Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 6, No. 1, Januari 2026, Hal. 205-222
DOI: https://doi.org/10.52436/1.jpti.1454
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Keamanan Data Berbasis Cloud: Evaluasi Konfigurasi Google Workspace for Education Plus di *International School*

Jasmine Lidwina Hanny Hedyana Putri[*1], Ulva Elviani[2]

[1,2]Pendidikan Sistem dan Teknologi Informasi, Universitas Pendidikan Indonesia, Indonesia
Email: [1]jasminelidwina06@upi.edu, [2]ulva@upi.edu

Abstrak

Digitalisasi pendidikan mendorong lembaga internasional untuk mengadopsi layanan komputasi awan dalam pengelolaan data akademik, administrasi, dan komunikasi internal. Google Workspace for Education Plus menjadi salah satu platform yang banyak digunakan karena menyediakan kemudahan akses serta fitur kolaboratif yang terintegrasi. Penggunaan platform ini membawa kebutuhan evaluasi menyeluruh terhadap keamanan data, terutama pada institusi yang memproses informasi pribadi guru dan siswa. Penelitian ini bertujuan menilai efektivitas kontrol keamanan Google Workspace melalui analisis log keamanan yang diperoleh dari Google Admin Console pada periode 12 Oktober hingga 12 November 2025. Data utama mencakup autentikasi pengguna, penggunaan 2-Step Verification, aktivitas phishing, enkripsi pesan, kebijakan Data Loss Prevention (DLP), serta aktivitas berbagi file eksternal dan akses aplikasi pihak ketiga. Evaluasi dilakukan dengan membandingkan temuan lapangan terhadap CIS Google Workspace Benchmark v1.5.0, ISO/IEC 27001:2022, dan regulasi nasional Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Hasil penelitian menunjukkan tingkat stabilitas yang tinggi pada proses autentikasi dan enkripsi data. Sistem mencatat 178 login gagal dan 14 percobaan login mencurigakan yang berhasil dihentikan. Lebih dari 33.000 pesan terenkripsi melalui TLS dan tidak ditemukan insiden DLP. Risiko signifikan muncul dari aktivitas berbagi file eksternal sebanyak 13.000 berkas serta keterhubungan dengan 85 aplikasi OAuth. Temuan tersebut menunjukkan perlunya penguatan kebijakan autentikasi, pengawasan aplikasi pihak ketiga, serta perluasan aturan pembatasan berbagi data. Penelitian ini memberikan gambaran empiris mengenai kesiapan keamanan cloud di sekolah internasional dan mendukung pengambilan kebijakan yang selaras dengan standar global dan regulasi nasional.

Kata kunci: *CIS Benchmark, Google Workspace For Education, ISO/IEC 27001, Keamanan Data, Komputasi Awan, Log Keamanan, UU PDP.*

Cloud-Based Data Security: A Descriptive Evaluative Analysis of Google Workspace for Education Plus in an International School

Abstract

The rapid digitalization of education has encouraged international schools to adopt cloud computing services to support academic management, administration, and internal communication. Google Workspace for Education Plus has emerged as a widely adopted platform due to its accessibility, collaborative tools, and integrated security features. The increasing dependence on cloud-based services creates a strong need for comprehensive security evaluations, especially for institutions handling sensitive personal data of teachers and students. This study evaluates the effectiveness of Google Workspace's security controls by analyzing security logs retrieved from the Google Admin Console between 12 October and 12 November 2025. The dataset includes user authentication activity, 2-Step Verification usage, phishing incidents, message encryption, Data Loss Prevention (DLP) status, external file-sharing activity, and third-party OAuth access. The findings are assessed against the CIS Google Workspace Benchmark v1.5.0, ISO/IEC 27001:2022 standards, and Indonesia's Personal Data Protection Law (Law No. 27 of 2022). The results indicate strong stability in authentication and data encryption processes. The system recorded 178 failed logins and 14 suspicious attempts that were successfully blocked. More than 33,000 messages were transmitted using TLS encryption and no DLP incidents were identified. Significant risks were identified in 13,000 external file-sharing activities and the presence of 85 third-party OAuth applications with active permissions. These findings highlight the need to strengthen authentication policies, monitor third-party integrations, and refine data-sharing restrictions. This study provides empirical insights into the readiness of cloud security in international schools and supports the formulation of policies aligned with global standards and national data-protection requirements.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Keywords: *CIS Benchmark, Cloud Computing, Data Security, Google Workspace For Education, ISO/IEC 27001, Personal Data Protection Law, Security Logs.*

1. PENDAHULUAN

Perkembangan teknologi komputasi awan (*cloud computing*) telah menjadi fondasi utama dalam digitalisasi pendidikan. Sekolah dan universitas kini banyak memanfaatkan layanan cloud untuk menyimpan data siswa, mengelola dokumen akademik, dan memfasilitasi kolaborasi daring yang efisien. Pemanfaatan platform seperti **Google Workspace for Education Plus** memberi kemudahan akses, fleksibilitas, dan efisiensi biaya dalam aktivitas belajar mengajar [1], [2]. Integrasi fitur *Drive*, *Docs*, *Sheets*, dan *Meet* terbukti meningkatkan efektivitas pelayanan pendidikan serta mendukung tata kelola data yang lebih cepat [3].

Kemudahan tersebut beriringan dengan peningkatan risiko kebocoran data pribadi guru dan siswa. Riset global menunjukkan bahwa lebih dari sepertiga institusi pendidikan mengalami serangan siber seperti *ransomware*, *phishing*, dan kebocoran data internal selama dekade terakhir [3]. Faktor penyebab yang paling sering ditemukan meliputi kesalahan konfigurasi sistem, lemahnya autentikasi pengguna, dan kurangnya kesadaran keamanan di kalangan staf pendidikan [4]. Studi terbaru juga mencatat bahwa hanya sebagian kecil organisasi pendidikan yang telah mengenkripsi lebih dari 80 persen data sensitif mereka di lingkungan cloud [3]. Situasi ini menunjukkan masih adanya kesenjangan antara penggunaan teknologi dan kesiapan sistem keamanan yang memadai.

Di Indonesia, adopsi sistem cloud oleh lembaga pendidikan terus meningkat, namun belum diimbangi dengan evaluasi mendalam terhadap keamanan data yang tersimpan di platform tersebut. Beberapa penelitian menemukan bahwa penerapan *Google Workspace for Education* sudah mendukung tata kelola data dan pelayanan akademik, tetapi belum banyak kajian yang menilai efektivitas kontrol keamanannya secara terukur [3]. Penelitian lain juga menyoroti perlunya penguatan kebijakan enkripsi, *data loss prevention* (DLP), serta pembatasan akses berbagi file eksternal di lingkungan pendidikan [1], [5]. Kondisi ini menunjukkan pentingnya analisis evaluatif yang berbasis data nyata seperti log keamanan dari *Google Admin Console* untuk memahami efektivitas perlindungan yang diterapkan di sekolah internasional.

Penelitian ini bertujuan **menilai efektivitas implementasi keamanan data berbasis cloud pada Google Workspace for Education Plus** dengan membandingkan hasil log keamanan terhadap tiga acuan utama: *CIS Google Workspace Benchmark v1.5.0*, *ISO/IEC 27001:2022 Information Security Management Systems*, dan *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)*. Pendekatan ini diharapkan dapat menggambarkan sejauh mana sistem keamanan cloud di sekolah internasional telah memenuhi standar teknis dan regulatif dalam perlindungan data pengguna.

Kontribusi penelitian mencakup empat hal penting. Pertama, memperkaya literatur empiris mengenai keamanan data berbasis cloud di sektor pendidikan dengan menggunakan data log aktual sebagai bukti. Kedua, memberikan dasar analisis yang dapat digunakan oleh administrator teknologi informasi sekolah untuk memperbaiki kebijakan keamanan internal. Ketiga, menghasilkan rekomendasi peningkatan keamanan yang mengacu pada standar global seperti CIS dan ISO 27001 agar lembaga pendidikan mampu menjaga integritas, kerahasiaan, dan ketersediaan data pengguna. Keempat, mendukung penerapan prinsip perlindungan data pribadi di lingkungan pendidikan sebagaimana diamanatkan dalam UU PDP [5], [6].

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif evaluatif dengan karakter kuantitatif dan kualitatif. Pendekatan deskriptif bertujuan menggambarkan kondisi keamanan data berbasis cloud pada layanan Google Workspace for Education Plus, sedangkan pendekatan evaluatif digunakan untuk menilai tingkat kepatuhan sistem terhadap standar keamanan global dan regulasi nasional. Model analisis ini berlandaskan pada konsep *Information Security Management System* (ISMS) sebagaimana dijelaskan dalam ISO/IEC 27001:2022 yang menekankan tiga pilar utama, yaitu kerahasiaan, integritas, dan ketersediaan data.

Objek penelitian adalah sistem keamanan data cloud pada satu sekolah internasional di Indonesia yang menggunakan domain institusional Google Workspace for Education Plus. Observasi difokuskan pada log keamanan di *Google Admin Console* yang meliputi autentikasi pengguna, penerapan *2-Step Verification*, aktivitas *phishing*, enkripsi pesan, berbagi file eksternal, serta kebijakan *Data Loss Prevention* (DLP). Sekolah dipilih karena memiliki tingkat adopsi sistem cloud yang tinggi dan melakukan pemrosesan data lintas batas, sesuai dengan temuan penelitian sebelumya mengenai risiko keamanan pada institusi pendidikan internasional [7] [8].

Data primer diperoleh dari observasi langsung terhadap log keamanan selama periode 12 Oktober hingga 12 November 2025, mencakup aktivitas login, enkripsi, dan berbagi data. Data sekunder bersumber dari *CIS Google*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Workspace Benchmark v1.5.0 (2024), *ISO/IEC 27001:2022 Information Security Management Systems*, dan *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi* . Analisis dilakukan secara bertahap melalui tiga pendekatan, yaitu deskriptif untuk memetakan pola keamanan, evaluatif untuk menilai tingkat kepatuhan terhadap standar CIS, ISO, dan UU PDP, serta kualitatif untuk menafsirkan hasil secara mendalam. Skema penilaian kepatuhan diadaptasi dari model ISMS yang dikembangkan sebelumnya [4]. Hasil penelitian diharapkan memberikan gambaran objektif tentang tingkat kepatuhan keamanan cloud di lingkungan pendidikan serta menjadi dasar perumusan kebijakan keamanan data digital di Indonesia

3. HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan berfungsi untuk menyajikan temuan penelitian serta menguraikan maknanya secara analitis berdasarkan teori dan standar yang digunakan. Pada bagian ini, data yang diperoleh dari log keamanan *Google Admin Console* diuraikan untuk menunjukkan tingkat efektivitas sistem keamanan data berbasis *cloud* di sekolah internasional. Hasil yang dipaparkan meliputi autentikasi pengguna, penerapan *2-Step Verification*, aktivitas *phishing*, enkripsi pesan, kebijakan *Data Loss Prevention* (DLP), serta kontrol berbagi file eksternal dan akses pihak ketiga. Setiap temuan dibandingkan dengan standar *CIS Benchmark v1.5.0*, *ISO/IEC 27001:2022*, dan ketentuan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pembahasan dilakukan secara deskriptif dan evaluatif untuk menilai sejauh mana sistem keamanan *Google Workspace for Education Plus* telah memenuhi prinsip kerahasiaan, integritas, dan ketersediaan data, sekaligus mengidentifikasi area yang masih berisiko dan memerlukan peningkatan kebijakan keamanan.

3.1. Keamanan Google Workspace

Sekolah internasional pada era digital semakin bergantung pada layanan berbasis *cloud* untuk menunjang kegiatan akademik, administrasi, dan kolaborasi antara guru dan siswa. Sistem ini memungkinkan akses data secara cepat dan fleksibel, mendukung pembelajaran jarak jauh, serta mempermudah penyimpanan dokumen institusional. Salah satu platform yang paling banyak digunakan adalah *Google Workspace for Education Plus*, karena menyediakan fitur kolaboratif dengan lapisan keamanan yang mencakup autentikasi pengguna, enkripsi data, dan kebijakan pencegahan kebocoran informasi. Infrastruktur ini dinilai mampu meningkatkan efisiensi sekaligus memberikan perlindungan data yang lebih baik di lingkungan pendidikan [6].

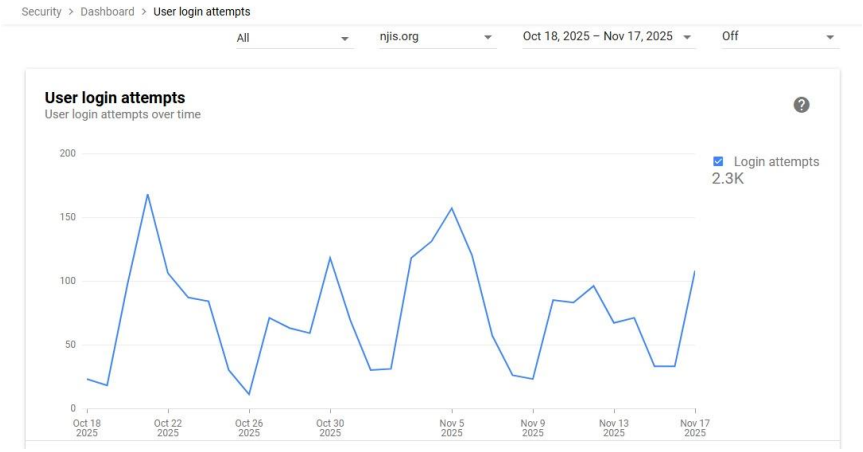
Meskipun demikian, peningkatan penggunaan layanan *cloud* juga membawa risiko keamanan baru. Salah satu penelitian menunjukkan bahwa sistem pendidikan berbasis *cloud* menghadapi ancaman seperti serangan *phishing*, penyalahgunaan kredensial, dan kebocoran data lintas batas [9]. Pengelolaan keamanan jaringan yang lemah dapat menyebabkan celah pada autentikasi dan transmisi data. Di sisi lain, terdapat temuan yang menekankan perlunya model keamanan yang lebih adaptif melalui penerapan algoritma tanda tangan digital dan *machine learning* untuk memperkuat deteksi ancaman serta menjaga integritas informasi [5].

Penerapan sistem keamanan yang efektif membutuhkan pendekatan yang sesuai dengan standar internasional seperti *ISO/IEC 27001:2022* dan *CIS Benchmark v1.5.0* yang menekankan prinsip kerahasiaan, integritas, dan ketersediaan data. Evaluasi berbasis log aktual menjadi penting untuk mengukur sejauh mana efektivitas kontrol keamanan tersebut berjalan pada platform pendidikan digital, terutama bagi sekolah internasional yang mengelola data lintas batas dan beroperasi di bawah regulasi perlindungan data pribadi.

3.2. Infrastruktur Keamanan Google Workspace

Lapisan keamanan identitas dan akses *(Authentication & Authorization)* berfungsi sebagai fondasi utama dalam menjaga keaslian dan keabsahan setiap pengguna yang terhubung ke sistem cloud pendidikan. Tujuan penerapannya adalah memastikan bahwa seluruh aktivitas digital dilakukan oleh individu yang sah dan memiliki hak akses sesuai peran yang ditetapkan. Pada *Google Workspace for Education Plus*, pengendalian identitas mencakup proses autentikasi pengguna, penerapan *2-Step Verification*, serta pemantauan aktivitas login melalui *Admin Console*. Keamanan identitas menjadi elemen krusial dalam mencegah penyalahgunaan akun, pencurian kredensial, dan akses tidak sah terhadap data akademik. *CIS Google Workspace Benchmark v1.5.0* menetapkan bahwa seluruh akun administratif wajib dilindungi autentikasi ganda dan merekomendasikan pemantauan login gagal dan pembatasan akses aplikasi pihak ketiga sebagai kontrol keamanan utama.sedangkan *ISO/IEC 27001:2022* melalui *Clause A.5.15* menekankan pentingnya pembatasan hak akses berbasis pengguna dan pemantauan aktivitas autentikasi secara berkelanjutan.

p-ISSN: 2775-4227
e-ISSN: 2775-4219



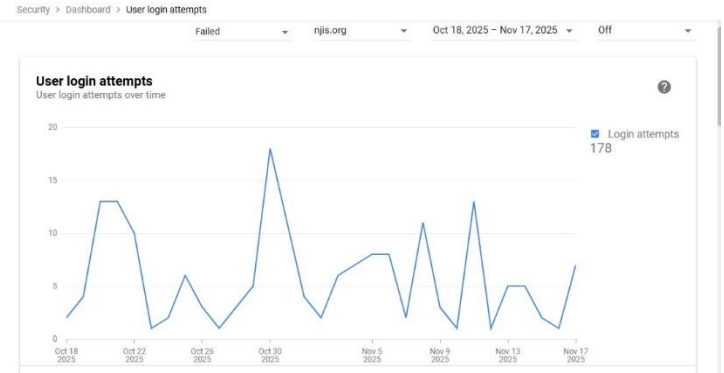
Gambar 1. User Login Attempts – All

Grafik *User Login Attempts* mencatat sekitar 2.300 aktivitas autentikasi selama periode observasi, yang menunjukkan tingginya ketergantungan pengguna terhadap layanan Google Workspace sebagai media utama dalam proses pembelajaran dan administrasi sekolah. Frekuensi akses yang konsisten mencerminkan bahwa sistem digunakan secara aktif oleh berbagai kelompok pengguna, termasuk tenaga pendidik, staf administrasi, dan peserta didik, dalam mendukung kegiatan operasional harian.

Pola fluktuasi aktivitas yang relatif stabil dari hari ke hari menunjukkan bahwa proses akses tidak mengalami lonjakan abnormal yang dapat mengindikasikan serangan otomatis berskala besar, seperti *distributed brute-force* atau *credential stuffing*. Kondisi ini memperlihatkan bahwa mekanisme pengelolaan identitas mampu menjaga stabilitas layanan meskipun digunakan secara intensif dalam lingkungan pendidikan digital.

Demikian, kestabilan pola akses juga mengindikasikan bahwa infrastruktur autentikasi memiliki kapasitas yang memadai dalam menangani beban pengguna tanpa menyebabkan gangguan layanan. Hal ini menjadi aspek penting dalam menjamin ketersediaan sistem (*availability*), mengingat proses pembelajaran dan komunikasi akademik sangat bergantung pada akses yang berkelanjutan terhadap platform cloud.

Dari perspektif manajemen keamanan informasi, hasil ini menunjukkan bahwa pengaturan autentikasi telah mendukung keseimbangan antara kemudahan akses dan keandalan sistem. Implementasi kontrol identitas yang stabil berperan dalam meminimalkan risiko gangguan layanan sekaligus memastikan bahwa aktivitas digital sekolah dapat berlangsung secara efektif dan berkesinambungan, selaras dengan prinsip *availability* dalam ISO/IEC 27001:2022.



Gambar 2. User Login Attempts – Failed

Data login gagal mencatat sebanyak 178 percobaan selama periode observasi satu bulan. Jika dibandingkan dengan total aktivitas autentikasi yang tercatat, proporsi kegagalan tergolong rendah, sehingga dapat disimpulkan bahwa mayoritas akses sistem dilakukan oleh pengguna yang sah dan berhasil melalui proses verifikasi identitas. Kondisi ini menunjukkan bahwa mekanisme autentikasi dasar telah berjalan secara efektif dalam memvalidasi kredensial pengguna.

Meskipun demikian, keberadaan percobaan login yang tidak berhasil tetap menjadi indikator penting dalam evaluasi keamanan identitas. Login gagal tidak hanya dapat disebabkan oleh kesalahan pengetikan kata sandi, tetapi juga berpotensi mencerminkan aktivitas percobaan akses tidak sah, penggunaan kredensial yang telah bocor,

p-ISSN: 2775-4227
e-ISSN: 2775-4219

atau upaya brute-force dalam skala terbatas. Demikian metrik ini berfungsi sebagai sinyal awal yang perlu dianalisis secara berkelanjutan untuk mengidentifikasi pola anomali.

CIS Google Workspace Benchmark v1.5.0 Control 6.3 menekankan bahwa aktivitas login gagal harus dipantau secara aktif karena sering kali menjadi tahap awal sebelum terjadinya kompromi akun. Peningkatan frekuensi kegagalan autentikasi pada akun tertentu dapat menunjukkan target spesifik yang sedang dicoba oleh pihak tidak berwenang, sehingga diperlukan mekanisme respons seperti pembatasan percobaan login atau verifikasi tambahan.

Dari perspektif ISO/IEC 27001:2022 Clause A.5.15, pencatatan dan evaluasi login gagal merupakan bagian dari kontrol manajemen akses yang bertujuan memastikan bahwa hanya pengguna berwenang yang dapat mengakses sistem informasi. Evaluasi ini juga mendukung prinsip akuntabilitas melalui audit trail yang memungkinkan administrator menelusuri aktivitas mencurigakan secara sistematis.

Dalam kerangka Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi Pasal 40, pengendali data memiliki kewajiban untuk menerapkan langkah teknis dan organisatoris guna mencegah akses ilegal terhadap data pribadi. Demikian, meskipun jumlah login gagal masih berada dalam batas wajar, penguatan autentikasi berlapis, pembatasan percobaan login, serta pemantauan berbasis risiko tetap diperlukan untuk menurunkan kemungkinan kompromi akun dan melindungi data pengguna secara menyeluruh.

Gambar 3. User Login Attempts – Suspicious

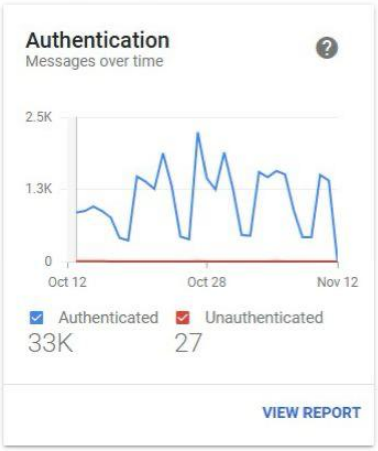
Gambar memperlihatkan tren aktivitas autentikasi pengguna yang terdeteksi sebagai upaya login mencurigakan selama periode **12 Oktober hingga 12 November 2025**. Berdasarkan data yang terekam, terdapat **14 kali percobaan login mencurigakan**, dengan peningkatan sekitar **40% dibandingkan periode sebelumnya**. Grafik menunjukkan pola fluktuatif, dengan lonjakan tertinggi terjadi pada pertengahan Oktober yang mencapai empat percobaan dalam satu hari, diikuti jeda aktivitas dan beberapa peningkatan kecil menjelang awal November.

Temuan ini menunjukkan bahwa sistem keamanan Google Workspace berhasil mendeteksi potensi anomali autentikasi, yang biasanya disebabkan oleh penggunaan kredensial tidak sah, percobaan login dari perangkat baru, atau akses dari lokasi geografis yang tidak dikenali. Mekanisme deteksi ini merupakan bagian dari *security intelligence* yang disediakan oleh *Google Admin Console*, yang berfungsi memberikan peringatan dini terhadap ancaman intrusi.

Jika dibandingkan dengan *CIS Google Workspace Benchmark v1.5.0 Control 6.3*, aktivitas semacam ini harus direspon melalui verifikasi identitas tambahan dan pembatasan akses otomatis pada akun yang mencurigakan. Berdasarkan prinsip *ISO/IEC 27001:2022 Clause A.5.15 (User Access Management)*, setiap upaya login abnormal harus dicatat dalam log audit dan diverifikasi untuk memastikan tidak ada pelanggaran autentikasi.

Kenaikan aktivitas login mencurigakan sebesar 40% dapat menjadi indikasi bahwa sebagian pengguna belum menerapkan autentikasi berlapis atau menggunakan sandi yang mudah ditebak. Dari sisi kepatuhan terhadap **UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi Pasal 40**, sekolah sebagai pengendali data wajib menjaga sistem autentikasi yang kuat agar tidak terjadi akses ilegal terhadap data pribadi guru, siswa, maupun dokumen institusional. Evaluasi berkala terhadap log keamanan perlu dilakukan agar setiap anomali dapat ditindak cepat sebelum menimbulkan risiko kebocoran data.

p-ISSN: 2775-4227
e-ISSN: 2775-4219



Gambar 4. Authentification - Messages over time

Gambar menunjukkan pola autentikasi yang terjadi pada sistem Google Workspace for Education Plus selama periode **12 Oktober hingga 12 November 2025**. Grafik mencatat total **33.000 pesan terautentikasi (authenticated)** dan hanya **27 pesan yang gagal terautentikasi (unauthenticated)**. Pola grafik terlihat stabil dengan beberapa fluktuasi kecil, menandakan proses autentikasi berjalan secara konsisten dan mekanisme verifikasi sistem bekerja dengan baik.

Volume autentikasi yang tinggi menunjukkan bahwa sebagian besar aktivitas komunikasi dan pertukaran data melalui akun pengguna telah melewati proses verifikasi yang sah. Angka *unauthenticated messages* yang rendah menggambarkan tingkat efektivitas enkripsi dan otorisasi pesan yang tinggi pada lapisan transport (*Transport Layer Security*). Pencapaian ini memperlihatkan kepatuhan sistem terhadap *CIS Benchmark Control 6.5* yang menekankan kewajiban validasi kredensial pengguna untuk setiap sesi komunikasi elektronik.

Dari perspektif *ISO/IEC 27001:2022*, hasil ini mencerminkan penerapan prinsip *confidentiality* dan *integrity* sesuai *Clause A.8.24* tentang *data protection in transit*, karena seluruh komunikasi telah melalui proses autentikasi dan verifikasi integritas data sebelum diterima oleh server tujuan. Sistem autentikasi ini juga mendukung keamanan end-to-end yang penting dalam melindungi informasi akademik dan dokumen internal sekolah dari manipulasi atau intersepsi pihak ketiga.

Pentingnya penguatan autentikasi berlapis juga didukung oleh pedoman NIST SP 800-63 yang menekankan bahwa penggunaan *multi-factor authentication* merupakan langkah fundamental dalam perlindungan identitas digital. Standar ini merekomendasikan kombinasi lebih dari satu faktor autentikasi untuk mengurangi ketergantungan pada kata sandi tunggal yang rentan terhadap pencurian kredensial, serangan phishing, dan penyalahgunaan akun. Penerapan autentikasi berlapis terbukti mampu menurunkan risiko kompromi identitas secara signifikan, khususnya pada lingkungan berbasis cloud yang diakses secara luas oleh berbagai perangkat dan lokasi pengguna[10].

Temuan ini mendukung penerapan kontrol manajemen akses sebagaimana diatur dalam ISO/IEC 27001:2022 Clause A.5.15, yang menekankan pentingnya pengendalian hak akses pengguna berdasarkan peran dan tanggung jawab. Standar ini juga menggarisbawahi perlunya pemantauan aktivitas akses secara berkelanjutan untuk memastikan bahwa setiap interaksi terhadap sistem informasi dapat ditelusuri dan diaudit. Pendekatan tersebut bertujuan mencegah akses tidak sah, membatasi penyalahgunaan hak akses, serta memperkuat akuntabilitas dalam pengelolaan keamanan informasi organisasi [11].

Walaupun angka *unauthenticated* tergolong rendah, keberadaannya tetap perlu diawasi karena dapat menandakan adanya pesan yang dikirim melalui kanal non-aman atau akun yang belum sepenuhnya mengikuti kebijakan autentikasi. Berdasarkan **Pasal 40 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi**, setiap pengendali data wajib memastikan proses komunikasi digital dilakukan dengan sistem verifikasi yang sah dan terenkripsi untuk mencegah kebocoran atau perubahan data selama pengiriman.

Evaluasi ini sejalan dengan rekomendasi CIS Google Workspace Benchmark v1.5.0 yang menekankan pentingnya pemantauan aktivitas login, pencatatan login gagal, serta penerapan kontrol akses sebagai bagian dari mekanisme deteksi dini terhadap potensi penyalahgunaan akun pengguna. CIS menempatkan pengawasan autentikasi sebagai elemen krusial dalam menjaga keamanan identitas pada lingkungan kolaborasi berbasis cloud.

Demikian, mekanisme keamanan yang teridentifikasi dalam penelitian ini juga sesuai dengan arsitektur perlindungan yang dijelaskan dalam Google Workspace Security Whitepaper. Dokumen tersebut menjabarkan penerapan pemantauan login terpusat, enkripsi komunikasi, serta sistem deteksi anomali berbasis kecerdasan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

keamanan bawaan Google untuk melindungi akun pengguna dari aktivitas mencurigakan dan ancaman siber modern [12].

Berdasarkan keseluruhan temuan autentikasi, dapat disimpulkan bahwa mekanisme identitas dan akses dalam lingkungan Google Workspace telah berfungsi secara stabil dalam mendukung aktivitas operasional sekolah. Namun, keberadaan login gagal dan aktivitas mencurigakan menunjukkan bahwa sistem autentikasi tetap menjadi salah satu titik kritis dalam keamanan cloud, khususnya pada lingkungan pendidikan yang memiliki jumlah pengguna besar dan karakteristik akses yang beragam.

Risiko utama pada sistem autentikasi tidak hanya berasal dari serangan teknis, tetapi juga dari perilaku pengguna seperti penggunaan kata sandi yang lemah, pengulangan kredensial pada layanan lain, serta rendahnya kesadaran keamanan digital. Kondisi ini memperbesar kemungkinan kompromi akun meskipun sistem telah dilengkapi dengan perlindungan otomatis.

Dalam konteks tersebut, penerapan autentikasi berlapis tidak hanya berfungsi sebagai kontrol teknis, tetapi juga sebagai mekanisme mitigasi risiko berbasis perilaku. Autentikasi berlapis mampu memutus rantai serangan meskipun kredensial utama telah diketahui oleh pihak tidak berwenang. Oleh karena itu, efektivitas keamanan identitas sangat bergantung pada konsistensi penerapan kebijakan autentikasi di seluruh kelompok pengguna.

Selain itu, pendekatan keamanan modern menekankan konsep *continuous authentication*, yaitu evaluasi berkelanjutan terhadap konteks akses seperti lokasi, perangkat, dan pola perilaku pengguna. Pendekatan ini relevan bagi lingkungan pendidikan yang mengandalkan akses jarak jauh dan penggunaan perangkat pribadi, sehingga sistem tidak hanya bergantung pada proses login awal, tetapi juga pada validasi berkelanjutan selama sesi berlangsung.

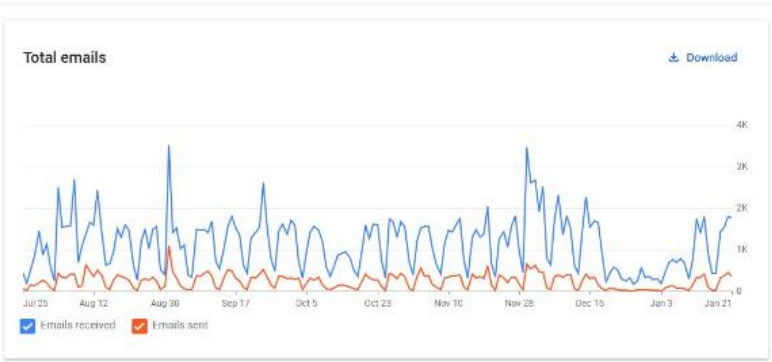
Dengan demikian, hasil observasi autentikasi dalam penelitian ini menegaskan bahwa keamanan identitas perlu dikelola sebagai proses berkelanjutan, bukan sekadar konfigurasi awal sistem. Integrasi antara kontrol teknis, kebijakan institusional, dan edukasi pengguna menjadi faktor kunci dalam menjaga keamanan akun serta melindungi data akademik dan administratif.

3.3. Observasi Log Keamanan

Observasi log keamanan menjadi fondasi penting dalam evaluasi sistem cloud karena log menyimpan seluruh aktivitas yang terjadi pada infrastruktur digital, mulai dari autentikasi, pergerakan data, hingga akses aplikasi pihak ketiga. Setiap pola aktivitas yang muncul dapat menunjukkan apakah mekanisme keamanan berjalan stabil atau terdapat indikasi ancaman. Malele (2023) menyatakan bahwa log berfungsi sebagai bagian inti dari deteksi ancaman karena mampu memperlihatkan anomali autentikasi dan penyimpangan perilaku pengguna pada platform pembelajaran berbasis cloud [13].

Turluev et al. (2023) menjelaskan bahwa institusi pendidikan menghadapi tekanan untuk memastikan keamanan data di tengah peningkatan integrasi teknologi digital. Penggunaan log memungkinkan administrator mengenali kerentanan dan menguatkan respons keamanan secara cepat [7]. Buku *Cloud Security: Concepts, Applications, and Practices* menegaskan bahwa log harus dianalisis secara berkelanjutan karena sering kali serangan muncul dari akses OAuth yang tampak normal atau dari pola login yang tidak terdeteksi oleh kontrol dasar.

Pemantauan terhadap seluruh trafik email menjadi dasar untuk memahami pola ancaman pada layanan cloud pendidikan. Email merupakan jalur masuk ancaman yang paling sering dimanfaatkan penyerang karena digunakan oleh seluruh pengguna, baik guru, staf, maupun siswa. Sistem spam filter menyediakan gambaran tentang seberapa besar volume pesan yang diterima dan seberapa efektif penyaringan otomatis yang dilakukan oleh Google Workspace.



Gambar 5. Total Emails (Received vs Sent)

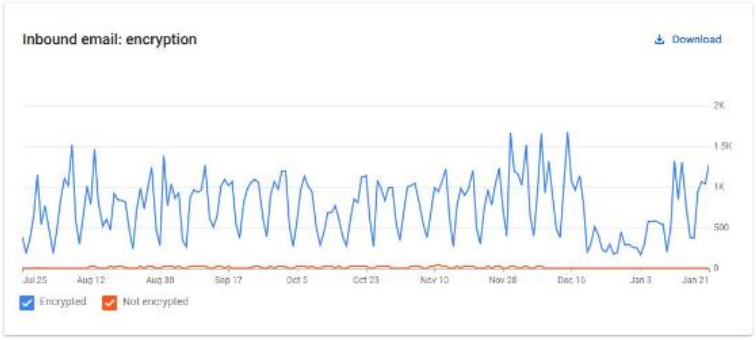
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Grafik total email memperlihatkan tingginya intensitas komunikasi digital selama periode observasi, dengan jumlah pesan masuk yang lebih dominan dibandingkan pesan keluar. Pola ini menunjukkan bahwa email berfungsi sebagai kanal utama pertukaran informasi antara sekolah, tenaga pendidik, peserta didik, serta pihak eksternal seperti orang tua dan mitra institusi.

Dominasi pesan masuk menggambarkan besarnya arus informasi yang diterima oleh pengguna dalam domain pendidikan. Kondisi ini menempatkan email sebagai salah satu titik masuk risiko keamanan yang paling signifikan, mengingat setiap pesan berpotensi membawa konten berbahaya, baik dalam bentuk tautan, lampiran, maupun teknik rekayasa sosial.

Tingginya volume pertukaran pesan juga meningkatkan kompleksitas pengelolaan keamanan, karena sistem harus mampu memproses lalu lintas email secara real-time tanpa mengganggu kelancaran komunikasi akademik. Dalam konteks ini, efektivitas mekanisme penyaringan otomatis menjadi faktor kunci untuk memastikan bahwa ancaman dapat dikendalikan sebelum menjangkau pengguna akhir.

Demikian, penerapan filter spam, deteksi phishing, serta enkripsi pesan berperan sebagai lapisan perlindungan utama dalam menjaga kerahasiaan dan integritas informasi. Kombinasi kontrol teknis tersebut penting untuk mengurangi paparan risiko sekaligus mempertahankan keandalan layanan komunikasi berbasis cloud di lingkungan pendidikan digital.



Gambar 6. Inbound Email Encryption

Grafik enkripsi email memperlihatkan bahwa hampir seluruh pesan masuk dikirim dalam kondisi terenkripsi, sementara jumlah pesan yang tidak terenkripsi berada pada tingkat yang sangat minimal. Dominasi komunikasi terenkripsi ini menunjukkan bahwa mekanisme Transport Layer Security (TLS) telah diterapkan secara konsisten dalam proses pertukaran pesan elektronik pada lingkungan Google Workspace.

Penerapan TLS berperan penting dalam melindungi data selama transmisi dengan mencegah pihak tidak berwenang melakukan penyadapan (*eavesdropping*) atau manipulasi isi pesan di jalur komunikasi. Dengan adanya proses enkripsi end-to-end pada lapisan transport, informasi yang dikirimkan tetap terlindungi meskipun melewati jaringan publik, sehingga risiko intersepsi data dapat diminimalkan secara signifikan.

Konsistensi enkripsi yang tinggi juga mencerminkan kematangan konfigurasi keamanan komunikasi, khususnya dalam memastikan bahwa koneksi antar server email memenuhi standar keamanan minimum. Hal ini mendukung prinsip *confidentiality* dan *integrity* sebagaimana diatur dalam ISO/IEC 27001:2022 Clause A.8.24 mengenai perlindungan data selama proses transmisi.

Demikian, hasil ini menunjukkan kesesuaian dengan rekomendasi CIS Benchmark yang menekankan kewajiban penggunaan saluran komunikasi aman untuk seluruh pertukaran data digital. Dalam konteks Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, penerapan enkripsi komunikasi menjadi langkah teknis penting dalam memenuhi kewajiban pengendali data untuk mencegah kebocoran informasi pribadi siswa dan tenaga pendidik selama proses pengiriman data.

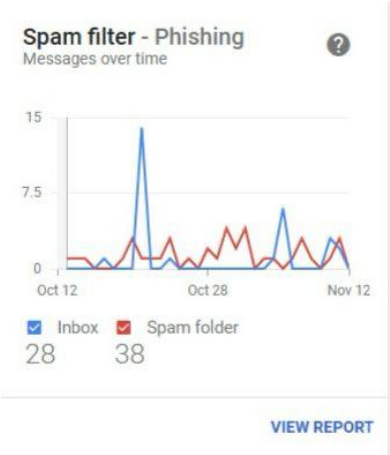
Meskipun jumlah pesan tidak terenkripsi relatif kecil, keberadaannya tetap perlu diawasi karena dapat menunjukkan keterbatasan dukungan TLS pada sistem eksternal tertentu. Demikian, pemantauan berkelanjutan dan evaluasi terhadap mitra komunikasi eksternal tetap diperlukan guna memastikan bahwa seluruh pertukaran data berlangsung melalui kanal yang aman.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Gambar 7. Spam Filter - All

Grafik menunjukkan bahwa selama periode observasi terdapat **30.000 pesan masuk** dan **3.200 pesan dialihkan ke folder spam**. Pola grafik memperlihatkan fluktuasi yang stabil, dengan volume spam yang relatif rendah dibandingkan total pesan masuk. Kondisi ini menandakan bahwa sistem filter bawaan Google Workspace bekerja efektif memisahkan pesan yang dianggap tidak aman. Volume spam yang konsisten juga menunjukkan bahwa ancaman email masih menjadi vektor utama pada lingkungan pendidikan berbasis cloud. Sistem filter tampak mampu mengurangi paparan pesan berisiko sebelum mencapai pengguna.

Serangan phishing sering menargetkan pengguna pendidikan karena profil mereka dianggap lebih mudah diarahkan pada rekayasa sosial.



Gambar 8. Spam Filter – Phishing

Data memperlihatkan **28 pesan phishing lolos ke inbox** dan **38 berhasil disaring** ke spam folder. Lonjakan besar pada akhir Oktober menunjukkan adanya upaya phishing lebih intens pada periode tersebut. Deteksi yang berhasil menempatkan lebih banyak phishing ke folder spam menunjukkan respons protektif yang berjalan baik, meskipun keberadaan 28 email phishing yang sempat masuk menunjukkan perlunya peningkatan kebijakan proteksi email atau pelatihan literasi keamanan bagi pengguna.

Temuan ini sejalan dengan laporan ENISA yang menyatakan bahwa sektor pendidikan merupakan salah satu target utama serangan phishing dan rekayasa sosial akibat tingginya intensitas komunikasi digital dan keberagaman profil pengguna [14].

Lampiran email menjadi sarana yang sering digunakan untuk menyebarkan malware atau kode berbahaya. Pemeriksaan terhadap lampiran yang ditandai sebagai mencurigakan memberikan gambaran mengenai kualitas perlindungan terhadap serangan berbasis file.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Gambar 9. Suspicious Attachments

Informasi ini membantu memahami kesiapan sistem dalam menangani ancaman yang berasal dari file yang dikirim pengguna eksternal maupun internal. Grafik menunjukkan ditemukannya **10 lampiran terenkripsi** yang dikategorikan sebagai suspicious attachments. Tidak ada lampiran yang mengandung skrip berbahaya atau anomali file lain. Penyebab tingginya jumlah encrypted attachments kemungkinan berasal dari mekanisme enkripsi otomatis atau file terproteksi password, bukan ancaman aktif. Ketiadaan file berbahaya menunjukkan lingkungan email relatif aman dari distribusi malware berbasis lampiran.

Email merupakan salah satu vektor serangan paling dominan dalam lingkungan digital modern, termasuk pada sektor pendidikan. Tingginya volume komunikasi yang teridentifikasi dalam penelitian ini memperlihatkan bahwa email menjadi media utama pertukaran informasi, namun sekaligus membuka peluang masuknya ancaman siber melalui teknik rekayasa sosial.

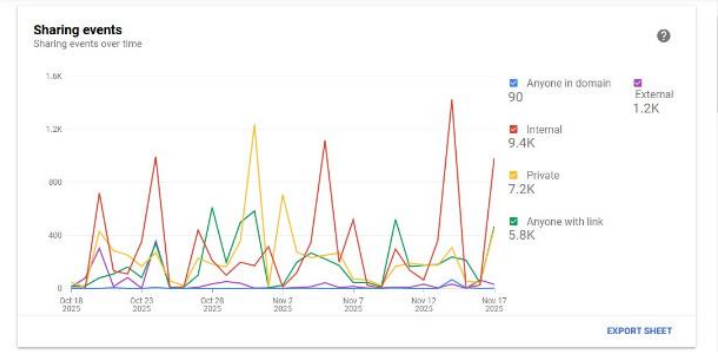
Meskipun sistem proteksi otomatis mampu menyaring sebagian besar pesan berbahaya, keberadaan email phishing yang masih dapat mencapai kotak masuk menunjukkan bahwa pendekatan berbasis teknologi saja belum sepenuhnya mampu mengeliminasi risiko. Serangan phishing modern sering kali dirancang menyerupai komunikasi akademik resmi, sehingga sulit dibedakan oleh pengguna, terutama siswa dan staf non-teknis.

Faktor manusia (*human factor*) menjadi elemen krusial dalam keamanan email. Tingkat kewaspadaan pengguna, kebiasaan membuka tautan, serta pemahaman terhadap ancaman digital sangat memengaruhi efektivitas sistem keamanan secara keseluruhan. Tanpa dukungan kesadaran keamanan, perlindungan teknis berpotensi dilewati melalui manipulasi psikologis.

Oleh karena itu, keamanan email perlu dipandang sebagai kombinasi antara teknologi, kebijakan, dan edukasi. Pelatihan keamanan siber secara berkala, simulasi phishing, serta pemberian peringatan kontekstual kepada pengguna dapat memperkuat ketahanan organisasi terhadap serangan berbasis pesan.

Temuan ini menegaskan bahwa pengelolaan keamanan email pada lingkungan pendidikan tidak hanya bertujuan memblokir ancaman, tetapi juga membangun budaya keamanan informasi yang berkelanjutan guna melindungi data pribadi dan komunikasi akademik.

Integrasi aplikasi pihak ketiga melalui OAuth membawa manfaat besar bagi produktivitas, tetapi juga menambah risiko apabila akses tidak diawasi dengan ketat. Aktivitas OAuth menunjukkan aplikasi yang baru saja memperoleh izin akses dari akun dalam domain. Data ini penting untuk menilai apakah integrasi eksternal dilakukan secara terkendali atau berpotensi membuka celah keamanan.



Gambar 10. Sharing Events Over Time

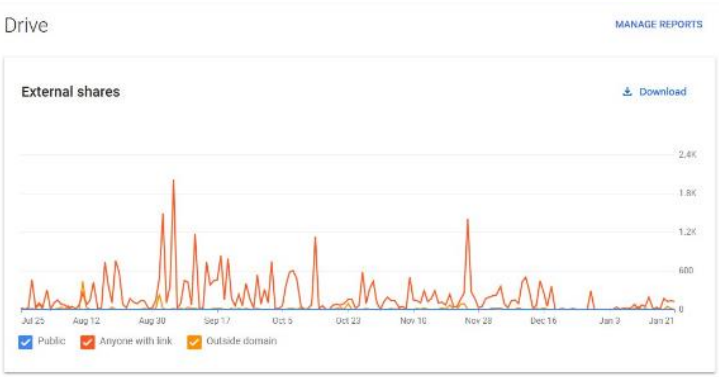
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Grafik *sharing events* memperlihatkan tingginya intensitas aktivitas kolaborasi selama periode observasi, yang mencerminkan pemanfaatan aktif fitur berbagi dokumen dalam mendukung proses pembelajaran, koordinasi administrasi, serta pertukaran materi akademik. Pola fluktuasi harian yang relatif konsisten menunjukkan bahwa aktivitas berbagi telah menjadi bagian rutin dari operasional digital sekolah.

Tingginya frekuensi kolaborasi ini menggambarkan manfaat utama Google Workspace sebagai platform kerja bersama yang mendorong efisiensi dan fleksibilitas. Namun, pada saat yang sama, peningkatan volume berbagi data juga memperluas permukaan risiko (*attack surface*) apabila kontrol akses tidak diterapkan secara proporsional terhadap tingkat sensitivitas informasi.

Aktivitas berbagi yang berlangsung secara masif berpotensi menyebabkan distribusi dokumen melebihi kebutuhan aktual pengguna, terutama apabila pengaturan akses tidak dievaluasi secara berkala. Tanpa mekanisme pembatasan berbasis peran, klasifikasi data, atau masa berlaku akses, dokumen internal berisiko tetap dapat diakses oleh pihak yang tidak lagi memiliki kepentingan operasional.

Demikian, tingginya volume *sharing events* menegaskan pentingnya pengawasan administratif terhadap pola kolaborasi digital. Pemantauan ini diperlukan untuk memastikan bahwa praktik berbagi data tetap selaras dengan prinsip *least privilege* serta mendukung perlindungan informasi akademik dan data pribadi pengguna dalam lingkungan pendidikan berbasis cloud.



Gambar 11. External Share by Type

Grafik *external share by type* memperlihatkan bahwa sebagian aktivitas berbagi dokumen dilakukan ke luar domain organisasi, termasuk melalui mekanisme "anyone with link". Pola ini menunjukkan bahwa kolaborasi tidak hanya berlangsung secara internal, tetapi juga melibatkan pihak eksternal yang berada di luar kendali langsung administrator sistem.

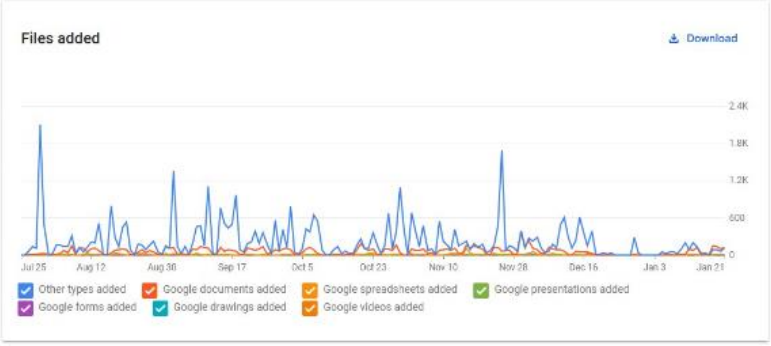
Mekanisme berbagi publik seperti "anyone with link" memiliki tingkat risiko tertinggi karena memungkinkan dokumen diakses tanpa proses autentikasi domain yang jelas. Dalam kondisi tertentu, tautan dapat diteruskan secara tidak sengaja, disimpan pada perangkat pribadi, atau diakses kembali di luar konteks kerja yang semestinya. Situasi ini berpotensi menyebabkan penyebaran data yang tidak terkontrol, terutama apabila dokumen mengandung informasi akademik, administratif, maupun data pribadi siswa.

Tingginya intensitas berbagi eksternal juga memperluas risiko kebocoran data lintas batas, yang menjadi isu penting bagi institusi pendidikan internasional. Tanpa pembatasan yang jelas, dokumen dapat diakses dari lokasi geografis yang berbeda dan oleh pihak yang tidak memiliki hubungan hukum langsung dengan institusi pengendali data.

ISO/IEC 27001:2022 menekankan bahwa akses terhadap informasi harus dibatasi berdasarkan prinsip *least privilege*, yaitu hanya diberikan kepada pihak yang benar-benar membutuhkan. Dalam konteks ini, berbagi data secara publik tanpa kontrol waktu dan identitas penerima berpotensi melanggar prinsip tersebut.

Selaras dengan itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mewajibkan pengendali data untuk memastikan bahwa distribusi data pribadi hanya dilakukan kepada pihak yang berwenang dan memiliki dasar hukum yang sah. Demikian, temuan ini menunjukkan perlunya kebijakan tambahan seperti pembatasan sharing publik, penerapan masa berlaku tautan (*link expiration*), penggunaan domain tepercaya (*trusted domains*), serta evaluasi berkala terhadap aktivitas berbagi eksternal guna menekan risiko kebocoran informasi.

p-ISSN: 2775-4227
e-ISSN: 2775-4219



Gambar 12. File Added by Tipe

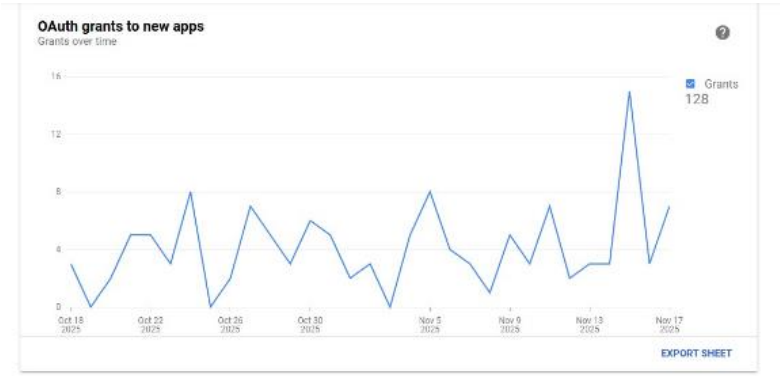
Grafik *files added by type* memberikan gambaran mengenai jenis berkas yang paling sering diunggah ke sistem cloud selama periode observasi. Dominasi dokumen teks, spreadsheet, presentasi, dan media pembelajaran menunjukkan tingginya aktivitas akademik digital yang melibatkan pembuatan dan pertukaran materi secara intensif.

Keberagaman jenis file yang tersimpan mencerminkan kompleksitas data yang dikelola oleh institusi pendidikan, mulai dari materi pembelajaran hingga dokumen administratif yang berpotensi mengandung informasi pribadi. Kondisi ini menegaskan bahwa tidak seluruh berkas memiliki tingkat sensitivitas yang sama, sehingga pendekatan perlindungan data tidak dapat diterapkan secara seragam.

Tanpa mekanisme klasifikasi informasi, dokumen yang bersifat sensitif berisiko diperlakukan sama seperti file umum, termasuk dalam pengaturan berbagi dan akses pengguna. Hal ini dapat menyebabkan data penting ikut tersebar melalui aktivitas kolaborasi sehari-hari tanpa disadari oleh pemilik dokumen.

ISO/IEC 27001:2022 Clause A.5.12 menekankan pentingnya klasifikasi informasi untuk memastikan bahwa setiap jenis data memperoleh tingkat perlindungan yang sesuai. Dalam konteks pendidikan, klasifikasi ini menjadi krusial karena sistem cloud menyimpan data akademik, identitas siswa, serta dokumen institusional yang memiliki implikasi hukum apabila terjadi kebocoran.

Demikian, temuan ini menunjukkan perlunya penerapan kebijakan klasifikasi data berbasis tipe file dan konteks penggunaan, yang dapat diintegrasikan dengan kontrol Data Loss Prevention (DLP) agar perlindungan terhadap dokumen sensitif dapat dilakukan secara lebih terarah.



Gambar 13. OAuth Grants to New Apps

Grafik *OAuth grants to new apps* menunjukkan adanya aktivitas pemberian izin akses terhadap aplikasi pihak ketiga secara berkala. Setiap aplikasi yang memperoleh token OAuth memiliki kemampuan untuk mengakses sebagian data pengguna sesuai cakupan izin yang disetujui, baik pada layanan penyimpanan maupun komunikasi digital.

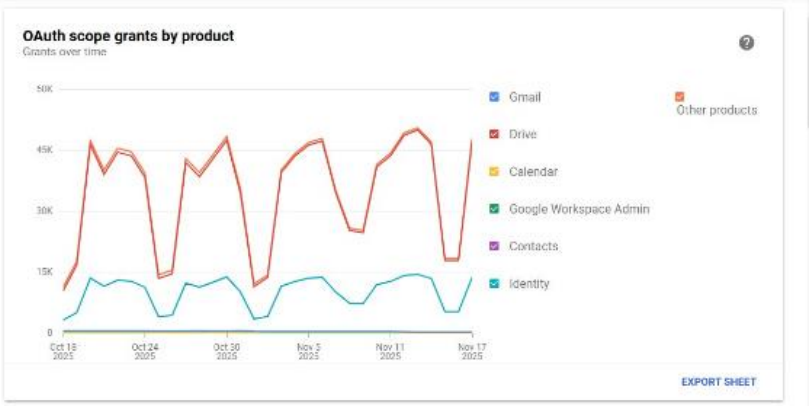
Integrasi aplikasi pihak ketiga memberikan manfaat dari sisi produktivitas dan efisiensi kerja, namun juga memperkenalkan risiko keamanan baru yang berada di luar kendali langsung penyedia layanan utama. Aplikasi eksternal dengan konfigurasi keamanan yang lemah dapat menjadi jalur masuk ancaman meskipun sistem inti Google Workspace telah terlindungi dengan baik.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Pertambahan jumlah aplikasi tanpa proses verifikasi administratif berpotensi menyebabkan akumulasi izin akses yang tidak lagi relevan dengan kebutuhan operasional. Kondisi ini dapat mengakibatkan terjadinya *privilege creep*, yaitu situasi di mana akun pengguna memiliki akses yang lebih luas daripada yang seharusnya.

CIS Benchmark dan ISO/IEC 27001 merekomendasikan agar integrasi pihak ketiga dikelola melalui kebijakan persetujuan terpusat, pembatasan cakupan akses, serta peninjauan izin secara berkala. Dalam konteks perlindungan data pribadi, akses aplikasi eksternal yang tidak dikendalikan secara ketat dapat meningkatkan potensi pelanggaran terhadap prinsip keamanan dan akuntabilitas.

Demikian, hasil observasi ini menunjukkan perlunya penerapan kebijakan pengelolaan OAuth yang lebih ketat, seperti penggunaan *application allowlist*, pembatasan scope berbasis kebutuhan, serta audit berkala terhadap aplikasi yang terhubung guna meminimalkan risiko paparan data melalui pihak ketiga.



Gambar 14. OAuth Scope Grants by Product

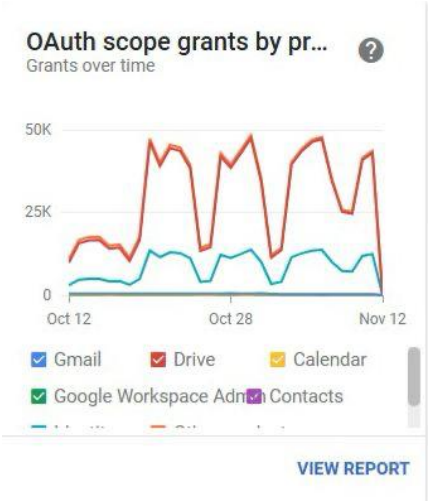
Grafik OAuth scope grants by product memperlihatkan bahwa cakupan akses terbesar berada pada layanan Gmail dan Google Drive. Hal ini menunjukkan bahwa sebagian besar aplikasi pihak ketiga memiliki akses terhadap komunikasi dan penyimpanan data pengguna. Akses berskala besar tersebut meningkatkan potensi paparan data apabila terjadi penyalahgunaan token atau kompromi aplikasi eksternal. CIS Benchmark dan ISO/IEC 27001 merekomendasikan penerapan prinsip least privilege serta peninjauan berkala terhadap izin aplikasi untuk meminimalkan risiko keamanan.

Gambar 15. OAuth grant activity

Bagian ini menunjukkan adanya **aktivitas pemberian izin aplikasi pihak ketiga** terhadap akun dalam domain. Bitly tercatat memperoleh **2 token OAuth**, sementara aplikasi lain seperti Behance, Agnes, atau BypassGPT.AI memperoleh **1 token**. Aktivitas ini memperlihatkan keterhubungan tinggi dengan aplikasi eksternal yang berpotensi menambah risiko apabila izin akses tidak dikendalikan dengan ketat. Setiap aplikasi dengan token OAuth memiliki kemampuan mengakses sebagian data pengguna sehingga pengawasan admin sangat diperlukan.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Setiap permintaan OAuth memiliki cakupan akses tertentu yang mencerminkan tingkat kedalaman aplikasi terhadap data pengguna. Data ini membantu memahami beban integrasi eksternal terhadap infrastruktur sekolah serta risiko yang muncul dari akses yang luas terhadap data penyimpanan, email, maupun kontak. Jumlah permintaan yang tinggi menunjukkan perlunya kebijakan akses yang lebih terukur.

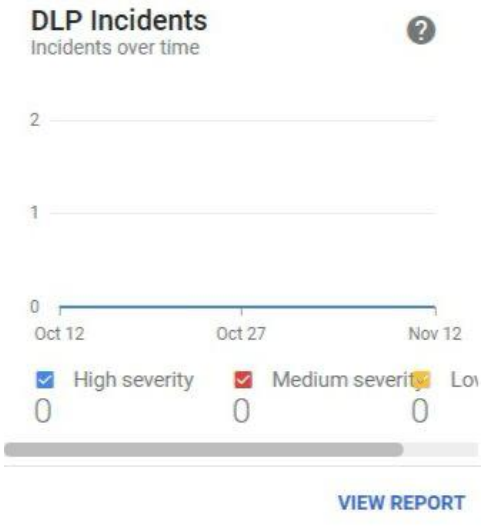


Gambar 16. OAuth scope grants

Grafik menunjukkan volume grant OAuth yang sangat tinggi pada **Drive** dan **Gmail**, mencapai **lebih dari 40.000 permintaan** pada beberapa titik. Ini menandakan tingginya integrasi antar aplikasi yang memerlukan akses ke penyimpanan cloud dan komunikasi email. Scope OAuth yang besar menunjukkan bahwa banyak proses internal maupun eksternal bergantung pada akses otomatis, sehingga kebijakan least-privilege dan peninjauan berkala harus diterapkan agar akses tetap aman.

Akses aplikasi pihak ketiga melalui mekanisme OAuth berpotensi meningkatkan risiko keamanan apabila tidak diawasi secara ketat, sebagaimana dijelaskan dalam penelitian mengenai manajemen risiko pihak ketiga pada platform kolaborasi berbasis cloud [15].

Kebijakan Data Loss Prevention (DLP) dirancang untuk mencegah penyebaran data sensitif secara tidak sengaja maupun disengaja. nformasi ini memberikan indikasi awal tentang kepatuhan pengguna terhadap aturan internal serta keefektifan konfigurasi DLP yang diterapkan. Ketiadaan insiden menunjukkan stabilitas kontrol, tetapi juga perlu ditinjau apakah aturan DLP sudah mencakup seluruh jenis data penting.



Gambar 17. DLP Incidents

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Data memperlihatkan **tidak ada insiden DLP** sepanjang periode observasi. Ini menunjukkan bahwa aturan perlindungan data telah berjalan dengan baik dan tidak ada pelanggaran yang terdeteksi. Ketiadaan insiden dapat menjadi indikator bahwa kebijakan DLP dipatuhi pengguna, atau justru menandakan bahwa aturan DLP perlu diperluas agar lebih sensitif dalam mendeteksi pola pelanggaran yang mungkin tidak terjangkau aturan saat ini.

Table 1. Ringkasan Temuan Log Keamanan

Area	Indikator	Hasil Observasi	Interpretasi Keamanan
Autentikasi	Total login	±2.300 aktivitas	Penggunaan sistem tinggi
Autentikasi	Login gagal	178 percobaan	Risiko rendah namun perlu pemantauan
Autentikasi	Login mencurigakan	14 aktivitas	Deteksi anomali berjalan
Email	Total email	>30.000 pesan	Email sebagai vektor utama
Email	Spam	±3.200 pesan	Filter berjalan efektif
Email	Phishing	Sebagian lolos inbox	Risiko rekayasa sosial
Enkripsi	TLS	Mayoritas terenkripsi	Kerahasiaan terjaga
File sharing	External sharing	Tinggi	Risiko kebocoran data
DLP	Insiden	Tidak ditemukan	Perlu validasi aturan
OAuth	Aplikasi pihak ketiga	85 aplikasi	Risiko akses tidak langsung

Untuk menilai kesesuaian temuan penelitian terhadap standar dan regulasi yang berlaku, hasil observasi log keamanan kemudian dipetakan ke dalam kerangka CIS Google Workspace Benchmark, ISO/IEC 27001:2022, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pemetaan ini bertujuan untuk mengidentifikasi tingkat kesesuaian kontrol keamanan yang telah diterapkan sekaligus menyoroti area yang masih memerlukan penguatan.

Table 2. Pemetaan Temuan Terhadap Standar CIS, ISO 27001, dan UU PDP

Temuan	CIS Benchmark	ISO/IEC 27001:2022	UU PDP No. 27/2022	Status
Login gagal terpantau	Control 6.3	A.5.15 Access Control	Pasal 40	Sesuai
MFA belum menyeluruh	Control 6.4	A.5.17 Authentication	Pasal 39	Perlu penguatan
Email terenkripsi TLS	Control 9.1	A.8.24 Transmission	Pasal 35	Sesuai
Phishing lolos inbox	Control 9.2	A.8.7 Malware	Pasal 40	Perlu peningkatan
External sharing tinggi	Control 11.1	A.5.12 Information Classification	Pasal 20	Risiko sedang
OAuth scope luas	Control 13.2	A.5.16 Identity Management	Pasal 39	Risiko tinggi

Hasil pemetaan menunjukkan bahwa sebagian kontrol keamanan telah selaras dengan standar yang direkomendasikan, khususnya pada aspek autentikasi dasar dan enkripsi komunikasi. Namun demikian, masih terdapat beberapa area dengan tingkat risiko menengah hingga tinggi, terutama pada pengelolaan berbagi eksternal dan integrasi aplikasi pihak ketiga, yang memerlukan perhatian lebih lanjut dalam kebijakan keamanan institusi. log keamanan Google Workspace for Education Plus pada periode 12 Oktober sampai 12 November 2025 menunjukkan bahwa mekanisme pengamanan cloud sekolah internasional berada pada kondisi stabil. Sistem mencatat 178 login gagal dan 14 aktivitas login mencurigakan yang berhasil dihentikan. Data ini memperlihatkan bahwa autentikasi dan pemantauan akses bekerja dengan baik dalam mencegah masuknya kredensial tidak sah. Penerapan autentikasi dua langkah sudah digunakan melalui IDV via phone dan offline OTP meski cakupannya belum penuh.

Volume pesan email sangat tinggi dengan lebih dari 30.000 pesan masuk. Sistem mendeteksi 3.200 pesan sebagai spam dan 38 pesan sebagai phishing. Deteksi terhadap 10 lampiran mencurigakan memperlihatkan bahwa pemindaian keamanan email berfungsi secara konsisten. Tidak tercatat pelanggaran Data Loss Prevention selama periode observasi yang berarti kebijakan pencegahan kebocoran data berjalan efektif. Proses enkripsi tercatat sangat kuat karena 33.000 pesan dikirim melalui TLS dan hanya sebagian kecil pesan yang tidak terenkripsi.

Risiko bernilai tinggi muncul dari aktivitas berbagi file eksternal dan akses aplikasi pihak ketiga. Terdapat 13.000 file yang dibagikan ke luar domain dan 24.000 total akses yang menunjukkan aktivitas sharing cukup

p-ISSN: 2775-4227
e-ISSN: 2775-4219

intens. Data OAuth mencatat 85 aplikasi yang memperoleh izin akses sehingga potensi paparan data semakin besar tanpa pengawasan kebijakan admin yang ketat.

Pearson menegaskan bahwa klasifikasi data dan pengelompokan dokumen berdasarkan tingkat sensitivitas merupakan fondasi utama dalam tata kelola keamanan data berbasis cloud di lingkungan Pendidikan [16].

Gambaran umum menunjukkan bahwa Google Workspace memberikan perlindungan kuat terhadap ancaman berbasis email, autentikasi, dan kebocoran data. Area peningkatan terletak pada perluasan autentikasi ganda, pengawasan identitas, dan kontrol akses eksternal agar selaras dengan standar CIS Controls, ISO/IEC 27001, serta prinsip perlindungan data UU PDP.

Implementasi platform kolaborasi berbasis cloud memberikan manfaat signifikan dalam mendukung fleksibilitas pembelajaran dan efisiensi kerja. Namun, hasil observasi menunjukkan bahwa peningkatan aktivitas kolaborasi secara langsung berdampak pada meningkatnya risiko distribusi data yang tidak terkontrol.

Paradoks utama dalam lingkungan cloud terletak pada kebutuhan untuk membuka akses demi kolaborasi, sekaligus menjaga pembatasan demi keamanan. Tanpa tata kelola yang jelas, praktik berbagi dapat berkembang menjadi *over-sharing*, yaitu kondisi ketika data dibagikan melebihi kebutuhan aktual pengguna.

Risiko ini menjadi semakin kompleks dalam lingkungan pendidikan internasional, di mana data siswa dapat melibatkan aspek lintas yurisdiksi dan regulasi perlindungan data yang berbeda. Distribusi data tanpa kontrol yang memadai berpotensi menimbulkan implikasi hukum, reputasi, dan kepercayaan publik terhadap institusi pendidikan.

Oleh karena itu, pengelolaan keamanan cloud perlu dilengkapi dengan kerangka *cloud data governance* yang mencakup klasifikasi informasi, kebijakan akses berbasis peran, serta mekanisme audit berkelanjutan. Pendekatan ini memungkinkan organisasi untuk menyeimbangkan kebutuhan kolaborasi dengan kewajiban perlindungan data.

Temuan penelitian ini menegaskan bahwa keamanan cloud tidak dapat dipisahkan dari kebijakan organisasi dan tata kelola data. Keberhasilan pengamanan tidak hanya ditentukan oleh fitur teknologi, tetapi juga oleh konsistensi implementasi kebijakan serta pengawasan administratif yang berkelanjutan.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan dalam interpretasi hasil. Pertama, periode observasi dilakukan dalam rentang waktu satu bulan sehingga belum sepenuhnya merepresentasikan pola keamanan jangka panjang.

Kedua, objek penelitian terbatas pada satu institusi pendidikan, sehingga hasil yang diperoleh tidak dapat digeneralisasi secara langsung ke seluruh lingkungan pendidikan dengan karakteristik berbeda.

Ketiga, penelitian ini berfokus pada analisis log keamanan tanpa melakukan pengujian aktif seperti *penetration testing* atau simulasi serangan, sehingga temuan yang diperoleh merefleksikan kondisi operasional, bukan tingkat ketahanan sistem terhadap eksploitasi teknis.

Keterbatasan tersebut membuka peluang bagi penelitian selanjutnya untuk memperluas cakupan waktu, melibatkan lebih banyak institusi, serta mengombinasikan analisis log dengan metode evaluasi keamanan aktif guna memperoleh gambaran risiko yang lebih komprehensif.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa sistem keamanan data berbasis cloud pada Google Workspace for Education Plus di sekolah internasional telah memberikan perlindungan yang kuat terhadap sebagian besar ancaman digital. Hasil observasi log keamanan selama periode 12 Oktober sampai 12 November 2025 memperlihatkan bahwa mekanisme autentikasi, enkripsi data, serta proteksi terhadap spam dan phishing berjalan efektif. Sistem mencatat 178 login gagal dan 14 percobaan login mencurigakan yang berhasil diblokir, menandakan bahwa kontrol identitas dan akses berfungsi dengan baik. Penggunaan autentikasi dua langkah telah diterapkan meski cakupannya belum penuh sehingga penguatan kebijakan autentikasi tetap diperlukan.

Pemrosesan email berlangsung dalam volume besar dengan lebih dari 30.000 pesan masuk. Sistem mampu menyaring spam dan phishing secara konsisten serta mendeteksi 10 lampiran mencurigakan tanpa menemukan file berbahaya. Tidak adanya insiden Data Loss Prevention menunjukkan bahwa perlindungan terhadap data sensitif berjalan sesuai konfigurasi. Enkripsi pesan berada pada tingkat sangat tinggi dengan 33.000 pesan melalui TLS dan hanya sebagian kecil pesan tidak terenkripsi.

Risiko signifikan muncul dari aktivitas berbagi file eksternal serta penggunaan aplikasi pihak ketiga yang memperoleh akses OAuth. Total 13.000 file dibagikan ke luar domain dan 85 aplikasi memperoleh izin akses sehingga meningkatkan potensi paparan data. Kondisi ini menunjukkan perlunya evaluasi ulang terhadap kebijakan akses eksternal agar tidak melewati batas keamanan yang seharusnya.

Berdasarkan hasil analisis log keamanan dan pembahasan yang telah dilakukan, penelitian ini menghasilkan sejumlah rekomendasi penguatan keamanan yang dapat diterapkan untuk meningkatkan perlindungan data dan pengelolaan risiko pada lingkungan Google Workspace for Education Plus.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Table 3. Rekomendasi Penguatan Keamanan Sistem

Area	Temuan Utama	Rekomendasi	Prioritas
Autentikasi	Login gagal & suspicious login	Wajibkan MFA seluruh pengguna	Tinggi
Email	Phishing lolos inbox	Security awareness & phishing simulation	Tinggi
File sharing	External sharing publik	Batasi "anyone with link"	Tinggi
Data sensitif	Tidak ada insiden DLP	Validasi dan perluasan aturan DLP	Sedang
OAuth	Banyak aplikasi pihak ketiga	Terapkan allowlist & audit berkala	Tinggi

Rekomendasi yang disusun diharapkan dapat menjadi acuan awal bagi institusi pendidikan dalam memperkuat kebijakan keamanan informasi, khususnya pada aspek autentikasi, komunikasi email, kolaborasi data, dan pengelolaan integrasi pihak ketiga. Implementasi rekomendasi ini perlu disesuaikan dengan kebijakan internal dan tingkat risiko masing-masing institusi.

Secara keseluruhan, sistem keamanan Google Workspace telah memenuhi sebagian besar prinsip kerahasiaan, integritas, dan ketersediaan data yang tertuang dalam CIS Benchmark dan ISO/IEC 27001:2022. Peningkatan diperlukan pada aspek manajemen identitas, perluasan autentikasi ganda, dan pengawasan integrasi aplikasi pihak ketiga agar kepatuhan terhadap UU Pelindungan Data Pribadi dapat terjaga secara menyeluruh.

DAFTAR PUSTAKA

[1] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Understanding Cyber Threats Against the Universities, Colleges, and Schools," *Elsevier*, pp. 1–27, Jul. 2023, doi: 10.3390/computers14020049.

[2] I. A. Loebis, M. Mustofa, S. Arifin, M. Angglena, and Y. Salim, "The Role of Cloud Computing Technology in Supporting Educational Accessibility and Scalability," *Journal International of Lingua and Technology*, vol. 3, no. 2, pp. 469–483, Aug. 2024, doi: 10.55849/jiltech.v3i2.682.

[3] I. Sopwandin and A. Junaidi, "USING GOOGLE WORKSPACE FOR EDUCATION AS A FOUNDATION FOR DATA GOVERNANCE AND STUDENT SERVICES IN HIGHER EDUCATION," *Jurnal Kependidikan Islam*, vol. 14, no. 02, 2024, doi: 10.24042/alidarah.v14i2.23893.

[4] M. Sheikh, A. Bajpai, R. Raheja, and M. Tiwari, "Cloud Data Security: Addressing Risks and Advanced Mitigation Strategies for the Modern Era," *International Research Journal of Education and Technology Peer Reviewed Journal*, vol. 07, no. 02, pp. 84–92, 2025.

[5] H. El-Sofany, S. A. El-Seoud, O. H. Karam, B. Bouallegue, and A. M. Ahmed, "A proposed secure framework for protecting cloud-based educational systems from hacking," *Egyptian Informatics Journal*, vol. 27, pp. 1–10, Sep. 2024, doi: 10.1016/j.eij.2024.100505.

[6] A. Alakuu and D. K. Dake, "Cloud Computing in Education: A review of Architecture, Applications, and Integration Challenges," *Int. J. Comput. Appl.*, vol. 186, no. 66, pp. 49–65, 2025.

[7] R. R. Turluev, D. A. Abdullayev, and S. A. Zyryanova, "Cloud Computing and Big Data Analytics in Education," *SHS Web of Conferences*, vol. 172, pp. 1–4, 2023, doi: 10.1051/shsconf/202317201015.

[8] M. A. Ayanwale, R. R. Molefi, and S. Liapeng, "Unlocking educational frontiers: Exploring higher educators' adoption of google workspace technology tools for teaching and assessment in Lesotho dynamic landscape," *Heliyon*, vol. 10, no. 9, pp. 1–19, May 2024, doi: 10.1016/j.heliyon.2024.e30049.

[9] X. Dong and Y. Xie, "Research on cloud computing network security mechanism and optimization in university education management informatization based on OpenFlow," *Systems and Soft Computing*, vol. 7, pp. 1–10, Dec. 2025, doi: 10.1016/j.sasc.2025.200225.

[10] National Institute of Standards and Technology, "Digital Identity Guidelines," 2023.

[11] "ISO/IEC 27001:2022 Information Security Management Systems," 2022, *Geneva, Switzerland*.

[12] Google Cloud, "Google Workspace Security Whitepaper," 2024.

[13] V. Malele, "Cybersecurity Cloud-Based Online Learning: A Literature Review Approach," *Journal of Information Systems and Informatics*, vol. 5, no. 4, pp. 1623–1632, Dec. 2023, doi: 10.51519/journalisi.v5i4.583.

[14] European Union Agency for Cybersecurity, "Cybersecurity Challenges in the Education Sector," 2023, *Athens, Greece*.

[15] A. Behl and S. Behl, "Managing Third-Party Risk in Cloud-Based Collaboration Platforms," *Comput. Secur.*, vol. 131, 2025.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[16] S. Pearson, "Data Governance and Cloud Security in Educational Institutions," *Journal of Cloud Computing*, vol. 12, no. 1, pp. 1–14, 2024.