Jurnal Penelitian Ilmu Pendidikan Indonesia
Volume 4, Nomor 4, Tahun 2025, Halaman 2284 -2292
https://jpion.org/index.php/jpi

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

Keamanan Layanan Cloud dalam Pendidikan terhadap Ancaman Malware dan DDoS (Studi Literatur)

Eliya Rahmawati[1)], Dafina Nur Faiza[2)] , Miranda Dwi Febrianti[3)], Nasyiwa Ega Palupi[4)], Ryan Prasetyo[5)], Mohammad Wildan Habibi[6)], I Gusti Lanang Eka Putra Prisman[7)]

[1,2,3,4,5,6,7)]Program Studi S1 Pendidikan Teknologi Informasi, Fakultas Teknik, Universitas Negeri Surabaya

*Eliya Rahmawati
Email : eliya.22012@mhs.unesa.ac.id
dafina.22035@mhs.unesa.ac.id
miranda.22042@mhs.unesa.ac.id
nasyiwa.22055@mhs.unesa.ac.id
ryan.22094@mhs.unesa.ac.id
mohammadhabibi@unesa.ac.id
lanangprismana@unesa.ac.id

Abstrak

Layanan cloud telah menjadi pondasi utama dalam dunia pendidikan untuk memberikan fleksibilitas dan efektivitas biaya yang sangat dibutuhkan, tetapi kenyamanan ini perlu dibayar dengan dihadapkan pada peningkatan risiko ancaman siber yang serius. Dua ancaman yang paling sering terlihat adalah malware yang dapat menyusup dan menghancurkan atau mencuri data sensitif dan serangan DDoS, yang dapat melumpuhkan seluruh sistem dengan membanjiri server dan membuatnya mengalami waktu henti yang mengganggu proses pengajaran. Karena itu, penting bagi kita untuk menggali lebih dalam ancaman malware dan DDoS dalam konteks cloud pendidikan dan menemukan serta memetakan solusi pertahanan terbaik yang dapat diterapkan. Studi literatur mengonfirmasi bahwa kedua jenis serangan ini merupakan ancaman signifikan terhadap integritas data dan aksesibilitas sistem. Oleh karena itu, institusi pendidikan didorong untuk segera memperkuat perlindungan mereka dengan menerapkan enkripsi yang ketat pada data, mengoptimalkan Manajemen Identitas dan Akses, dan memanfaatkan SIEM untuk memastikan deteksi anomali dan respons cepat terhadap serangan siber. Studi ini juga menekankan pentingnya evaluasi dan pembaruan berkala terhadap sistem perlindungan untuk menghadapi ancaman yang terus berkembang.

***Kata Kunci**: Keamanan cloud, ancaman malware, serangan DDoS, mitigasi, pendidikan.*

Abstract

Cloud services have become the main foundation in the world of education to provide flexibility and cost-effectiveness that is very much needed, but this comfort needs to be paid for by being faced with an increased risk of serious cyber threats. The two spectres most frequently seen are malware-which can infiltrate and destroy or steal sensitive data-and DDoS attacks, which can completely paralyze the whole system by flooding servers and making it experience downtime that disturbs the teaching process. Because of this, it is important that we dig deeper into the malware and DDoS threats in the context of education clouds and find and map the best defense solutions that can be applied. Literature study confirms that these two kinds of attacks are significant threats against data integrity and system accessibility. Therefore, educational institutions are encouraged to immediately strengthen their protection by implementing strict encryption on data, optimizing Identity and Access Management, and utilizing SIEM so as to assure anomaly detection and quick response to cyber-attacks. The study also emphasizes the importance of regular evaluation and updating of protection systems to address evolving threats.

***Keywords:** Cloud security, malware threats, DDoS attacks, mitigation, education.*

PENDAHULUAN

Dengan meningkatnya teknologi informasi, banyak sektor, termasuk pendidikan mulai menggunakan layanan *cloud* untuk memfasilitasi berbagai fungsi akademik dan administrasi (Abidah et al., 2020). Layanan ini memberikan banyak manfaat, seperti skalabilitas, fleksibilitas, dan peningkatan kemampuan kolaboratif (Maimun, 2023). Meskipun demikian, ketergantungan

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

pada layanan *cloud*, rentan menimbulkan risiko keamanan sistem data. Oleh karena itu, perlu diperhatikan lebih akan adanya ancaman malware dan serangan *DDoS (Distributed Denial of Service)* (Ali et al., 2024).

Ancaman *malware* dalam ekosistem *cloud* pendidikan sangatlah berbahaya, sebab *malware* mampu merusak atau mencuri data sensitif yang tersimpan (Ahmadi, 2024; Dawood et al., 2023). Jenis malware seperti *ransomware*, *trojan*, dan virus berpotensi besar merusak integritas sistem dan mengganggu seluruh proses pendidikan. Institusi pendidikan sering kali menjadi target empuk karena mereka menyimpan informasi berharga dan sensitif seperti catatan akademis dan data keuangan, dan sistem keamanan *cloud* mereka sebagian besar waktu dikonfigurasi dengan buruk untuk mengatasi ancaman yang terus berkembang. Akibatnya, menjaga layanan *cloud* di bidang pendidikan, wajib untuk menerapkan langkah-langkah keamanan yang lebih ketat, pemantauan aktivitas anomali yang mendalam dan berkelanjutan. Kesenjangan dalam infrastruktur *cloud* juga dapat mengakibatkan pengelolaan *cloud* yang buruk, yang merupakan titik masuk utama untuk malware, oleh karena itu ini adalah risiko yang memerlukan investasi berkelanjutan dalam sistem pertahanan malware (Mykhaylova et al, 2024). Peningkatan kesadaran siber dari pengguna sistem, yang merupakan staf universitas dan mahasiswa, juga sangat penting karena faktor manusia sering kali merupakan tautan terlemah yang menjadi target *malware* melalui teknik *phishing* dan rekayasa sosial.

Sebagai alternatif, serangan *DDoS* adalah taktik yang digunakan oleh penjahat siber (peretas) untuk melumpuhkan suatu sistem dengan membanjirnya dengan permintaan yang berlebihan ke server yang pada akhirnya mengarahkannya ke total server down (Zidane, 2022). Dengan pembelajaran jarak jauh *(Distant Learning)* yang saat ini luas diterapkan, serangan *DDoS* dalam lingkungan pembelajaran jarak jauh dapat melumpuhkan proses akademik, mengganggu ribuan siswa dan staf universitas untuk mengakses materi, yang mengakibatkan kerugian finansial dan reputasi yang signifikan. Serangan semacam itu tidak mengganggu ketersediaan layanan *(availability)*, tetapi juga menguras sumber daya komputasi dan bandwidth. Oleh karena itu, upaya mitigasi terhadap serangan *DDoS*, melalui penggunaan solusi teknis yang tepat, seperti layanan anti-DDoS berbasis cloud yang dapat menyaring traffic berbahaya sebelum mencapai server utama untuk menjaga kelangsungan layanan *cloud* di institusi pendidikan (Marlina, 2025).

Penelitian terdahulu telah membahas berbagai aspek keamanan siber yang relevan, seperti risiko keamanan sistem *Internet of Things (IoT)* berbasis komputasi awan dalam e-commerce (Fauzi et al., n.d.), pentingnya ketahanan bisnis digital melawan kejahatan siber canggih (Puspita Maharani et al., 2025), analisis risiko kebocoran data di *cloud* (Risky Kurniawan et al., n.d.) hingga penyelidikan ancaman siber pada sistem *e-commerce IoT* (Alfian Saputra et al., 2025). Selain itu, terdapat studi yang menganalisis ancaman *cloud*, termasuk *DDoS* dan kebocoran data, serta mengusulkan strategi mitigasi seperti enkripsi dan manajemen identitas (Marlina, 2025).

Berdasarkan latar belakang dan telaah literatur ini, penulis memfokuskan pembahasan pada keamanan layanan *cloud* dalam pendidikan terhadap ancaman *malware* dan *DDoS*. Tujuan dari studi literatur ini adalah menggambarkan bentuk spesifik ancaman malware dan *DDoS* dalam pendidikan hingga merumuskan solusi konkret untuk mengatasinya. Artikel ini diharapkan dapat memberikan kontribusi literatur dan manfaat yang berarti bagi penelitian berikutnya, khususnya dalam membantu pengambil kebijakan di sektor pendidikan mengadopsi postur keamanan yang lebih tangguh dan menyadari bahwa pencegahan adalah investasi yang jauh lebih murah daripada pemulihan pasca-serangan.

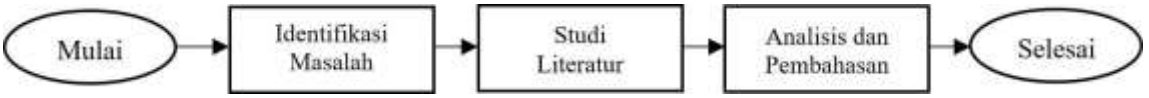
METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur untuk mengeksplorasi dan menilai tantangan serta solusi terkait keamanan layanan cloud dalam bidang pendidikan, dengan fokus utama pada ancaman seperti *malware* dan serangan *DDoS*. Artikel-artikel yang digunakan dalam penelitian ini dipilih dari Google Scholar dan SciSpace berdasarkan relevansi topik yang dibahas,

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

serta kualitas dan kedalaman analisis yang disajikan. Variabel yang dianalisis dalam literatur mencakup berbagai tantangan yang dihadapi oleh layanan *cloud* dalam pendidikan, seperti kerentanannya terhadap malware, serangan *DDoS*, dan ancaman lainnya. Solusi yang diusulkan untuk mengatasi tantangan tersebut, seperti penggunaan enkripsi, pemantauan berbasis *AI*, dan pendekatan deteksi dini, juga menjadi bagian penting dalam analisis.

Proses analisis dilakukan dengan menggunakan metode analisis konten untuk menemukan pola utama dalam studi literatur yang ada. Analisis konten ini bertujuan untuk mengidentifikasi tema-tema yang sering muncul serta untuk mengelompokkan tantangan dan solusi yang ditemukan dalam literatur yang relevan. Melalui pendekatan ini, peneliti dapat menyintesis dan merangkum temuan-temuan utama yang ada dalam literatur, sehingga memberikan gambaran menyeluruh mengenai masalah keamanan layanan *cloud* dalam pendidikan. Pendekatan ini merujuk pada pedoman yang diusulkan oleh Snyder, yang menyatakan bahwa studi literatur yang efektif dapat menyintesis temuan-temuan yang relevan untuk mengidentifikasi kesenjangan pengetahuan dan mengarah pada pengembangan teori lebih lanjut (Snyder, 2019). Selain itu, penelitian ini juga mengikuti pendekatan yang diusulkan oleh Kraus dkk., yang menekankan pentingnya analisis konten untuk mengidentifikasi pola dan tren dalam literatur yang ada, serta menemukan area yang belum banyak dieksplorasi dalam topik ini (Kraus dkk., 2022). Analisis ini juga mengacu pada metodologi yang diuraikan oleh Hill dkk., dalam menilai hubungan sebab-akibat dalam literatur (Hill dkk., 2021). Alur penelitian secara rinci dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian
Sumber: Rumetna, M. S. (2018)

HASIL DAN PEMBAHASAN

Tabel 1. Studi Literatur

No.	Judul	Peneliti	Tujuan	Hasil
1.	Analisis Keamanan Layanan E-Learning Terhadap Serangan Dos Dan Implementasi Mitigasi Pada Universitas Budi Luhur	Joko Christian Chandra (2022)	Menganalisis keamanan sistem *e-learning* di Universitas Budi Luhur, terutama terhadap serangan *DoS* dan *DDoS*, serta mengembangkan mitigasi untuk meningkatkan ketahanan sistem.	Hasil penelitian menunjukkan bahwa setelah mitigasi konfigurasi ulang *Linux kernel* dan *Apache server*, sistem mampu mengatasi serangan *DoS* dan *DDoS*, meningkatkan ketahanan tiga kali lipat terhadap *serangan Application Layer* seperti *Slowloris* dan *HTTP Flood*.
2.	Implementasi Keamanan Anti Ddos Menggunkan Router Mikrotik Pada Layanan Cloud Storage Basis Local Di Sekolah Menengah Kejuruan	M. Ihsan et al. (2025)	Merancang sistem keamanan anti-*DDoS* untuk *cloud storage* lokal di SMK, menggunakan Router Mikrotik untuk perlindungan.	Dengan Filter *Rules* pada Mikrotik, serangan *DDoS* dapat ditekan, menjaga stabilitas server dan menghindari *downtime*. Artikel ini membahas serangan *DDoS* secara eksplisit dan memberikan solusi teknis untuk mitigasinya.

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

3.	Edukasi Trend Kejahatan Cyber pada SMA Negeri 2 Baubau	Mashendra et al. (2024)	Meningkatkan kesadaran siswa SMA Negeri 2 Baubau tentang ancaman kejahatan siber seperti *phishing*, virus, *malware*, dan serangan *DDoS*.	Meningkatnya kesadaran siswa tentang kejahatan siber, seperti *phishing*, *malware*, dan *DDoS* dengan perubahan perilaku seperti mengubah kata sandi rutin dan lebih berhati-hati dalam berbagi informasi pribadi *online*
4.	Audit Keamanan Jaringan Komputer Server dari Serangan DDoS Menggunakan Snort Intrusion Detection System	Iqbal et al. (2024)	Meningkatkan keamanan jaringan di SMKS YPPI Tualang dengan audit keamanan dan implementasi *Snort IDS* untuk mendeteksi dan mencegah serangan *DDoS*.	Implementasi *Snort* meningkatkan deteksi dini terhadap ancaman dan memperkuat keamanan jaringan, mengurangi dampak serangan *DDoS* pada operasional sekolah
5.	Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi	Madina, dan Fadhli. (2024)	Menguji ketahanan server website Prodi Pendidikan Teknologi Informasi terhadap serangan *DDoS* menggunakan *penetration testing* dengan *tools Slowloris* dan C2.	Serangan *DDoS* dapat menyebabkan website down. Rekomendasi untuk meningkatkan *socket*, memori, dan melakukan uji penetrasi rutin setiap bulan untuk mencegah serangan keamanan jaringan
6.	Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity	Syed Adnan Jawaid (2022)	Untuk mengeksplorasi ancaman keamanan siber di institusi pendidikan, khususnya yang muncul akibat penggunaan platform *cloud* dan *e-learning*.	Penelitian menemukan bahwa institusi pendidikan menjadi sasaran serangan siber, termasuk *DDoS*, *phishing*, dan *malware*. *Malware* mengancam integritas sistem dan dapat mengakses data sensitif. Rekomendasi: memperkuat kebijakan keamanan dan memperbarui sistem secara teratur.
7.	Understanding Cyber Threats Against Universities, Colleges, and Schools	Lallie et al. (2023)	Untuk menilai ancaman siber di universitas, perguruan tinggi, dan sekolah, dengan fokus pada ancaman dari dalam yang dilakukan oleh mahasiswa.	Ditemukan bahwa *ransomware* adalah serangan yang paling umum, dan peretasan untuk keuntungan pribadi adalah serangan internal yang paling sering. Ditekankan pentingnya respon yang disesuaikan untuk ancaman dari dalam
8.	Cyber Threats to the Private Academic Cloud	Lakhno et al. (2024)	Menganalisis ancaman siber yang mengarah pada cloud akademik pribadi di universitas dan mengusulkan metode mitigasi untuk mencegah ancamannya.	Mengusulkan "Threat Analyzer" untuk mendeteksi malware dan ancaman lainnya menggunakan algoritma prediktif. Fokus pada keamanan sistem virtualisasi dan hypervisor di PAC.
9.	Review on Cloud Security and Challenges on Higher Education	Khalid, Muhamad Irwan Ihfan & Zolkipli, Mohamad Fadli (2022)	Untuk mengkaji tantangan keamanan cloud yang dihadapi oleh lembaga pendidikan tinggi, serta masalah keamanan dan privasi data yang muncul terkait	Penelitian ini menemukan bahwa teknologi cloud menawarkan manfaat penghematan biaya, akses mudah, namun masalah keamanan seperti kebocoran/manipulasi data, serangan DDoS, akses tidak sah

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

			dengan penggunaan layanan cloud.	menghambat adopsi di sektor pendidikan.
10.	Cyber-Aware Threats and Management Strategies in Cloud Environments	Liubchenko, dan Volkov (2024)	Meninjau secara sistematis penelitian-terbaru mengenai keamanan komputasi awan (cloud computing), dengan fokus pada ancaman yang muncul serta strategi mitigasi yang digunakan untuk mengatasinya.	Menyoroti prevalensi malware, phishing, dan serangan DDoS. Merekomendasikan strategi seperti kebijakan kata sandi yang kuat, pembaruan perangkat lunak, dan pemantauan berkelanjutan untuk mengurangi ancaman.

Pada bagian ini, akan dibahas hal-hal terkait keamanan layanan *cloud* yang berfokus pada ancaman *malware* dan *DDoS (Distributed Denial of Service)* dalam lingkup Pendidikan. Melalui studi literatur yang mengacu pada sepuluh artikel terkait, kita dapat mengidentifikasi ancaman utama, strategi mitigasi, tantangan, serta solusi yang dapat dilakukan oleh institusi pendidikan dalam menjaga keamanan layanan *cloud* mereka.

1. Ancaman Malware pada Layanan Cloud Pendidikan

Seiring dengan meningkatnya jumlah institusi pendidikan yang beralih ke platform *cloud*, ancaman malware pada layanan *cloud* pendidikan juga semakin meningkat. Berbagai malware contohnya *ransomware*, *trojan*, dan *spyware* dapat masuk ke dalam system dengan berbagai jalur, seperti email phising dan perangkat yang tidak terjaga keamanannya. Penelitian yang dilakukan oleh Liubchenko dan Volkov (2024) menunjukkan bahwa terdapat banyak universitas menjadi sasaran utama ancaman *malware*, hal tersebut karena pihak kampus tidak memiliki sistem pertahanan yang sesuai untuk menyimpan data sensitif.

Meskipun ancaman *malware* terbukti nyata, berbagai penelitian mengugkapkan bahwa dengan menggunakan kebijakan keamanan yang tepat, ancaman dapat diminimalkan dampaknya. Beberapa cara yang dapat dilakukan untuk membantu pencegahan dari serangan *malware* yaitu melakukan patching perangkat lunak secara berkala, menggunakan antivirus terpusat, serta memantau jaringan secara *real-time*. Studi yang dilakukan oleh Ihsan et al. (2025) menjelaskan bahwa terdapat upaya untuk mengurangi ancaman *malware* pada layanan *cloud* pendidikan di Sekolah Menengah Kejuruan yaitu dengan menerapkan kebijakan pengamanan perangkat dan server. Sehubungan dengan hal ini, cara untuk melindungi data sensitif di sistem *cloud* Pendidikan adalah dengan pendekatan berbasis edukasi keamanan dan pengelolaan perangkat yang lebih ketat.

Tantangan terbesar terletak pada kesadaran pengguna, walaupun mitigasi berbasis perangkat keras dan perangkat lunak dapat membantu mencegah ancaman *malware*. Terdapat banyak serangan *malware* terjadi karena kurangnya pengetahuan pengguna dalam mengenali ancaman, misalnya *email phising* ataupun lampiran berbahaya. Dengan demikian, tidak hanya penerapan teknoogi canggih, pelatihan literasi digital kepada mahasiswa dan staf mengenai potensi ancaman *malware* penting dilaksanakan bagi institusi Pendidikan. Program ini tidak hanya akan membantu mendukung mereka dalam mengenali dan mencegah serangan, namun sekaligus meningkatkan kemampuan mereka untuk memastikan keamanan data pribadi dan institusional dari berbagai ancaman siber yang semakin canggih.

2. Ancaman DDoS pada Layanan Cloud Pendidikan

Terdapat permasalah serius yang dihadapi oleh layanan *cloud* pendidikan yaitu ancaman *DDoS (Distributed Denial of Service)*. Serangan *DDoS* digunakan untuk memenuhi server atau layanan dengan lalu lintas data yang berlebihan, sehingga layanan tersebut tidak dapat diakses oleh pengguna yang sah. Hal ini dapat terjadi pada beragam aplikasi pendidikan berbasis *cloud*,

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

sebagai contoh yakni sistem *e-learning*, portal pendaftaran ujian, dan sistem administrasi akademik. Penelitian yang dilakukan oleh Madina dan Fadhli (2024) mengungkapkan bahwa serangan *DDoS* berdampak pada kelancaran proses belajar mengajar, karena dapat mengakibatkan *down time* yang signifikan pada website pendidikan. Serangan ini dapat merusak reputasi institusi pendidikan dan juga mengganggu pengguna yang bergantung pada layanan berbasis *cloud* untuk operasional mereka.

Pada umumnya, ancaman *DDoS* melibatkan banyak perangkat terserang, yang secara bersamaan mengirimkan permintaan ke server target. Hal tersebut menyebabkan ketersediaan layanan terancam, dengan akibat website ataupun aplikasi pendidikan tidak dapat diakses selama periode serangan terjadi. Penelitian yang dilakukan oleh Chandra (2022), serangan *DDoS* pada Universitas Budi Luhur menyebabkan gangguan pada sistem e-learning mereka, sehingga mengakibatkan terhambatnya mahasiswa dalam mengakses materi dan menyelesaikan tugas. Dengan demikian, layanan pendidikan yang membutuhkan stabilitas dan ketersediaan tinggi, penting untuk memahami jenis serangan ini beserta dampaknya.

Untuk mengurangi risiko serangan *DDoS*, institusi pendidikan dapat menerapkan berbagai strategi, termasuk penggunaan *firewall*, *CDN (Content Delivery Network)*, dan *WAF (Web Application Firewall)*. Dalam penelitian yang dilakukan oleh Ihsan et al. (2025) menjelaskan bahwa penggunaan Mikrotik Router untuk *filtering rules* dapat mengurangi dampak serangan *DDoS*, bahkan pada serangan yang cukup besar. Selain itu, strategi mitigasi lainnya untuk mendistribusikan beban trafik serangan adalah dengan memanfaatkan *autoscaling* dan l*oad balancing*, serta apabila untuk menyebarkan trafik ke server yang lebih tersebar dan mengurangi beban pada satu titik dapat menggunakan *Anycast*. Meskipun solusi ini dapat meningkatkan ketahanan terhadap serangan *DDoS*, tantangan terbesar untuk mengimplementasikan solusi tersebut secara efektif tetap ada pada biaya dan infrastruktur yang dibutuhkan.

3. Strategi Mitigasi terhadap Ancaman pada Layanan Cloud Pendidikan

Pencegahan terhadap ancaman *malware* dan *DDoS* memerlukan pendekatan yang komprehensif dan multi-lapis. Berdasarkan penelitian yang dilakukan oleh Chandra (2022), penggunaan *Intrusion Detection System (IDS)* seperti *Snort*, merupakan salah satu langkah mitigasi yang paling efektif untuk mendeteksi potensi serangan lebih awal. *Snort* dapat mendeteksi trafik yang mencurigakan, sehingga dapat menjadi tanda bahwa adanya serangan, yaitu *DDoS* dan *malware*. Di sisi lain, penggunaan antivirus yang terpusat dan penerapan kebijakan patching di server pendidikan juga berperan penting dalam mengurangi risiko *malware* pada platform *cloud* pendidikan.

Selain hal tersebut, untuk mengurangi dampak serangan *DDoS* dapat dengan menggunakan *firewall* dan *rate-limiting* pada aplikasi web. Penelitian yang dilakukan oleh Madina dan Fadhli (2024) mengungkapkan bahwa serangan *Application Layer DDoS* yang lebih sulit dideteksi, dapat diatasi dengan optimasi server web seperti *Apache* dan *Nginx*. Pemanfaatan *Content Delivery Network (CDN)* juga menjadi alternatif yang efektif, karena *CDN* dapat menyaring sebagian besar trafik berbahaya sebelum mencapai server utama. Oleh karena itu, penggunaan mitigasi berbasis teknologi dan penguatan sistem sangat penting untuk melindungi layanan *cloud* pendidikan dari ancaman ataupun risiko yang dapat mengganggu proses belajar mengajar dan operasional.

Terlepas dari teknologi mitigasi, monitoring berkelanjutan dan audit keamanan penting juga untuk dilakukan secara rutin. *Implementasi Security Information and Event Management (SIEM)* dapat membantu mendeteksi dan merespons serangan lebih cepat. Penelitian oleh Liubchenko dan Volkov (2024) menunjukkan bahwa analisis *log real-time* sangat penting dalam mengidentifikasi ancaman secara dini, sehingga dapat mengurangi kerusakan yang ditimbulkan. Selain itu, penerapan *multi-factor authentication (MFA)* dan kebijakan *least-privilege access* akan mengurangi kemungkinan akses tidak sah yang disebabkan oleh kesalahan pengguna atau serangan *phishing*.

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

4. Tantangan dalam Menjaga Keamanan Layanan Cloud di Pendidikan

Keterbatasan sumber daya dan kesadaran keamanan di kalangan pengguna menjadi tantangan utama dalam menjaga keamanan layanan *cloud* di institusi pendidikan. Di negara berkembang, banyak institusi pendidikan yang tidak memiliki anggaran yang cukup untuk mengimplementasikan solusi keamanan yang komprehensif. Dalam penelitian yang dilakukan oleh Jawaid (2022) mengungkapkan bahwa banyak perguruan tinggi yang memiliki keterbatasan terkait kebijakan keamanan yang memadai dan tidak adanya tim IT yang terlatih untuk menangani ancaman siber yang semakin berkembang. Selain itu, peningkatan serangan siber yang lebih canggih, seperti serangan yang menggunakan teknik *phishing* dan *social engineering*, juga membuat perlindungan data dan sistem menjadi semakin kompleks.

Beberapa hambatan besar dalam menjaga integritas dan keamanan layanan *cloud* pendidikan yaitu dengan keterbatasan dana serta kesadaran keamanan yang rendah di kalangan mahasiswa dan staf. Berdasarkan penelitian yang dilakukan oleh Mashendra et al. (2024) di SMA Negeri 2 Baubau menunjukkan bahwa hal yang membuat para siswa rentan terhadap ancaman karena sebagian besar dari mereka tidak memahami ancaman *phishing* dan *malware*. Dengan adanya situasi tersebut, perlu diselenggarakan program edukasi yang terstruktur untuk meningkatkan pemahaman keamanan siber di kalangan mahasiswa dan staf. Edukasi ini akan membantu mereka mengenali tanda-tanda serangan dan menghindari tindakan yang dapat merusak sistem keamanan.

Selain itu, tantangan lainnya adalah pengelolaan risiko berbasis *cloud* yang memerlukan kolaborasi erat antara penyedia layanan *cloud* dan institusi pendidikan itu sendiri. Penelitian oleh Liubchenko dan Volkov (2024) menjelaskan bahwa pengelolaan keamanan fisik dan virtualisasi menjadi sangat krusial dalam *private academic cloud*. Terdapat penerapan solusi yang dapat dilakukan, seperti *cloud security posture management (CSPM)* mampu membantu institusi pendidikan mengidentifikasi dan mengurangi celah keamanan di platform *cloud* mereka.

5. Solusi untuk Meningkatkan Keamanan Layanan Cloud Pendidikan

Solusi yang paling efektif untuk meningkatkan keamanan layanan *cloud* pendidikan adalah penggunaan kebijakan keamanan berbasis teknologi dan pelatihan pengguna. Berdasarkan hasil penelitian yang ada, penggunaan *cloud security frameworks* seperti *CSPM* dapat membantu institusi pendidikan melindungi struktur keamanan *cloud* mereka tetap terjaga dengan baik. Selain itu, penting untuk memitigasi ancaman dari serangan eksternal maupun internal, misalnya dengan menerapkan MFA, enkripsi data, dan keamanan jaringan berbasis *Zero-Trust*.

Dalam institusi pendidikan juga penting untuk membangun kebijakan data *governance* yang jelas, termasuk pengelolaan akses data, retensi data, dan penghapusan aman. Penelitian oleh Ihsan et al. (2025) menungkapkan bahwa penerapan *filtering rules* pada perangkat keras seperti Mikrotik Router dapat mencegah serangan *DDoS* pada sistem *cloud* lokal, menjaga kestabilan dan aksesibilitas layanan *cloud* pendidikan. Dengan menerapkan solusi ini, sistem *cloud* pendidikan akan lebih kuat dan aman, mengurangi gangguan pada kegiatan akademik.

Kunci keberhasilan dalam mengoptimalkan keamanan layanan *cloud* pendidikan adalah kolaborasi antara teknologi, kebijakan, dan manusia. Pendidikan yang berkelanjutan mengenai pentingnya keamanan siber dan pelatihan untuk mahasiswa, dosen, dan staf IT adalah langkah awal untuk menciptakan ekosistem digital yang aman di lingkungan pendidikan. Dengan pemahaman yang dimiliki dapat meningkatkan kemampuan dalam mengidentifikasi dan menangani potensi ancaman keamanan dengan lebih efektif.

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

KESIMPULAN

Keamanan layanan *cloud* di sektor pendidikan menghadapi berbagai ancaman serius, seperti malware dan serangan *DDoS*, yang dapat mengganggu proses belajar mengajar dan merusak reputasi institusi pendidikan. Beberapa ancaman *Malware*, seperti *ransomware*, *trojan*, dan *spyware*, sering masuk melalui jalur seperti *email phishing* atau perangkat yang tidak terlindungi. Meskipun begitu, kebijakan keamanan yang tepat dan teknologi seperti antivirus terpusat dan pemantauan real-time dapat meminimalkan dampak ancaman tersebut.

Serangan *DDoS* juga menambah tantangan, dengan mengancam ketersediaan layanan *cloud*, termasuk aplikasi seperti sistem *e-learning* dan portal ujian. Serangan ini dapat menyebabkan *downtime* yang mengganggu kegiatan pendidikan. Berbagai strategi mitigasi, seperti penggunaan *firewall*, *CDN*, dan *WAF*, serta penerapan *load balancing* dan *autoscaling*, dapat membantu mengurangi dampak *DDoS*. Meskipun demikian, tantangan terbesar tetap terletak pada biaya dan infrastruktur yang dibutuhkan..

Strategi mitigasi ancaman di layanan *cloud* pendidikan bersifat komprehensif, mencakup berbagai lapisan perlindungan. Terdapat beberapa cara untuk mengurangi ancaman malware, yaitu dengan menggunakan *Intrusion Detection System (IDS)*, patching perangkat lunak, serta kebijakan antivirus terpusat. Selain itu, pemanfaatan teknologi seperti *Content Delivery Network (CDN)* dan optimasi server web dapat membantu mencegah serangan *DDoS*. Sementara itu, implementasi monitoring berkelanjutan dan *multi-factor authentication (MFA)* akan mempercepat deteksi dan respons terhadap ancaman siber.

Tantangan utama dalam menjaga keamanan layanan *cloud* pendidikan adalah keterbatasan sumber daya dan rendahnya kesadaran akan pentingnya keamanan siber. Banyak institusi pendidikan, terutama di negara berkembang, tidak memiliki anggaran yang cukup untuk solusi keamanan yang efektif. Program edukasi terstruktur untuk mahasiswa dan staf mengenai ancaman siber sangat penting. Begitu pun dengan implementasi solusi berbasis teknologi seperti *CSPM* dan kebijakan data *governance* yang jelas dapat membantu meningkatkan keamanan layanan *cloud*. Jadi, kunci untuk menciptakan ekosistem digital yang aman di lingkungan pendidikan adalah dengan adanya kolaborasi antara teknologi, kebijakan, dan manusia.

REFERENSI

Abidah, I. N., Hamdani, M. A., & Amrozi, Y. (2020). Implementasi Sistem Basis Data Cloud Computing pada Sektor Pendidikan. *KELUWIH: Jurnal Sains Dan Teknologi*, *1*(2), 77–84. https://doi.org/10.24123/saintek.v1i2.2868

Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security*, *15*(02), 148–167. https://doi.org/10.4236/jis.2024.152010

Alfian Saputra, R., Dito Ridwansyah, R., Alfiana Erlangga, D., & Rilvani, E. (2025). Keamanan Sistem Operasi dalam Era Internet of Things. In *Jurnal Mahasiswa Teknik Informatika)* (Vol. 9, Issue 2).

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. In *Journal of Computer Information Systems*. Taylor and Francis Ltd. https://doi.org/10.1080/08874417.2024.2329985

Aula Madina, T., & Fadhli, M. (2024). Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *7*(6).

Chandra, J. C. (n.d.). Analisis Keamanan Layanan E-Learning Terhadap Serangan Dos Dan Implementasi Mitigasi Pada Universitas Budi Luhur. *Jurnal TICOM: Technology of Information and Communication*, *10*(3), 2022. https://elearning.budiluhur.ac.id,

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry*, *15*(11). https://doi.org/10.3390/sym15111981

Fauzi, A., Maharani Putri, A., Fitriyani, F., Astriyani, R., Arisana, V., & Indah Cahyani, Y. (n.d.). *Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis*. https://doi.org/10.38035/jkmt.v2i2

E-ISSN : 2961 - 9386
P-ISSN : 2963 - 1742

Hill, A. D., Johnson, S. G., Greco, L. M., O'Boyle, E. H., & Walter, S. L. (2021). Endogeneity: A Review and Agenda for the Methodology-Practice Divide Affecting Micro and Macro Research. *Journal of Management*, *47*(1), 105–143. https://doi.org/10.1177/0149206320960533

Jawaid, S. A. (2023). Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity. *International Journal of Data Science and Big Data Analytics*, *2*(2). https://doi.org/10.51483/ijdsbda.2.2.2022.11-17

Khalid, M. I. I., & Zolkipli, M. F. (2022). Review on Cloud Security and Challenges on Higher Education. *Malaysian Journal of Applied Sciences*, *7*(1), 1–9. https://doi.org/10.37231/myjas.2022.7.1.284

Kraus, S., Breier, M., Lim, W. M., Dabić, M., Kumar, S., Kanbach, D., Mukherjee, D., Corvello, V., Piñeiro-Chousa, J., Liguori, E., Palacios-Marqués, D., Schiavone, F., Ferraris, A., Fernandes, C., & Ferreira, J. J. (2022). Literature reviews as independent studies: guidelines for academic practice. *Review of Managerial Science*, *16*(8), 2577–2595. https://doi.org/10.1007/s11846-022-00588-8

Lakhno, V., Akhmetov, B., Kryvoruchko, O., Chubaievskyi, V., Desiatko, A., Bereke, M., & Shalabaeva, M. (2024). Cyber threats to the Private Academic Cloud. *International Journal of Electronics and Telecommunications*, *70*(2), 413–420. https://doi.org/10.24425/ijet.2024.149560

Lallie, H., Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (n.d.). *Understanding Cyber Threats Against the Universities, Colleges, and Schools*. https://www.researchgate.net/publication/372655992

Liubchenko, V. V., & Volkov, D. V. (2024). Cyber-aware threats and management strategies in cloud environments. *Herald of Advanced Information Technology*, *7*(2), 158–170. https://doi.org/10.15276/hait.07.2024.11

Maimun. (2023). Evaluation of the Use of Cloud Computing Technology in Managing Organizational Information Systems. *Journal Informatic, Education and Management (JIEM)*, *5*(1), 21–25. https://doi.org/10.61992/jiem.v5i1.72

Marlina, S. (2025). Keamanan Siber pada Aplikasi Cloud Computing: Analisis Ancaman dan Strategi Mitigasi. In *Jurnal Komputer dan Teknologi Informasi* (Vol. 01, Issue 1). https://jurnal.samudrailmu.com/index.php/jukomtik

Mashendra, M., Salam, S., Kahar, A., Satria, E., Karim, L. O. M., Mansyah, M. S., Rahim, A., & Serah, Y. (2024). Edukasi Trend Kejahatan Cyber Pada SMA Negeri 2 Baubau. *Journal of Community Development*, *5*(2), 333–339. https://doi.org/10.47134/comdev.v5i2.291

M.Iqbal, M. I., Yuhandri Yunus, & Syafri Arlis. (2024). Audit Keamanan Jaringan Komputer Server dari Serangan DDoS Menggunakan Snort Intrusion Detection System. *The Indonesian Journal of Computer Science*, *13*(5). https://doi.org/10.33022/ijcs.v13i5.4391

Mykhaylova, O., Korol, M., & Kyrychok, R. (2024). *Research and analysis of issues and challenges in ensuring cyber security in cloud computing ⋆*.

Puspita Maharani, H., Sidauruk, H. B., Naisyah, D., & Syafitri, Q. (2025). *Peranan Cybersecurity dalam Meningkatkan Ketahanan Bisnis Digital Terhadap Cybercrime* (Vol. 3, Issue 2).

Risky Kurniawan, H., Nur Sofiyanto, I., & Faqih Habiburrohman, M. (n.d.). *Analisis Risiko Keamanan Data pada Platform Cloud Computing*. 18–2024.

Rumetna, M. S. (2018). Title Case. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *5*(3), 305–314. https://doi.org/10.25126/jtiik.201853595

Siregar, M. I., Lubis, I., & Liza, R. (n.d.). Implementasi Keamanan Anti DDoS Menggunakan Router Mikrotik Pada Layanan Cloud Storage Basis Local Di Sekolah Menengah Kejuruan. In *Jurnal Networking System and Security System E-ISSN* (Vol. 2, Issue 1).

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Zidane, M. (2022). *Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes* (Vol. 6, Issue 1). http://j-ptiik.ub.ac.id