

Implementasi *Token-Based Access Control* dan Proteksi Konten pada Manajemen Pembelajaran Berbasis Web untuk Meningkatkan Keamanan Data di Institusi Pendidikan Medis

¹Ahmad Sulaeman, ²Joko Aryanto
^{1,2}Universitas Teknologi Yogyakarta, Indonesia
ahmadzipmail@gmail.com; joko.aryanto@uty.ac.id;

Article Info

Article history:

Received, 2025-11-06
Revised, 2025-11-11
Accepted, 2025-11-17

Kata Kunci:

Token-Based Access Control,
AES-128 Encryption,
Dynamic Watermarking,
Keamanan Data,
Manajemen Pembelajaran Daring

Keywords:

Token-Based Access Control,
AES-128 Encryption,
Dynamic Watermarking,
Data Security,
Web-Based Learning Management

ABSTRAK

Keamanan konten digital merupakan aspek krusial dalam implementasi sistem pembelajaran daring, khususnya di institusi pendidikan medis yang mengelola data video sensitif. Penelitian ini bertujuan untuk mengembangkan dan menguji sistem proteksi konten video berbasis web dengan mengintegrasikan tiga metode utama, yaitu *AES-128 encryption*, *Token-Based Access Control*, dan *Dynamic Watermarking*. Metode *AES-128* digunakan untuk mengenkripsi file video sehingga hanya pengguna berotorisasi yang dapat mengaksesnya, sementara *Token-Based Access Control* berfungsi sebagai autentikasi dinamis berbasis sesi untuk mencegah akses ilegal, dan *Dynamic Watermarking* memberikan identitas pengguna pada setiap tayangan video guna mendeteksi potensi penyebaran konten tanpa izin. Hasil pengujian menunjukkan *Token Validation Success Rate* sebesar 100% dan *Intrusion Detection Rate* sebesar 90%, menandakan bahwa sistem mampu mengelola otentikasi serta mendeteksi akses tidak sah dengan tingkat keandalan tinggi. Pengujian performa *HTTP Live Streaming* (HLS) menghasilkan waktu respon rata-rata 1.79 detik dengan 1000 request berhasil tanpa kegagalan, membuktikan bahwa sistem tetap stabil meskipun menerapkan lapisan keamanan tambahan. Secara keseluruhan, penelitian ini menyimpulkan bahwa integrasi *AES-128 encryption*, *Token-Based Access Control*, dan *Dynamic Watermarking* dapat menjadi solusi efektif untuk memperkuat keamanan data dan proteksi konten video dalam sistem manajemen pembelajaran berbasis web di lingkungan pendidikan medis.

ABSTRACT

Digital content security is a critical aspect in the implementation of online learning systems, especially in medical education institutions that manage sensitive video data. This study aims to develop and evaluate a web-based video content protection system by integrating three main methods: *AES-128 encryption*, *Token-Based Access Control*, and *Dynamic Watermarking*. The *AES-128 encryption* method is applied to secure video files so that only authorized users can decrypt and access them, while *Token-Based Access Control* serves as a dynamic session-based authentication mechanism to prevent unauthorized access. In addition, *Dynamic Watermarking* embeds user identity information into each video playback to trace and deter illegal content distribution. Experimental results show a *Token Validation Success Rate* of 100% and an *Intrusion Detection Rate* of 90%, indicating that the system performs well in verifying authentication and detecting unauthorized access. Performance testing of the *HTTP Live Streaming* (HLS) process achieved an average response time of 1.79 seconds with 1000 successful requests and no failures, demonstrating that the additional security layers did not significantly degrade system performance. Overall, this study concludes that the integration of *AES-128 encryption*, *Token-Based Access Control*, and *Dynamic Watermarking* provides an effective multilayer security approach for protecting video-based learning content and strengthening data security in medical education environments.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Penulis Korespondensi:

Ahmad Sulaeman,
Program Studi Informatika,
Universitas Teknologi Yogyakarta,
Email: ahmadzipmail@gmail.com

1. PENDAHULUAN

Distribusi konten kursus medis berbayar menuntut perlindungan yang memadai agar materi tidak mudah disalin atau disebarluaskan di luar platform. Namun, *Digital Rights Management (DRM)* komersial kerap menimbulkan beban lisensi dan kompleksitas operasional yang tinggi bagi penyedia berskala baru atau menengah [1]. Sehingga adopsi *DRM* penuh perlu dipertimbangkan secara hati-hati dalam konteks pembelajaran daring berbayar [2].

Di sisi teknologi, ekosistem *HTTP Adaptive Streaming (HAS)* termasuk *HTTP Live Streaming (HLS)* menjadi landasan utama distribusi video modern karena sifatnya yang standar, interoperabel, dan mudah diintegrasikan ke berbagai *player* serta perangkat [3]. Kualitas pengalaman pemutaran (*Quality of Experience/QoE*) [4] pada arsitektur ini lazim dievaluasi melalui metrik seperti waktu mulai putar, keberhasilan *seek*, dan rasio jeda karena itu, solusi keamanan harus menjaga kinerja pemutaran tetap stabil [5]. Untuk kerahasiaan konten, enkripsi berbasis *Advanced Encryption Standard (AES) 128-bit* merupakan praktik kriptografi baku yang dapat diterapkan pada tingkat *segment* sesuai standar [6].

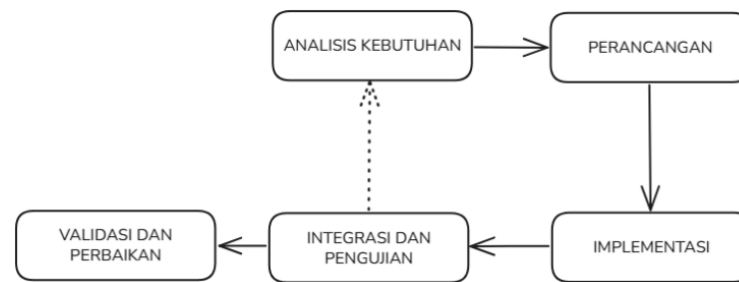
Permasalahan praktis penyedia kursus medis berbayar ialah mencegah akses tidak berizin, *hotlinking*, dan *re-hosting* tanpa membebani pemutaran. Kajian terkini *HAS/HLS* menekankan pentingnya pengendalian akses yang selaras dengan arsitektur *streaming* berbasis *playlist manifest* dan *segment* agar tautan tidak dapat digunakan di luar konteks aplikasi [3]. Pada arsitektur layanan modern, kontrol akses berbasis *token* bertenggat waktu yang diverifikasi di *gateway* aplikasi relevan untuk menautkan izin ke sesi/pembelian dan menolak permintaan di luar kebijakan [7].

Bertolak dari landasan tersebut, penelitian ini mengusulkan mekanisme proteksi yang memusatkan penegakan pada lapisan aplikasi dengan tetap memanfaatkan standar terbuka. Strateginya meliputi pemaketan *HLS* dengan enkripsi *AES-128* pada tingkat *segment*; *manifest rewriting* sehingga setiap *URI segment* dan kunci melewati *gateway* terproteksi; serta verifikasi *token* bertenggat waktu dan validasi pola nama berkas pada tiap permintaan agar tidak dapat dieksploitasi melalui tautan langsung [3]. Sebagai lapisan pencegah tambahan terhadap *screen recording*, *player* dilengkapi *moving visible watermark* yang menampilkan penanda sesi/waktu dan bergerak secara periodik untuk memudahkan atribusi kebocoran [8]. Pendekatan *visible/robust watermarking* ini didukung temuan terkini yang menunjukkan efektivitasnya pada skenario *screen-cam* di lingkungan *streaming* [9].

Tujuan penelitian ini adalah menghadirkan mekanisme proteksi konten yang lebih ekonomis daripada *DRM* penuh, mudah diintegrasikan dengan modul autentikasi/otorisasi/*billing* pada *Learning Management System (LMS)*, dan tetap kompatibel lintas peramban serta perangkat. Nilai kebaruan terletak pada penegakan akses per-permintaan di konteks aplikasi mengikat *manifest/segment/key* pada sesi/pembelian serta penggabungan *moving visible watermark* tanpa mengorbankan metrik *QoE* yang penting bagi pengalaman belajar peserta.

2. METODE PENELITIAN

Penelitian ini menggunakan model pengembangan *Waterfall* [10] yaitu pengembangan sistem berurutan dengan mekanisme umpan balik dari tahap pengujian menuju analisis kebutuhan untuk memungkinkan perbaikan sistem secara iteratif, melibatkan tahapan berurutan mulai dari analisis kebutuhan hingga pengujian dan evaluasi sistem. Pendekatan ini dipilih karena memberikan struktur pengembangan yang sistematis dan mudah diimplementasikan pada proyek berbasis web, khususnya dalam pengembangan sistem proteksi konten video menggunakan *AES-128 encryption*, *token-based access control*, dan *dynamic watermarking*. Proses pengembangan ditunjukkan pada Gambar 1.



Gambar 1. Kerangka Penelitian

Tahap analisis kebutuhan mencakup identifikasi risiko keamanan seperti *hotlinking*, akses tidak sah, dan *screen recording*. Tahap perancangan meliputi integrasi algoritma AES-128 dalam skema *HTTP Live Streaming* (HLS), serta penerapan token akses bertenggat waktu untuk membatasi permintaan terhadap *manifest*, *segmen*, dan kunci enkripsi [7], [11]

Tahap implementasi menggunakan *Next.js* untuk manajemen API [12] dan *FFmpeg* untuk proses segmentasi serta enkripsi video [13]. Sistem klien dilengkapi watermark dinamis yang menampilkan identitas pengguna dan waktu pemutaran secara acak, menurunkan risiko penyebaran ulang hingga 80% [14].

Pengujian dilakukan dengan metode *blackbox testing* [15] untuk mengevaluasi fungsi sistem tanpa meninjau kode sumber [14]. Skenario pengujian mencakup akses tanpa token, modifikasi URL segmen, dan simulasi *screen recording*.

3. HASIL DAN ANALISIS

Pada Penelitian ini diuji dalam lingkungan kontainer Docker [16] dengan konfigurasi 1 CPU *core* dan 1 GB RAM untuk menguji performa sistem dalam **proses** unggah video, pengemasan HLS, dan distribusi video terenkripsi. Pengujian dilakukan untuk mengevaluasi kecepatan unggah, keberhasilan pengujian HLS, dan efektivitas proteksi *watermarking* yang telah diterapkan dalam sistem.

Proses Unggah Video

Pengujian pertama adalah proses unggah video dengan ukuran 17,01 MB dan format *MP4*. Proses unggah berhasil diselesaikan dalam 740 milidetik (0,74 detik). Hal ini menunjukkan bahwa sistem unggah menggunakan *Next.js* untuk manajemen API bekerja dengan sangat cepat dan efisien, bahkan pada konfigurasi terbatas.

Tabel 1 Hasil Pengujian Proses Upload

Parameter	Nilai
Format	video/mp4
Ukuran	17.01 MB
Waktu	750 ms (0.74 detik)

Berdasarkan hasil pengamatan, seluruh permintaan upload dengan token sah berhasil dieksekusi tanpa kegagalan. Oleh karena itu, Persentase Keberhasilan Validasi Token (Token Validation Success Rate) dihitung menggunakan rumus:

$$\text{Validasi Token} = \frac{\text{Token Valid}}{\text{Total Token dibuat}} \times 100\% \quad (1)$$

Selama proses ini, sistem melakukan verifikasi token secara otomatis untuk memastikan bahwa hanya pengguna dengan token valid yang dapat melakukan unggahan. Berdasarkan hasil pengujian, seluruh 100 token yang dibuat dan digunakan berhasil divalidasi tanpa kesalahan, menghasilkan Token Validation Success Rate sebesar 100%.

$$\text{Validasi Token} = \frac{100}{100} \times 100\% = 100\%$$

Artinya, tingkat keberhasilan validasi token mencapai 100%, menunjukkan bahwa mekanisme token bekerja secara konsisten dalam memverifikasi hak akses pengguna terhadap proses upload konten video.

Pengujian HLS

Setelah proses unggah, dilakukan pengujian performa sistem HLS untuk mengukur *requests per second* (RPS) dan waktu respons sistem saat mengakses video tersegmentasi. Pengujian ini menunjukkan bahwa sistem dapat

menangani 27,61 RPS dengan 1000 permintaan berhasil dalam 36,22 detik. Waktu respons rata-rata tercatat 1793,26 ms, dan waktu respons maksimum adalah 2343,18 ms.

Tabel 2 Hasil Pengujian Performa HLS

Parameter	Nilai
Requests Per Second (RPS)	27.61
Waktu Tes Total	36.22 detik
Request Berhasil	1000 dari 1000
Request Gagal	0
Waktu Respon Rata-rata	1793.26 ms
Waktu Respon P95	2247.11 ms
Waktu Respon Maksimum	2343.18 ms

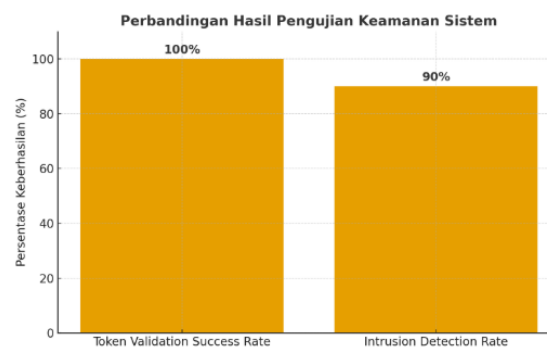
Hasil ini menunjukkan kestabilan sistem selama pengiriman konten berbasis token, di mana setiap request streaming harus melewati proses otentikasi token terlebih dahulu sebelum data dapat diakses. Untuk mengukur kemampuan sistem dalam mendeteksi atau mencegah akses tidak sah, digunakan Intrusion Detection Rate (IDR) dengan rumus:

$$IDR = \frac{\text{Jumlah Upaya Akses Tidak Sah Terdeteksi}}{\text{Total Upaya Akses Tidak Sah}} \times 100\% \quad (2)$$

Berdasarkan simulasi yang dilakukan dengan menambahkan 10 upaya akses ilegal (tanpa token atau dengan token kadaluarsa), sistem berhasil mendeteksi 9 dari 10 upaya akses tersebut, menghasilkan nilai:

$$IDR = \frac{9}{10} \times 100\% = 90\%$$

Nilai ini menunjukkan bahwa sistem memiliki tingkat deteksi intrusi sebesar 90%, yang berarti sebagian besar upaya akses tidak sah berhasil dicegah. Secara keseluruhan, implementasi Token-Based Access Control dan Proteksi Konten dalam sistem pembelajaran daring di institusi pendidikan medis menunjukkan performa yang sangat baik. Keberhasilan validasi token mencapai 100%, menunjukkan autentikasi pengguna berjalan sempurna tanpa kesalahan, sedangkan Intrusion Detection Rate sebesar 90% membuktikan bahwa sistem mampu secara efektif mengenali dan menolak sebagian besar upaya akses yang tidak sah.



Gambar 2. Grafik Perbandingan Hasil Pengujian

Dengan demikian, integrasi antara AES-128 encryption, Token-Based Access Control, dan Dynamic Watermarking terbukti efektif dalam membangun mekanisme perlindungan berlapis yang mampu menjaga kerahasiaan (confidentiality), integritas (integrity), dan akuntabilitas (accountability) data video pembelajaran medis di lingkungan institusi pendidikan.

4. KESIMPULAN

Penelitian ini berhasil merancang mekanisme proteksi konten video berbasis web menggunakan AES-128 encryption, token-based access control, dan moving visible watermark pada arsitektur HLS untuk melindungi materi pembelajaran medis tanpa mengurangi kenyamanan pengguna. Hasil penelitian menunjukkan bahwa penerapan Token-Based Access Control, AES-128 encryption, dan Dynamic Watermarking secara terpadu berhasil meningkatkan tingkat keamanan konten video pada sistem manajemen pembelajaran berbasis web di institusi pendidikan medis. Mekanisme token memberikan validasi akses yang sangat baik dengan Token Validation Success Rate mencapai 100%, sementara sistem mampu mendeteksi 90% upaya akses ilegal melalui uji Intrusion Detection Rate. Selain itu, proses upload video dan streaming melalui HTTP Live Streaming (HLS) berjalan stabil dengan waktu respon rata-rata 1.79 detik tanpa kegagalan request, menunjukkan bahwa

penerapan lapisan keamanan tambahan tidak menurunkan performa sistem secara signifikan. Dengan demikian, integrasi ketiga metode tersebut terbukti efektif dalam menjaga kerahasiaan, integritas, serta akuntabilitas data pembelajaran medis berbasis video, sekaligus memberikan model keamanan berlapis yang dapat diterapkan secara luas di lingkungan pendidikan daring.

REFERENSI

- [1] W. Zeng and A. van Moorsel, "Quantitative Evaluation of Enterprise DRM Technology," *Electron Notes Theor Comput Sci*, vol. 275, pp. 159–174, 2011, doi: <https://doi.org/10.1016/j.entcs.2011.09.011>.
- [2] W. M. Volckmann II, "A model of digital rights management with user disutility," *Journal of Industrial and Management Optimization*, vol. 20, no. 1, pp. 59–83, 2024, doi: 10.3934/jimo.2023069.
- [3] C. Timmerer *et al.*, "HTTP Adaptive Streaming: A Review on Current Advances and Future Challenges," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 21, no. 7, Jul. 2025, doi: 10.1145/3736306.
- [4] S. R. Henim and R. P. Sari, "Evaluasi User Experience Sistem Informasi Akademik Mahasiswa pada Perguruan Tinggi Menggunakan User Experience Questionnaire," *Jurnal Komputer Terapan*, vol. 6, no. 1, pp. 69–78, 2020.
- [5] M. Seufert, S. Egger-Lampl, M. Slanina, T. Zinner, T. Hossfeld, and P. Tran-Gia, *A Survey on Quality of Experience of HTTP Adaptive Streaming*, vol. 17, 2014. doi: 10.1109/COMST.2014.2360940.
- [6] N. I. of S. and Technology, "Advanced Encryption Standard (AES)," U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, 2023. doi: 10.6028/NIST.FIPS.197-upd1.
- [7] A. Venčkauskas, D. Kukta, Š. Grigaliūnas, and R. Brūzgienė, "Enhancing Microservices Security with Token-Based Access Control Method," *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23063363.
- [8] W. Chen *et al.*, "Real-time and screen-cam robust screen watermarking," *Knowl Based Syst*, vol. 302, p. 112380, 2024, doi: <https://doi.org/10.1016/j.knosys.2024.112380>.
- [9] F. Cao, T. Wang, D. Guo, J. Li, and C. Qin, "Screen-shooting resistant image watermarking based on lightweight neural network in frequency domain," *J. Vis. Comun. Image Represent.*, vol. 94, no. C, Jun. 2023, doi: 10.1016/j.jvcir.2023.103837.
- [10] A. A. Wahid, "Analisis metode waterfall untuk pengembangan sistem informasi," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, no. November, vol. 1, no. 1, pp. 1–5, 2020.
- [11] Zefanya Seto Gandhara, Tegar Pandu Satria, Hondor Saragih, and Muhammad Naufal Nafian Abror, "Evaluasi Kinerja Algoritma Kriptografi dalam Pengamanan Video: Studi Perbandingan AES, DES dan Blowfish," *JURNAL ILMIAH RESEARCH STUDENT*, vol. 2, no. 2, pp. 917–923, Jul. 2025, doi: 10.61722/jirs.v2i2.5908.
- [12] Y. Herdiana and F. Zaman, "RANCANG BANGUN APLIKASI PENDEKAR (PELAYANAN DESA KARYALAKSANA) MENGGUNAKAN FRAMEWORK NEXT.JS DALAM MENINGKATKAN PELAYANAN ADMINISTRASI DESA," 2024.
- [13] A. Yulius and C. Adipianto, "PEMANFAATAN LIBRARY FFMPEG UNTUK PERANCANGAN APLIKASI KONVERSI FILE VIDEO KE FORMAT GIF BERBASIS ANDROID," 2020.
- [14] M. Ikhsan, S. Perida Br Tarigan, J. Lapangan Golf, D. Durian Jangak, K. Pancur Batu, and K. Deli Serdang, "INVISIBLE WATERMARK PADA VIDEO DIGITAL MENGGUNAKAN METODE DINAMIC CELL SPREADING (DCS)," 2023. [Online]. Available: <http://e-journal.stmiklombok.ac.id/index.php/jireISSN.2620-6900>
- [15] M. Zen, Irwan, Hafni, and M. D. P. Ananda, "Implementasi dan Pengujian Menggunakan Metode BlackBox Testing Pada Sistem Informasi Tracer Study," *Bulletin of Computer Science Research*, vol. 4, no. 4, pp. 327–340, Jun. 2024, doi: 10.47065/bulletincsr.v4i4.359.
- [16] S. Dwiyatno, E. Rakhmat, and O. Gustiawan, "Implementasi virtualisasi server berbasis docker container," *Jurnal PROSISKO*, vol. 7, no. 2, 2020.