

Penerapan Role-Based Access Control Berbasis Klaim JWT untuk Mitigasi Ancaman Orang Dalam pada Jitsi Meet

Abdul Hadi^{1*}, Muzakkir Pangri², Doddy Teguh Yuwono³

¹Program Studi Teknik Informatika, STMIK Palangkaraya, Palangka Raya

²Program Studi Teknik Informatika, Universitas Muhammadiyah Sorong, Sorong

³Program Studi Manajemen Informasi Kesehatan, Universitas Muhammadiyah Palangkaraya, Palangka Raya

E-mail: *¹abdulhadi@stmikplk.ac.id, ²muzakkir@um-sorong.ac.id, ³doddyty@umpr.ac.id

Abstrak

Sebagian besar ajakan untuk mengganggu pertemuan daring (zoombombing) berasal dari orang dalam, yaitu peserta sah yang memiliki tautan dan hak akses ke ruang pertemuan. Penelitian terdahulu menerapkan Role-Based Access Control (RBAC) dan JSON Web Token (JWT) pada antarmuka dan API aplikasi web, tetapi belum membatasi hak peserta di dalam ruang konferensi video. Penelitian ini bertujuan menerapkan RBAC berbasis klaim JWT pada server Jitsi Meet stable-11146-2. Server tersebut digunakan oleh lima akun pengelola untuk 16 kelas dengan 306 catatan kehadiran peserta. Peran administrator, pemilik kelas, moderator, dan peserta dipetakan ke dalam klaim JWT bertanda tangan HS256 yang memuat status moderator, izin perekaman, nama ruang, masa berlaku, penerbit token, dan audiens. Token diverifikasi oleh server Prosody, lalu modul token_affiliation menetapkan peran peserta di dalam ruang. Pengujian menggunakan matriks kontrol akses berisi 21 skenario ancaman orang dalam dan 9 hak sah. Setiap kasus diuji tiga kali pada empat konfigurasi, yaitu konfigurasi bawaan Jitsi, JWT seragam, model awal, dan model setelah perbaikan. Pada sembilan kasus serangan yang berlaku di semua konfigurasi, tingkat eskalasi hak mencapai 33,3% pada konfigurasi bawaan dan 88,9% pada JWT seragam, sedangkan pada kedua model sebesar 0%. Pada matriks lengkap, model awal masih meloloskan 2 dari 21 serangan (9,5%), yaitu perolehan hak moderator oleh akun moderator portal di kelas milik pengguna lain dan permintaan perekaman yang tidak diperiksa server. Setelah hak moderator dibatasi pada pemilik kelas dan modul filter_iq_jibri diaktifkan, tingkat eskalasi dan tingkat penolakan keliru menjadi 0%, sedangkan kesesuaian terhadap matriks RBAC mencapai 100% pada ketiga ulangan.

Kata kunci - Role-Based Access Control, JSON Web Token, Jitsi Meet, ancaman orang dalam, eskalasi hak

1. PENDAHULUAN

Sejak pandemi COVID-19, konferensi video menjadi sarana utama perkuliahan sinkron dan hingga kini tetap digunakan untuk kelas daring, rapat, dan seminar. Peningkatan penggunaan tersebut diikuti oleh munculnya *zoombombing*, yaitu masuknya pihak yang tidak diundang ke dalam pertemuan daring untuk menayangkan konten yang tidak pantas atau mengacaukan jalannya pertemuan, yang kemudian berkembang menjadi bentuk perundungan daring pada berbagai platform [1]. Ling dkk. [2] menganalisis ajakan *zoombombing* di Twitter dan 4chan. Sebagian besar ajakan tersebut berasal dari orang dalam yang memiliki akses sah, terutama pelajar dan mahasiswa yang membagikan tautan kelasnya sendiri. Kata sandi ruang tidak efektif

menghadapi pelaku semacam ini, sedangkan tautan masuk yang unik untuk setiap peserta terbukti lebih efektif.

Kajian keamanan konferensi video sejauh ini lebih banyak menilai aplikasi komersial dari sisi pengguna, antara lain kesadaran dosen terhadap pengaturan keamanan dan privasi [3], kebocoran data peserta melalui tangkapan layar pertemuan [4], pemantauan mikrofon ketika tombol bisu aktif [5], dan pemrosesan data pribadi pada aplikasi Android [6]. Kajian-kajian tersebut belum merancang kebijakan otorisasi yang dapat diterapkan institusi pada server yang dikelolanya sendiri.

Platform sumber terbuka yang dipasang pada server milik institusi memberikan kendali penuh atas data dan konfigurasi. Penelitian tentang Jitsi di Indonesia masih berfokus pada kualitas layanan jaringan, misalnya perbandingan Jitsi dan BigBlueButton pada *virtual private server* [7] dan pengujian Jitsi berbasis kontainer pada Amazon Web Services [8]. Mahmoud dan Abozariba [9] mengulas penerapan dan tantangan WebRTC yang menjadi dasar platform tersebut. Pengaturan hak peserta di dalam ruang konferensi belum dikaji.

Ancaman orang dalam lebih sulit ditangani daripada ancaman dari luar karena pelaku memiliki akses sah ke aset organisasi [10]. Sebagian besar penelitian tentang ancaman orang dalam berfokus pada deteksi, antara lain dengan *machine learning* [11], deteksi eskalasi hak pada layanan *cloud computing* [12], dan integrasi teknik *cyber deception* ke dalam Attribute-Based Access Control [13]. Pendekatan deteksi bekerja setelah suatu tindakan terjadi. Padahal, pada kelas daring, satu tindakan saja, seperti mengeluarkan seluruh peserta atau mengakhiri rapat, sudah cukup untuk menghentikan perkuliahan. Oleh karena itu, pencegahan melalui kontrol akses pada sisi server menjadi kebutuhan utama.

Role-Based Access Control (RBAC) adalah model kontrol akses yang melekatkan izin pada peran sehingga pengguna memperoleh izin melalui keanggotaannya dalam suatu peran. Model ini dibakukan dalam usulan standar NIST yang mencakup RBAC inti, hierarki peran, dan pemisahan tugas [14]. Mohamed dkk. [15] menegaskan perbedaan antara autentikasi, otorisasi, dan kontrol akses, sedangkan Abdurraheem dkk. [16] menunjukkan bahwa penerapan RBAC cenderung menyimpang dari prinsip hak minimum seiring dengan berkembangnya sistem. Kegagalan penegakan otorisasi (*broken access control*) memungkinkan pengguna sah bertindak di luar haknya [17], [18] dan menempati peringkat teratas risiko keamanan aplikasi web menurut OWASP. Oleh sebab itu, penelitian terkini menekankan pentingnya kasus uji keamanan yang andal [19] dan verifikasi kebijakan akses secara sistematis [20].

JSON Web Token (JWT) adalah format klaim ringkas bertanda tangan digital yang dapat memuat identitas dan atribut otorisasi pengguna [21]. Praktik terbaik penggunaan JWT mensyaratkan validasi terhadap algoritma, kunci, penerbit token (*issuer*, klaim *iss*), audiens (*aud*), dan masa berlaku (*exp*) [22], [23]. Penerbit token adalah sistem yang membuat dan menandatangani token, sedangkan audiens adalah aplikasi yang menjadi tujuan token tersebut. Klaim khusus pada JWT telah digunakan untuk autentikasi heterogen pada *edge computing* [24] dan untuk kontrol akses pada arsitektur *microservices* [25]. Di Indonesia, JWT telah diterapkan untuk autentikasi berbasis HMAC [26], [27], sedangkan RBAC telah diterapkan pada sistem rantai pasok, otorisasi terpusat, sistem *multi-tenant*, *e-learning*, dan *microservices* [28], [29], [30], [31], [32], serta pemetaan hak akses berbasis ISO/IEC 27001 [33]. Muhammad dkk. [34] menunjukkan dampak kegagalan kontrol akses di lingkungan pendidikan. Manipulasi peran pengguna pada *Learning Management System* (LMS) sebuah universitas memberikan akses administrator kepada penyerang dan membuka lebih dari 117.000 data pengguna. Ringkasan penelitian terdahulu disajikan pada Tabel 1.

Tabel 1 Perbandingan penelitian terdahulu dengan penelitian ini

Penelitian	Objek	Mekanisme	Lapisan penegakan	Metode pengujian
[7], [8]	Jitsi, BigBlueButton	–	–	Kualitas layanan jaringan
[26], [27]	Layanan web REST	JWT HMAC	API	Fungsional dan waktu proses

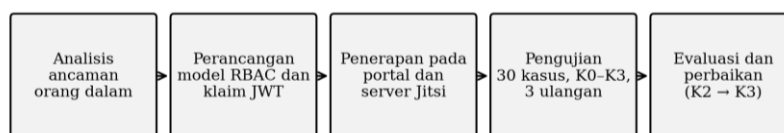
Penelitian	Objek	Mekanisme	Lapisan penegakan	Metode pengujian
[28], [29], [30], [31]	Aplikasi web	RBAC	Aplikasi web	<i>Black-box</i>
[32]	<i>Microservices</i>	RBAC Keycloak dan JWT	API dan layanan	OWASP ASVS dan pemindaian ZAP
[34]	LMS universitas	–	Aplikasi web	Uji penetrasi
Penelitian ini	Jitsi Meet	RBAC berbasis klaim JWT	Portal dan server konferensi (Prosody)	30 kasus otomatis, 4 konfigurasi, 3 ulangan

Tabel 1 menunjukkan bahwa penelitian terdahulu menegakkan peran pada tingkat aplikasi web atau API. Pada konferensi video, tindakan di dalam ruang, seperti mengeluarkan peserta, membisukan mikrofon, menaikkan peran, mengaktifkan *lobby*, mengakhiri rapat, dan memulai perekaman, dikirim langsung ke *signaling server* tanpa melalui API aplikasi. Jitsi Meet menyediakan autentikasi JWT melalui server XMPP Prosody. Akan tetapi, konfigurasi yang umum digunakan memberikan peran moderator kepada setiap pengguna terautentikasi atau kepada pengguna pertama yang masuk ke ruang. Akibatnya, setiap peserta yang memegang token sah dapat melakukan seluruh tindakan moderator.

Berdasarkan permasalahan tersebut, kebaruan penelitian ini terletak pada penegakan RBAC berbasis klaim JWT hingga ke tingkat server konferensi video Jitsi Meet yang dikelola secara mandiri, bukan hanya pada antarmuka atau API. Pengujian dilakukan dengan matriks 30 kasus (21 ancaman orang dalam dan 9 hak sah) yang dijalankan secara otomatis tiga kali pada empat konfigurasi, yaitu konfigurasi bawaan Jitsi, JWT seragam, model awal, dan model setelah perbaikan. Temuan utamanya adalah bahwa autentikasi JWT seragam meningkatkan eskalasi hak, sedangkan model yang memetakan peran ke klaim JWT dan menegakkannya di server Prosody menekan tingkat eskalasi menjadi 0% setelah dua celah pada model awal diperbaiki.

2. METODE PENELITIAN

Penelitian ini dilaksanakan dalam lima tahap, yaitu analisis ancaman, perancangan model RBAC, penerapan pada portal dan server Jitsi, pengujian pada server uji yang terpisah, serta evaluasi dan perbaikan. Tahapan penelitian ditunjukkan pada Gambar 1.



Gambar 1 Tahapan penelitian

2.1 Objek dan Data Penelitian

Objek penelitian adalah layanan Jitsi Meet (*Docker image* stable-11146-2) yang terhubung dengan portal manajemen kelas. Portal tersebut menyimpan akun pengelola, data kelas, kode akses (*passcode*), dan daftar hadir, serta menerbitkan token akses ruang. Pada periode 7 September hingga 10 Oktober 2026, portal digunakan oleh lima akun pengelola, yang terdiri atas tiga administrator dan dua moderator, untuk 16 kelas milik dua pemilik. Seluruh kelas menggunakan kode akses, dan tercatat 306 baris kehadiran pada 15 kelas. Nama pada daftar hadir diisi sendiri oleh peserta sehingga angka tersebut menyatakan jumlah catatan kehadiran, bukan jumlah individu yang berbeda. Data produksi hanya digunakan dalam bentuk agregat tanpa identitas peserta.

2.2 Model Ancaman

Pelaku yang dikaji dalam penelitian ini adalah orang dalam, yaitu pihak yang memiliki kode akses kelas atau akun portal yang sah. Pelaku diasumsikan mampu membaca dan mengubah token miliknya, membuat token baru dengan kunci sembarang, serta menjalankan JavaScript pada *browser console* untuk memanggil fungsi konferensi secara langsung tanpa melalui tombol

antarmuka. Sebaliknya, pelaku diasumsikan tidak mengetahui kunci rahasia penandatanganan JWT dan tidak memiliki akses ke server. Berdasarkan pola gangguan yang telah dilaporkan [1], [2] dan kategori *broken access control* [17], [18], ancaman dikelompokkan ke dalam tiga kategori berikut.

1. Manipulasi token, yaitu mengubah klaim tanpa menandatangani ulang, mengganti algoritma menjadi *none*, menandatangani token dengan kunci lain, menggunakan token kedaluwarsa, menggunakan token dengan audiens atau penerbit lain, dan menggunakan token ruang A untuk masuk ke ruang B [22].
2. Penyalahgunaan hak di dalam ruang, yaitu peserta mengeluarkan peserta lain, membisukan pemilik kelas, menaikkan peran diri sendiri atau peserta lain, mengaktifkan *lobby*, mengakhiri rapat, memulai perekaman, serta memperoleh peran moderator karena masuk lebih awal atau karena pemilik kelas telah keluar.
3. Penyalahgunaan peran portal, yaitu akun moderator atau pengguna yang bukan pemilik kelas meminta token moderator untuk kelas milik pengguna lain, serta moderator yang tidak memiliki izin perekaman memulai perekaman.

2.3 Perancangan Model RBAC

Model yang dirancang mengacu pada RBAC inti [14] yang terdiri atas komponen pengguna, peran, izin, penugasan pengguna ke peran, dan penugasan izin ke peran. Penelitian ini membedakan dua jenis peran, yaitu *peran portal* dan *peran ruang*. Peran portal (administrator, moderator, dan pengguna) melekat pada akun, sedangkan peran ruang (moderator dan peserta) hanya berlaku di dalam satu ruang konferensi. Agar tidak rancu, istilah *moderator portal* dan *pengguna portal* dipakai untuk peran pada akun, sedangkan *moderator ruang* dan *peserta ruang* dipakai untuk peran di dalam konferensi. *Pemilik kelas* bukan peran portal, melainkan relasi akun–kelas: akun yang membuat suatu kelas menjadi pemilik kelas tersebut, terlepas dari peran portalnya.

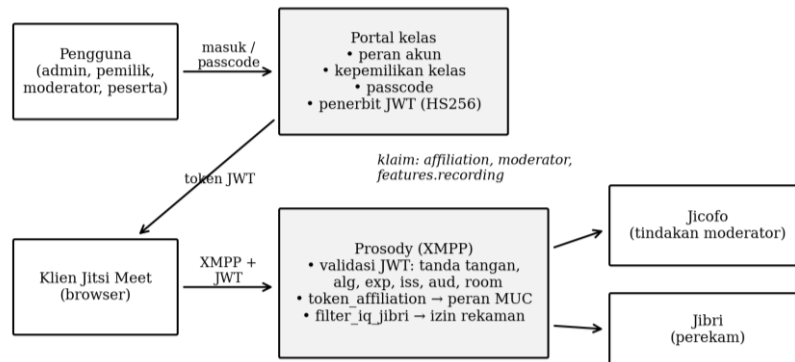
Peran ruang ditentukan oleh hubungan antara akun dan kelas dengan aturan sebagai berikut: (1) administrator menjadi moderator ruang di semua kelas; (2) pemilik kelas, yaitu akun yang membuat kelas dengan peran portal apa pun, menjadi moderator ruang hanya di kelasnya sendiri; (3) akun lain yang bukan pemilik kelas dan peserta tamu yang masuk dengan kode akses menjadi peserta ruang; dan (4) izin perekaman hanya diberikan kepada moderator ruang apabila pemilik kelas tersebut memiliki hak perekaman. Aturan (1)–(4) merupakan kebijakan target. Pada penerapan awal (K2), portal masih memberikan klaim moderator ruang kepada setiap akun bermoderator portal tanpa memeriksa kepemilikan kelas. Penyimpangan itu diuji sebagai kasus A19 dan diselaraskan dengan kebijakan target pada K3. Aturan target tersebut dituangkan ke dalam klaim JWT [21] yang ditandatangani oleh portal menggunakan algoritma HMAC SHA-256 (HS256), sebagaimana ditunjukkan pada Tabel 2. Setiap token diterbitkan untuk satu pengguna dan satu ruang sehingga sejalan dengan rekomendasi penggunaan tautan masuk yang unik untuk setiap peserta [2].

Tabel 2 Pemetaan peran dan izin ke dalam klaim JWT

Klaim	Isi	Fungsi otorisasi
iss, aud	huma_meet	Menolak token dari penerbit atau aplikasi lain
exp	Batas waktu tautan kelas (bawaan 4 jam)	Menolak token kedaluwarsa
room	Nama ruang kelas	Membatasi token pada satu ruang
context.user.affiliation	<i>owner</i> (moderator ruang) atau <i>member</i> (peserta ruang)	Menentukan peran ruang
context.user.moderator	true atau false	Penanda peran bagi klien
context.features.recording	true hanya untuk moderator ruang yang memiliki hak perekaman	Izin memulai perekaman
context.features.livestreaming	Sama dengan izin perekaman	Izin siaran langsung

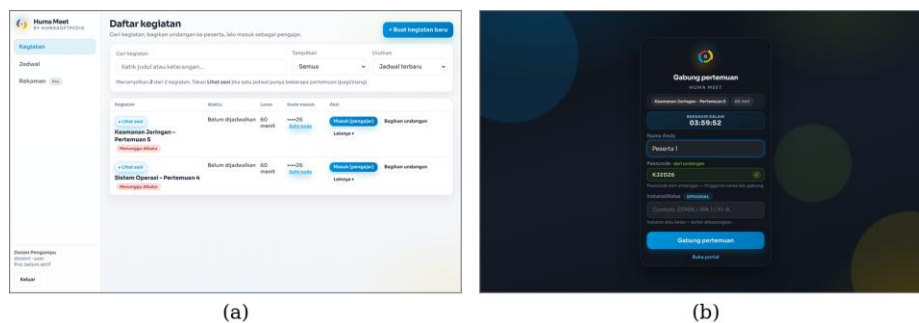
2.4 Penerapan

Jitsi Meet terdiri atas beberapa komponen, yaitu Prosody sebagai server XMPP yang mengelola sesi dan ruang, Jicofo sebagai pengatur konferensi, Jitsi Videobridge sebagai penerus aliran audio dan video, serta Jibri sebagai komponen perekaman dan siaran langsung (*live streaming*). Pada portal, penerbit token pada K3 menetapkan klaim moderator berdasarkan aturan `asModerator = canManageMeeting(user, meeting)`. Aturan ini bernilai benar apabila pengguna merupakan administrator atau pemilik kelas. Pada K2, portal masih memberikan klaim moderator ruang kepada setiap akun bermoderator portal. Pada server Jitsi, konfigurasi yang digunakan adalah `AUTH_TYPE=jwt`, `JWT_ALLOW_EMPTY=0`, `ENABLE_GUESTS=0`, `ENABLE_AUTO_OWNER=0`, `JICOFO_ENABLE_AUTH=0`, `WAIT_FOR_HOST_DISABLE_AUTO_OWNERS=1`, dan `ENABLE_LOBBY=1`. Modul Prosody token `affiliation` membaca klaim afiliasi pada saat peserta akan bergabung, lalu menetapkan afiliasi *owner* (moderator) atau *member* (peserta) sebelum peserta tersebut tampil di dalam ruang. Pada K3, modul filter `iq_jibri` mencocokkan setiap permintaan perekaman dan siaran langsung dengan klaim fitur pada token, lalu menolak permintaan yang tidak diizinkan dengan respons *error auth/forbidden*. Arsitektur penegakan kontrol akses ditunjukkan pada Gambar 2.



Gambar 2 Arsitektur penegakan RBAC berbasis klaim JWT pada Jitsi Meet

Antarmuka portal ditunjukkan pada Gambar 3. Pemilik kelas membuat kelas, menetapkan kode akses, dan membagikan tautan gabung melalui dasbor (Gambar 3a). Peserta membuka tautan tersebut, mengisi nama, lalu portal memeriksa kode akses sebelum menerbitkan token peserta untuk ruang yang dituju (Gambar 3b). Pemilik kelas yang bergabung dari dasbor memperoleh token dengan afiliasi *owner*, sedangkan peserta memperoleh token dengan afiliasi *member*.



Gambar 3 Antarmuka portal: (a) dasbor kelas pemilik dan (b) halaman gabung peserta dengan kode akses

2.5 Lingkungan dan Konfigurasi Uji

Pengujian tidak dilakukan pada server produksi agar kelas yang sedang berlangsung tidak terganggu. Server Jitsi uji dijalankan pada perangkat keras yang sama dengan server produksi, yaitu prosesor Intel Core i7-8700T (6 core, 12 thread), memori 32 GB, dan sistem operasi Synology DSM 7.4.1 dengan Docker. Server uji menggunakan *Docker image* yang sama (stable-

11146-2), tetapi dengan jaringan Docker, *port*, dan kunci rahasia JWT yang berbeda dari server produksi. Portal uji menjalankan salinan kode portal produksi dengan basis data yang terpisah. Klien pengujian berupa *browser* Chrome mode *headless* yang dikendalikan oleh Puppeteer 23.5.3, dan setiap pengguna simulasi dijalankan pada *browser context* yang terpisah. Empat konfigurasi pembandingan disajikan pada Tabel 3. Konfigurasi K0 dan K1 mewakili cara pemasangan Jitsi yang umum digunakan, K2 merupakan model sebelum perbaikan, dan K3 merupakan model setelah perbaikan.

Tabel 3 Konfigurasi pembandingan

Kode	Konfigurasi	Pengaturan utama
K0	Bawaan Jitsi	Tanpa autentikasi; pengguna pertama menjadi moderator ruang
K1	JWT seragam	JWT wajib; autentikasi Jicofo aktif sehingga setiap pengguna terautentikasi menjadi moderator ruang
K2	Model awal	JWT wajib, token <i>affiliation</i> , tanpa tamu, tanpa <i>auto owner</i> , <i>wait for host</i> ; portal sebelum perbaikan
K3	Model setelah perbaikan	K2 ditambah modul filter <i>iq_jibri</i> ; portal setelah perbaikan

Keberhasilan bergabung dibaca dari status aplikasi Jitsi pada *browser*, yaitu status bergabung, peran di dalam ruang, dan pesan *error* koneksi. Sesuai dengan model ancaman, tindakan moderator dikirim melalui API konferensi pada sisi klien (*kickParticipant*, *muteParticipant*, *grantOwner*, *enableLobby*, *end*, dan *startRecording*), lalu hasilnya dinilai dari keadaan ruang sesudahnya, misalnya target keluar dari ruang atau mikrofon target menjadi bisu. Server uji tidak dilengkapi Jibri sehingga hasil permintaan perekaman dinilai dari respons server. Respons *error* not-allowed atau forbidden dicatat sebagai ditolak, sedangkan respons *service-unavailable* (tidak ada Jibri yang tersedia) dicatat sebagai diizinkan karena permintaan tersebut telah lolos pemeriksaan otorisasi.

2.6 Kasus Uji dan Metrik

Ke-30 kasus uji diturunkan secara sistematis dari tiga kategori ancaman pada Subbab 2.2 dan dari aturan RBAC pada Subbab 2.3. Kategori manipulasi token menghasilkan A01 (masuk tanpa token), A02–A08 (tujuh bentuk manipulasi klaim sesuai RFC 8725), dan A09 (permintaan token tanpa kode akses). Kategori penyalahgunaan hak di dalam ruang menghasilkan A10–A16 (tujuh tindakan moderator oleh peserta ruang) serta A17 dan A18 (perolehan peran karena urutan masuk). Kategori penyalahgunaan peran portal menghasilkan A19 (moderator portal pada kelas milik akun lain), A20 (pengguna portal pada kelas milik akun lain), dan A21 (perekaman tanpa izin). Sembilan hak sah (L01–L09) merupakan pasangan positif aturan (1)–(4) sehingga terdapat 21 kasus serangan yang seharusnya ditolak dan 9 kasus hak sah yang seharusnya diizinkan. Setiap konfigurasi diuji sebanyak tiga kali, dan setiap kasus dijalankan pada ruang yang baru. Suatu kasus dinyatakan tidak berlaku apabila mekanisme yang diuji tidak ada pada konfigurasi tersebut. Kasus yang tidak berlaku meliputi A02–A09, A19–A21, L02, dan L09 pada K0 karena konfigurasi ini tidak menggunakan token maupun akun portal, serta kasus pemberian peran A13 dan L06 pada K1 karena target telah menjadi moderator sebelum tindakan dilakukan. Tingkat eskalasi hak (*privilege escalation rate*, E), tingkat penolakan keliru terhadap hak sah (*false denial rate*, FD), dan tingkat kesesuaian terhadap matriks RBAC (*conformance*, C) dihitung menggunakan persamaan (1), (2), dan (3).

$$E = (S_a / N_a) \times 100\% \quad (1)$$

$$FD = (T_l / N_l) \times 100\% \quad (2)$$

$$C = (N_s / N) \times 100\% \quad (3)$$

Pada persamaan tersebut, S_a adalah jumlah serangan yang berhasil, N_a adalah jumlah kasus serangan yang berlaku, T_l adalah jumlah hak sah yang ditolak, N_l adalah jumlah kasus hak sah yang berlaku, N_s adalah jumlah kasus yang hasilnya sesuai dengan harapan, dan N adalah jumlah seluruh kasus yang berlaku. Jumlah kasus yang berlaku berbeda pada setiap konfigurasi. Oleh karena itu, nilai E juga dihitung pada sembilan kasus serangan yang berlaku di keempat

konfigurasi, yaitu A01, A10, A11, A12, A14, A15, A16, A17, dan A18. Skrip pengujian dan berkas hasil uji dalam format JSON dapat diperoleh dari penulis atas permintaan.

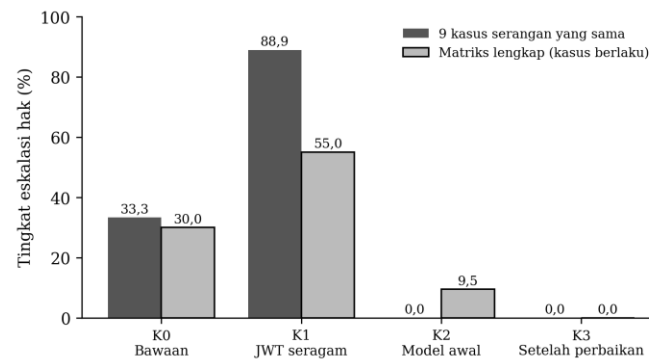
3. HASIL DAN PEMBAHASAN

3.1 Hasil Keseluruhan

Asal-usul ke-30 kasus diuraikan pada Subbab 2.6 sebagai pemetaan dari model ancaman dan aturan RBAC. Pengujian dilaksanakan sebanyak 12 kali (empat konfigurasi dengan tiga ulangan) pada 11 Oktober 2026. Ketiga ulangan pada setiap konfigurasi menghasilkan nilai yang identik sehingga simpangan baku seluruh metrik bernilai 0. Ringkasan hasil pengujian disajikan pada Tabel 4 dan Gambar 4.

Tabel 4 Ringkasan hasil pengujian (tiga ulangan)

Konfigurasi	Kasus berlaku	Serangan berhasil	E (%)	E pada 9 kasus sama (%)	FD (%)	C (%)
K0 Bawaan Jitsi	17	3 dari 10	30,0	33,3	0,0	82,4
K1 JWT seragam	28	11 dari 20	55,0	88,9	0,0	60,7
K2 Model awal	30	2 dari 21	9,5	0,0	0,0	93,3
K3 Model setelah perbaikan	30	0 dari 21	0,0	0,0	0,0	100,0



Gambar 4 Tingkat eskalasi hak pada setiap konfigurasi

Seluruh konfigurasi memberikan hak sah tanpa penolakan keliru ($FD = 0\%$). Dengan demikian, perbedaan tingkat kesesuaian antarkonfigurasi sepenuhnya disebabkan oleh serangan yang berhasil lolos. Hasil pengujian untuk setiap kasus disajikan pada Tabel 5.

Tabel 5 Hasil pengujian setiap kasus (D = ditolak, I = diizinkan, – = tidak berlaku, * = tidak sesuai harapan; kasus dengan hasil identik digabung)

Kasus	Skenario	Harapan	K0	K1	K2	K3
A01	Orang luar masuk ruang tanpa token	D	I*	D	D	D
A02–A08	Manipulasi token: klaim diubah tanpa tanda tangan ulang, algoritma none, kunci lain, token kedaluwarsa, audiens lain, penerbit palsu, dan token ruang lain	D	–	D	D	D
A09	Orang luar meminta token tanpa kode akses	D	–	D	D	D
A10	Peserta mengeluarkan peserta lain	D	D	I*	D	D
A11	Peserta membisukan pemilik kelas	D	D	I*	D	D
A12	Peserta menaikkan perannya menjadi moderator	D	D	I*	D	D
A13	Peserta menjadikan peserta lain moderator	D	D	–	D	D
A14	Peserta mengaktifkan <i>lobby</i>	D	D	I*	D	D
A15	Peserta mengakhiri rapat untuk semua	D	D	I*	D	D
A16	Peserta memulai perekaman	D	D	I*	D	D
A17	Peserta masuk sebelum pemilik lalu menjadi moderator	D	I*	I*	D	D
A18	Peserta menjadi moderator setelah pemilik keluar	D	I*	I*	D	D
A19	Moderator portal meminta token kelas milik pengguna lain	D	–	I*	I*	D
A20	Pengguna biasa meminta token kelas milik pengguna lain	D	–	I*	D	D
A21	Moderator tanpa izin perekaman memulai perekaman	D	–	I*	I*	D
L01	Pemilik menjadi moderator di ruangnya	I	I	I	I	I

Kasus	Skenario	Harapan	K0	K1	K2	K3
L02	Administrator menjadi moderator di semua ruang	I	–	I	I	I
L03	Peserta bergabung dengan kode akses yang benar	I	I	I	I	I
L04, L05, L07, L08	Pemilik mengeluarkan dan membisukan peserta, mengaktifkan <i>lobby</i> , serta mengakhiri rapat	I	I	I	I	I
L06	Pemilik menjadikan peserta moderator	I	I	–	I	I
L09	Pemilik dengan izin perekaman memulai perekaman	I	–	I	I	I

3.2 Konfigurasi Bawaan dan JWT Seragam

Pada konfigurasi K0, siapa pun yang mengetahui nama ruang dapat bergabung (A01), dan peran moderator diberikan kepada pengguna pertama yang masuk ke ruang. Akibatnya, peserta yang masuk sebelum pemilik kelas (A17) atau peserta yang tersisa setelah pemilik keluar (A18) memperoleh peran moderator. Tindakan moderator yang dilakukan oleh peserta (A10–A16) ditolak karena peserta tidak berperan sebagai moderator. Namun, perlindungan ini hanya berlaku selama pemilik kelas masuk lebih dahulu dan tetap berada di dalam ruang.

Konfigurasi K1 menolak akses tanpa token dan seluruh bentuk manipulasi token (A01–A09) sehingga validasi token oleh Prosody telah sesuai dengan praktik terbaik JWT [22]. Namun, K1 menghasilkan tingkat eskalasi tertinggi, yaitu 88,9% pada sembilan kasus yang sama, karena setiap pengguna terautentikasi dijadikan moderator ruang. Akibatnya, peserta dengan token sah dapat mengeluarkan peserta lain, membisukan pemilik kelas, mengaktifkan *lobby*, mengakhiri rapat, dan memulai perekaman (A10–A12 dan A14–A16). Temuan ini menunjukkan bahwa autentikasi JWT tanpa pemetaan peran justru memperluas ancaman orang dalam dibandingkan dengan konfigurasi bawaan. JWT hanya menentukan pihak yang boleh masuk, sedangkan tindakan setelah masuk harus ditentukan oleh klaim peran yang ditegakkan server, sejalan dengan perbedaan autentikasi dan otorisasi oleh Mohamed dkk. [15].

3.3 Model Awal dan Dua Celah yang Ditemukan

Konfigurasi K2 menolak seluruh sembilan kasus serangan yang sama ($E = 0\%$). Modul `token_affiliation` menetapkan peran ruang berdasarkan klaim afiliasi sebelum peserta tampil di dalam ruang sehingga urutan masuk tidak lagi menentukan peran (A17 dan A18 ditolak). Selain itu, penonaktifan fitur *auto owner* mencegah peserta memperoleh peran moderator setelah pemilik keluar. Permintaan perekaman oleh peserta (A16) ditolak oleh Jicofo dengan respons *error not-allowed*.

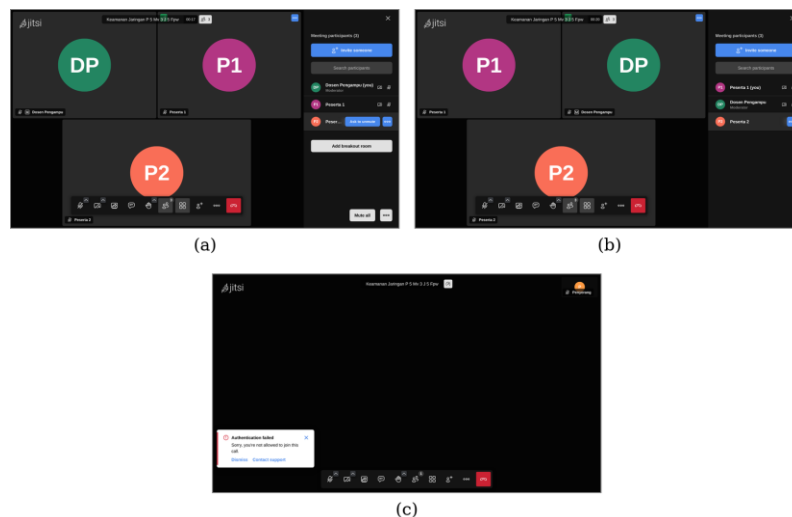
Pada matriks lengkap, K2 masih meloloskan dua serangan ($E = 9,5\%$; $C = 93,3\%$). Celah pertama (A19) terdapat pada portal. Akun moderator portal yang bukan pemilik kelas dapat meminta token untuk kelas milik pengguna lain, menerima token dengan klaim `affiliation=owner`, lalu bergabung sebagai moderator ruang. Penyebabnya adalah aturan lama yang memberikan klaim moderator kepada setiap akun bermoderator portal, bukan hanya kepada pemilik kelas. Celah A19 bukan inkonsistensi kebijakan pada Subbab 2.3, melainkan penyimpangan penerapan awal terhadap kebijakan target tersebut. Kasus A20 menunjukkan bahwa pengguna portal tidak terdampak. Celah ini termasuk *broken access control* karena pengguna sah dapat bertindak atas sumber daya milik pengguna lain [17], [18]. Polanya serupa dengan eskalasi hak melalui manipulasi peran pada LMS yang dilaporkan oleh Muhammad dkk. [34].

Celah kedua (A21) terdapat pada server. Pemilik kelas yang tidak memiliki hak perekaman menerima token dengan klaim `recording=false` dan peran moderator ruang. Ketika fungsi `startRecording` dipanggil melalui *browser console*, Jicofo tetap meneruskan permintaan karena pengirimnya berperan sebagai moderator. Server kemudian memberikan respons *service-unavailable* (tidak ada Jibri yang tersedia), bukan penolakan otorisasi. Pada server yang dilengkapi Jibri, permintaan tersebut berpotensi menghasilkan rekaman karena klaim `features.recording` hanya dipakai antarmuka untuk menyembunyikan tombol perekaman. Temuan ini menegaskan bahwa klaim otorisasi pada token hanya efektif apabila terdapat komponen server yang memeriksanya. Hal ini sesuai dengan ketentuan bahwa penerima token wajib memvalidasi setiap klaim yang digunakan untuk keputusan akses [23].

3.4 Perbaikan dan Hasil Setelah Perbaikan

Pada portal, aturan klaim moderator diubah menjadi `canManageMeeting(user, meeting)` sehingga klaim moderator hanya diberikan kepada administrator atau pemilik kelas. Pada server, modul filter `iq_jibri` ditambahkan ke dalam daftar modul XMPP sehingga Prosody memeriksa klaim fitur perekaman sebelum permintaan diteruskan ke Jicofo. Setelah perbaikan (K3), akun moderator portal yang bukan pemilik kelas menerima token dengan klaim `affiliation=member` dan bergabung sebagai peserta ruang (A19 ditolak). Permintaan perekaman oleh moderator tanpa izin (A21) ditolak oleh Prosody dengan respons `error auth/forbidden`, sedangkan pemilik kelas yang memiliki izin perekaman (L09) tetap diizinkan. Permintaan perekaman oleh peserta (A16), yang pada K2 ditolak oleh Jicofo, kini telah ditolak lebih awal oleh Prosody. Dengan demikian, perekaman dibatasi oleh dua lapis pemeriksaan, yaitu peran ruang dan klaim fitur pada token.

Tampilan ruang konferensi pada K3 ditunjukkan pada Gambar 5. Pemilik kelas ditandai sebagai *Moderator* dan memperoleh kontrol moderasi pada panel peserta, antara lain *Mute all*, *Ask to unmute*, dan *Add breakout room* (Gambar 5a). Peserta melihat pemilik kelas sebagai moderator, tetapi tidak memperoleh kontrol moderasi tersebut (Gambar 5b). Token peserta yang klaim perannya dinaikkan tanpa tanda tangan ulang ditolak dengan pesan *Authentication failed* sehingga pelaku tidak dapat bergabung ke ruang (Gambar 5c). Tampilan antarmuka ini hanya mencerminkan peran yang ditetapkan server. Penolakan terhadap tindakan yang dipanggil langsung melalui *browser console* dibuktikan oleh hasil pengujian pada Tabel 5.



Gambar 5 Tampilan ruang konferensi pada K3: (a) pemilik kelas, (b) peserta, dan (c) token yang dimanipulasi ditolak

Konfigurasi K3 menghasilkan tingkat eskalasi 0%, tingkat penolakan keliru 0%, dan tingkat kesesuaian 100% pada ketiga ulangan. Perbaikan tersebut tidak mengurangi hak sah karena pemilik kelas tetap dapat mengeluarkan dan membisukan peserta, menaikkan peran peserta, mengaktifkan *lobby*, mengakhiri rapat, dan melakukan perekaman apabila memiliki izin (L01–L09). Kedua perbaikan kemudian diterapkan pada server produksi. Pemeriksaan riwayat produksi menunjukkan bahwa seluruh 9 proses perekaman berasal dari pemilik kelas yang memiliki hak perekaman sehingga perbaikan tidak mengganggu perekaman yang sah.

3.5 Perbandingan dengan Penelitian Terdahulu

Penerapan RBAC pada aplikasi web di Indonesia umumnya diuji dengan metode *black-box* [28], [30], [31] atau dengan OWASP ASVS dan pemindaian otomatis [32]. Pengujian tersebut memastikan bahwa menu dan API sesuai dengan peran pengguna, tetapi tidak mencakup tindakan yang dikirim langsung ke *signaling server*. Kasus A10–A12 dan A14–A16 pada K1 serta A21 pada K2 menunjukkan bahwa menyembunyikan tombol pada antarmuka tidak mencegah pemanggilan fungsi secara langsung. Penelitian ini menambahkan kasus serangan dari sisi peserta

sesuai dengan model ancaman orang dalam serta konfigurasi pembandingan yang memisahkan pengaruh autentikasi dari pengaruh pemetaan peran. Hasilnya melengkapi temuan Ling dkk. [2]: token yang unik untuk setiap peserta hanya efektif terhadap orang dalam apabila disertai pembatasan hak di dalam ruang. Dibandingkan dengan pendekatan deteksi [11], [12], [13], penegakan peran pada server mencegah tindakan sebelum tindakan tersebut mengganggu jalannya kelas.

Dari sisi penerapan, model ini tidak memerlukan perubahan kode Jitsi Meet. Penegakan cukup dilakukan melalui pengaturan konfigurasi dan pengaktifan modul Prosody yang telah tersedia dalam distribusi Jitsi Meet, ditambah satu aturan penerbitan klaim pada portal. Oleh karena itu, institusi lain yang mengelola Jitsi Meet dapat menerapkan model yang sama dengan menyesuaikan pemetaan peran pada sistem penerbit tokennya.

4. KESIMPULAN

Berdasarkan hasil pengujian dan pembahasan, kesimpulan penelitian ini adalah sebagai berikut.

1. RBAC berbasis klaim JWT dapat diterapkan pada server Jitsi Meet dengan memetakan peran portal ke dalam klaim afiliasi, izin perekaman, ruang, masa berlaku, penerbit, dan audiens yang ditegakkan oleh server Prosody.
2. Autentikasi JWT seragam mampu menolak seluruh bentuk manipulasi token, tetapi meningkatkan tingkat eskalasi hak menjadi 88,9% pada sembilan kasus serangan yang sama, dibandingkan dengan 33,3% pada konfigurasi bawaan, karena setiap pengguna terautentikasi menjadi moderator ruang.
3. Model awal menurunkan tingkat eskalasi pada sembilan kasus tersebut menjadi 0%, tetapi pada matriks lengkap masih meloloskan 2 dari 21 serangan (9,5%), yaitu perolehan hak moderator lintas kelas oleh akun moderator portal dan klaim izin perekaman yang tidak ditegakkan oleh server.
4. Setelah hak moderator dibatasi pada pemilik kelas dan modul filter_iq_jibri diaktifkan, tingkat eskalasi dan tingkat penolakan keliru menjadi 0%, sedangkan tingkat kesesuaian terhadap matriks RBAC mencapai 100%. Dengan demikian, mitigasi ancaman orang dalam pada kelas daring memerlukan penegakan klaim peran dan izin di server konferensi video, tidak cukup dengan autentikasi atau penyembunyian tombol pada antarmuka.

5. SARAN

Penelitian selanjutnya disarankan untuk menguji pembatasan fitur berbagi layar dan fitur lain yang belum diuji pada lingkungan yang dilengkapi Jibri; mengganti tanda tangan HS256 dengan algoritma kunci publik, seperti RS256, agar Prosody hanya menyimpan kunci verifikasi; menambahkan pencatatan audit untuk setiap penolakan otorisasi di server guna mendeteksi upaya eskalasi hak; dan mengukur pengaruh penegakan peran terhadap waktu bergabung peserta pada kelas dengan jumlah peserta yang lebih besar.

DAFTAR PUSTAKA

- [1] G. Elmer, S. J. Neville, A. Burton, and S. Ward-Kimola, "Zoombombing during a global pandemic," *Social Media + Society*, vol. 7, no. 3, 2021, doi: 10.1177/20563051211035356.
- [2] C. Ling, U. Balci, J. Blackburn, and G. Stringhini, "A first look at zoombombing," in *Proc. 2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 1452–1467, doi: 10.1109/SP40001.2021.00061.
- [3] A. Alammary, M. Alshaikh, and A. R. Pratama, "Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic," *PeerJ Computer Science*, vol. 8, p. e1021, 2022, doi: 10.7717/peerj-cs.1021.

- [4] D. Kagan, G. F. Alpert, and M. Fire, "Zooming into video conferencing privacy," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 1, pp. 933–944, 2024, doi: 10.1109/TCSS.2022.3231987.
- [5] Y. Yang, J. West, G. K. Thiruvathukal, N. Klingensmith, and K. Fawaz, "Are you really muted?: A privacy analysis of mute buttons in video conferencing apps," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, no. 3, pp. 373–393, 2022, doi: 10.56553/popets-2022-0077.
- [6] G. Achilleos, K. Limniotis, and N. Kolokotronis, "Exploring personal data processing in video conferencing apps," *Electronics*, vol. 12, no. 5, p. 1247, 2023, doi: 10.3390/electronics12051247.
- [7] I. B. A. I. Iswara and I. P. P. K. Yasa, "Analisis dan perbandingan quality of service video conference Jitsi dan BigBlueButton pada virtual private server," *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, vol. 4, no. 2, pp. 192–203, 2021, doi: 10.31598/jurnalresistor.v4i2.794.
- [8] Q. Priyadi and L. Lukman, "Uji kualitas video conference Jitsi berbasis container pada Amazon Web Services (AWS)," *Pseudocode*, vol. 10, no. 2, pp. 74–79, 2023, doi: 10.33369/pseudocode.10.2.74-79.
- [9] H. Mahmoud and R. Abozariba, "A systematic review on WebRTC for potential applications and challenges beyond audio video streaming," *Multimedia Tools and Applications*, vol. 84, no. 6, pp. 2909–2946, 2025, doi: 10.1007/s11042-024-20448-9.
- [10] R. A. Alsowail and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," *Electronics*, vol. 10, no. 9, p. 1005, 2021, doi: 10.3390/electronics10091005.
- [11] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," *IEEE Access*, vol. 12, pp. 30907–30927, 2024, doi: 10.1109/ACCESS.2024.3369906.
- [12] M. Mehmood, R. Amin, M. M. A. Muslam, J. Xie, and H. Aldabbas, "Privilege escalation attack detection and mitigation in cloud using machine learning," *IEEE Access*, vol. 11, pp. 46561–46576, 2023, doi: 10.1109/ACCESS.2023.3273895.
- [13] M. Alohal, O. Balogun, and D. Takabi, "Integrating cyber deception into attribute-based access control (ABAC) for insider threat detection," *IEEE Access*, vol. 10, pp. 108965–108978, 2022, doi: 10.1109/ACCESS.2022.3213645.
- [14] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224–274, 2001, doi: 10.1145/501978.501980.
- [15] A. K. Y. S. Mohamed, D. Auer, D. Hofer, and J. Küng, "A systematic literature review for authorization and access control: Definitions, strategies and models," *International Journal of Web Information Systems*, vol. 18, no. 2/3, pp. 156–180, 2022, doi: 10.1108/IJWIS-04-2022-0077.
- [16] W. K. Abdulraheem, E. M. Ibbini, H. Kanaker, S. Smadi, N. A. Karim, H. N. Fakhouri, L. Albdour, and S. Fakhouri, "Least-privilege role-based access control improvement for cloud container security," *Computers*, vol. 15, no. 5, p. 326, 2026, doi: 10.3390/computers15050326.
- [17] A. Anas, S. Elgamal, and B. Youssef, "Survey on detecting and preventing web application broken access control attacks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 1, pp. 772–781, 2024, doi: 10.11591/ijece.v14i1.pp772-781.
- [18] E.-T. EL Ghachi and B. Raouyane, "Web application security: A review of broken access control in web applications," in *Lecture Notes on Data Engineering and Communications Technologies*. Cham, Switzerland: Springer, 2025, pp. 25–34, doi: 10.1007/978-3-031-91351-8_3.
- [19] Abdurasyid, Y. Asnar, and G. A. P. Saptawati, "Mutation based improvement of security test case quality for broken access control," *EURASIP Journal on Information Security*, vol. 2026, no. 1, p. 7, 2026, doi: 10.1186/s13635-026-00226-w.

-
- [20] T. Zhang, F. Hao, Y. Wang, B. Zhang, and G. Xie, “VeriFlow: A framework for the static verification of web application access control via policy-graph consistency,” *Electronics*, vol. 14, no. 18, p. 3742, 2025, doi: 10.3390/electronics14183742.
 - [21] M. Jones, J. Bradley, and N. Sakimura, “JSON Web Token (JWT),” RFC 7519, RFC Editor, 2015, doi: 10.17487/RFC7519.
 - [22] Y. Sheffer, D. Hardt, and M. Jones, “JSON Web Token best current practices,” RFC 8725, RFC Editor, 2020, doi: 10.17487/RFC8725.
 - [23] V. Bertocci, “JSON Web Token (JWT) profile for OAuth 2.0 access tokens,” RFC 9068, RFC Editor, 2021, doi: 10.17487/RFC9068.
 - [24] L. Zhang, C. Zhou, and J. Wen, “APSH-JWT: An authentication protocol based on JWT with scalability and heterogeneity in edge computing,” *Wireless Networks*, vol. 31, no. 3, pp. 2939–2953, 2025, doi: 10.1007/s11276-025-03926-2.
 - [25] A. Venčkauskas, D. Kukta, Š. Grigaliūnas, and R. Brūzgienė, “Enhancing microservices security with token-based access control method,” *Sensors*, vol. 23, no. 6, p. 3363, 2023, doi: 10.3390/s23063363.
 - [26] F. C. Ramdani, A. Rahmatulloh, and R. N. Shofa, “Implementation of JSON web token on authentication with HMAC SHA-256 algorithm,” *Sistemasi: Jurnal Sistem Informasi*, vol. 12, no. 1, pp. 194–205, 2023, doi: 10.32520/stmsi.v12i1.2450.
 - [27] S. Dalimunthe, E. H. Putra, and M. A. F. Ridha, “Restful API security using JSON web token (JWT) with HMAC-Sha512 algorithm in session management,” *IT Journal Research and Development*, vol. 8, no. 1, pp. 81–94, 2023, doi: 10.25299/itjrd.2023.12029.
 - [28] Y. Yuricha and I. K. Phan, “Penerapan role based access control dalam sistem supply chain management berbasis cloud,” *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 3, no. 2, pp. 339–348, 2023, doi: 10.57152/malcom.v3i2.1259.
 - [29] Y. A. Praselia and D. Manongga, “Role-based access control (RBAC) untuk sistem otorisasi terpusat berbasis Flask studi kasus PT. XYZ,” *JIPi (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 4, pp. 1768–1778, 2024, doi: 10.29100/jipi.v9i4.5403.
 - [30] D. Fitrianto and W. Y. Sulisty, “Penerapan role-based access control untuk keamanan data multi-tenant SIMPEL Lazismu,” *Insect (Informatics and Security): Jurnal Teknik Informatika*, vol. 12, no. 1, pp. 1–10, 2026, doi: 10.33506/insect.v12i01.5009.
 - [31] R. Firmansyah, A. Hamdi, and D. Riandini, “Perancangan sistem autentikasi multi-role berbasis RBAC pada platform e-learning pemberdayaan ekonomi perempuan,” *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 11, no. 1, pp. 1094–1104, 2026, doi: 10.36341/rabit.v11i1.7226.
 - [32] I. Gamayanto, M. C. Kurniawan, and G. K. Sanyoto, “Security evaluation of Keycloak-based role-based access control in microservice architectures using the OWASP ASVS framework,” *Journal of Applied Informatics and Computing*, vol. 9, no. 6, pp. 3964–3973, 2025, doi: 10.30871/jaic.v9i6.11604.
 - [33] M. H. Prayitno, A. Hiswara, and J. X. Guterres, “Mitigating access control vulnerabilities through ISO/IEC 27001-based granular role-based access control rights mapping,” *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 25, no. 3, pp. 641–650, 2026, doi: 10.30812/matrik.v25i3.6653.
 - [34] A. Muhammad, A. I. Hadiana, and R. Ilyas, “Eksplorasi broken access control untuk eskalasi hak akses pada LMS Universitas XYZ,” *Jurnal Algoritma*, vol. 22, no. 2, pp. 1–11, 2025, doi: 10.33364/algoritma/v.22-2.2287.
-