahyani, N. D. (2024). Edukasi Literasi Keamanan Digital di PAUD RA-Al-Ghiffari, Sukabirus, Dayeuhkolot, Bandung. *Jurnal Pengabdian Kepada Masyarakat (JPKM) TABIKPUN*, *5*(1), 81–88. https://tabikpun.fmipa.unila.ac.id/index.php/jpkm_tp/article/view/150

Susanti, D., & Sriyanto, S. (2024). Analisis Uji Kualitas Keamanan Website PPDB SMK X Menggunakan Metode Isaaf. *IndraTech*. http://www.ojs.stmikindragiri.ac.id/index.php/jit/article/view/139%0Ahttps://www.ojs.stmikindragiri.ac.id/index.php/jit/article/viewFile/139/117

SY, T. P. V, Shuvaev, A. V, Natsubize, A. S., & Vasilyev, I. A. (2018). Development of the Education System in the Conditions of Digitalization of Modern Society. In *Sciences*. elibrary.ru. https://elibrary.ru/item.asp?id=58801287

Szcyrek, S., & Stewart, B. (2022). Surveillance in the System: Data as Critical Change in Higher Education. *The Open/Technology in Education, Society, and Scholarship Association Journal*, *2*(2), 1–20. https://doi.org/10.18357/otessaj.2022.2.2.34

Tanjung, A. Q., Suciptaningsih, O. A., & Asikin, N. (2024). Urgensi Etika Dalam Literasi Digital Di Era Globalisasi. *WASIS : Jurnal Ilmiah Pendidikan*, *5*(1), 32–41. https://doi.org/10.24176/wasis.v5i1.11566

Yandra, R., Mahfudnurnajamuddin, M., & Suriyanti, S. (2024). Implementasi Teknologi dalam Manajemen Pemasaran Pendidikan: Tantangan dan Peluang. *Journal of Education Research*, *5*(2), 2008–2024. https://doi.org/10.37985/jer.v5i2.1071

PROFIL PENULIS

Dr. Ir. Isminarti, S.T., M.T

Penulis lahir di Makassar, 30 Januari 1979. Penulis adalah dosen di Politeknik Bosowa, Kota Makassar Provinsi Sulawesi Selatan. Menyelesaikan pendidikan D3 pada Teknik Elektro Politeknik Negeri Ujung Pandang, S1 pada Teknik Elektro Universitas Hsanuddin, S2 pada Teknik Elektro Universitas Hsanuddin dan S3 pada Teknik Elektro Universitas Hasanuddin. Penulis menekuni bidang menulis setelah menempuh Pendidikan doctor.

Penulis saat ini berstatus sebagai dosen tetap Yayasan Aksa Mahmud Program Studi Teknik Mekatronika Politeknik Bosowa sejak tahun 2013, sebelumnya pernah mengajar di Sekolah Tinggi Managemen Informatika dan Komputer (STMIK) Dipanegara Makassar tahun 2011 – 2012, Dosen di Universitas Indonesia Timur tahun 2012 – 2013, dan pernah bekerja sebagai Asisten Manager di PT. Singa Langit tahun 2005 – 2013, serta sebagai General Manager di PT. Dhelmara Kurnia Raya Jakarta Selatan tahun 2000 - 2002.

Pengalaman menulis artikel ilmiah nasional dan internasional juga menjadi salah satu pencetus ketertarikan penulis dengan menulis. Beberapa artikel ilmiah internasional terindeks scopus, terakreditasi sinta, buku referensi telah terbit dua tahun terakhir.

Penulis memiliki kepakaran di bidang teknologi rekayasa otomasi meliputi Pemodelan dan Identifikasi Sistem, Elektronika Otomasi Industri, dan Internet of Things (IoT). Melalui kepakaran ini penulis mendapatkan hibah dari kemenristekDIKTI salah satunya adalah Penelitian Disertasi Doktor dan Hibah Inovokasi.

Email Penulis: isminarti@politeknikbosowa.ac.id

DATA PENGAJUAN ISBN DAN HKI

1. Untuk pengajuan ISBN dan HKI, mohon mengisi data berikut sesuai yang tertera pada KTP:

Nama Lengkap	**:**	Dr. Ir. Isminarti, S.T., M.T
Alamat Lengkap	**:**	Jl. Tamalate III STP 52 No. 43/11 Makassar, Prov. Sulawesi Selatan 90222
NIK	**:**	7371137001790007
Email	**:**	isminarti@politeknikbosowa.ac.id
Hp. Aktif	**:**	081355080221

FOTO KTP

(bidang data saja tidak perlu bolak-balik)

TTD DIATAS MATERAI

Pastikan Bertandatangan diatas MATERAI 10.000 menggunakan kertas putih bersih (tanpa nama dibawahnya) dan warna pulpen yang jelas (hitam atau biru)

Materai HKI

Materai ISBN

NOTE:

1. Untuk pengajuan ISBN dan HKI mohon isi data sesuai yang tertera di KTP , bukan alamat tinggal sekarang,
2. Seluruh data wajib diisi, termasuk Kode Pos, Email, dan Hp. Aktif,
3. TTD harus di dua materai yang berbeda , 1 Materai untuk HKI dan 1 Untuk ISBN

0% Overall Similarity

NO MATCHES FOUND

This submission did not match any of the content we compared it against.