JETISH: Journal of Education Technology Information Social Sciences and Health
E-ISSN: 2964-2507 P-ISSN: 2964-819X
Vol. 5 No. 2 September 2026

Analisis Keamanan Login pada Sistem Oracle UIM

Dedy Kiswanto[1] Yesy Simanjuntak[2] Rani Indah Sari[3]
Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan, Kota Medan, Sumatera Utara, Indonesia[1,2,3]
Email: dedykiswanto@mhs.unimed.ac.id[1] yesysmjtk.4233550045@unimed.ac.id[2] rani.4233550011@mhs.unimed.ac.id[3]

Abstrak

Keamanan login merupakan aspek penting dalam sistem informasi karena berfungsi sebagai gerbang utama akses pengguna ke dalam sistem. Pada sistem Oracle Unified Inventory Management (UIM), keamanan akses menjadi sangat penting karena sistem digunakan untuk mengelola data inventaris jaringan yang bersifat kritis. Penelitian ini dilakukan untuk menganalisis mekanisme keamanan login yang diterapkan pada Oracle UIM, mengkaji peran Virtual Private Network (VPN) dalam mendukung keamanan akses, serta mengevaluasi penerapan keamanan berlapis (layered security) pada proses autentikasi pengguna. Metode yang digunakan adalah penelitian kualitatif dengan pendekatan deskriptif melalui observasi dan studi literatur. Metode ini dipilih karena mampu memberikan gambaran mendalam mengenai mekanisme keamanan yang diterapkan tanpa melakukan intervensi terhadap sistem. Hasil penelitian menunjukkan bahwa Oracle UIM telah menerapkan keamanan berlapis melalui penggunaan VPN GlobalProtect dengan Multi-Factor Authentication (MFA), autentikasi berbasis username dan password, penggunaan HTTPS, serta pengelolaan autentikasi melalui WebLogic Server dengan embedded LDAP. Namun, masih ditemukan beberapa kelemahan, seperti tidak diterapkannya MFA pada halaman login Oracle UIM, tidak adanya mekanisme account locking untuk mencegah serangan brute force, belum diterapkannya digest authentication pada web services API, dan penggunaan role default yang belum sepenuhnya menerapkan prinsip least privilege. Berdasarkan hasil tersebut, dapat disimpulkan bahwa keamanan login Oracle UIM telah memenuhi sebagian besar prinsip keamanan informasi, namun masih memerlukan peningkatan pada aspek autentikasi, otorisasi, dan pengendalian akses. Penelitian selanjutnya disarankan melakukan pengujian penetrasi secara langsung serta mengkaji implementasi MFA pada sistem Oracle UIM untuk meningkatkan keamanan akses pengguna.

Kata Kunci: Oracle UIM, keamanan login, VPN, Multi-Factor Authentication (MFA), layered security.

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong berbagai organisasi untuk memanfaatkan sistem informasi dalam mendukung kegiatan operasional dan pengelolaan data. Seiring meningkatnya penggunaan sistem berbasis digital, aspek keamanan menjadi faktor penting yang harus diperhatikan, terutama pada proses login sebagai gerbang utama akses pengguna ke dalam sistem. Mekanisme login berfungsi untuk memverifikasi identitas pengguna agar hanya pihak yang berwenang yang dapat mengakses sistem. Namun, penggunaan metode login yang sederhana masih memiliki berbagai kelemahan, seperti rentan terhadap pencurian kredensial, serangan brute force, maupun akses tidak sah yang dapat mengancam kerahasiaan dan integritas informasi. Oleh karena itu, diperlukan mekanisme keamanan yang mampu melindungi proses login agar lebih aman dan terkontrol. Pada sistem Oracle Unified Inventory Management (UIM), keamanan akses menjadi aspek yang penting karena sistem digunakan untuk mengelola data inventaris jaringan yang bersifat kritis. Berdasarkan hasil observasi, akses ke Oracle UIM dilakukan melalui Virtual Private Network (VPN) sebelum pengguna dapat melakukan proses login ke dalam sistem, sehingga menarik untuk dianalisis dari aspek keamanan yang diterapkan.

Penelitian Terdahulu yang Relavan

Tabel 1. Penelitian Terdahulu

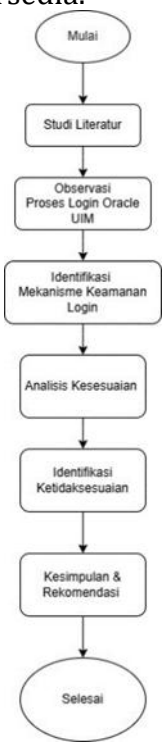
No	Penulis/ Tahun	Judul	Tujuan	Metode	Hasil	Kontribusi dan relevansi
1	Heriyanto, Qalban, & Mukaromah (2022)	Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik	Mengembangkan metode login 2FA untuk meningkatkan keamanan sistem informasi akademik	Prototyping dengan implementasi OTP melalui Telegram dan autentikasi kalkulasi	Metode 2FA mampu meningkatkan keamanan login melalui OTP dan autentikasi tambahan sehingga mempersulit akses oleh pihak yang tidak berwenang	Relevan karena menunjukkan bahwa keamanan login dapat ditingkatkan melalui penerapan autentikasi berlapis (OTP dan verifikasi tambahan)
2	Raffles Agustinus Supit, Yeremia Alfa Susetyo (2026)	Implementasi JWT untuk Autentikasi dan Otorisasi pada Sistem Pembayaran Digital dengan Flask	Meningkatkan keamanan autentikasi dan otorisasi API	Pengembangan sistem berbasis Flask dengan JWT + pengujian black-box, OWASP, dan concurrency	Sistem aman, semua pengujian lulus, JWT valid, dan transaksi tetap konsisten saat beban tinggi	JWT + Flask efektif untuk keamanan API pembayaran digital, meningkatkan kontrol akses dan konsistensi transaksi
3	Sangjaya Megananda, Torang Mogensyah, Nadyfa Ramadhanty, dan Heimemayu Rudiyono (2024)	Integrasi Sistem MRP ke Sistem ERP Oracle pada PT Ultrajaya Milk Industry di Bandung Barat	Menganalisis integrasi MRP ke ERP Oracle pada PT Ultrajaya.	Studi literatur dan analisis data sekunder.	Integrasi ERP Oracle meningkatkan efisiensi operasional, pengelolaan persediaan, dan laba perusahaan.	Menjadi referensi tentang penerapan ERP untuk meningkatkan efektivitas proses bisnis dan kinerja perusahaan manufaktur.
4	Jaelani dkk. (2025)	Pengujian Kerentanan pada Sistem Informasi ABC untuk Peningkatan Keamanan	Mendeteksi celah keamanan sistem.	VA, Penetration Testing, Black Box.	Ditemukan 10 kerentanan, terutama IDOR dan username enumeration.	Menjadi referensi penerapan kontrol akses dan keamanan API pada sistem informasi.
5	Haniwijaya Pahlawansah dkk. (2025))	Analisis Kerentanan Website SMK Muhammadiyah 2 Bontoala Makassar Menggunakan Metode OWASP (Open Web Application Security Project)	Mengidentifikasi dan menganalisis kerentanan keamanan pada website SMK Muhammadiyah 2 Bontoala Makassar berdasarkan standar OWASP Top 10.	OWASP Top 10, Penetration Testing, Black Box Testing, OWASP ZAP.	Ditemukan 5 kerentanan keamanan, terutama Stored XSS, komponen usang, IDOR, misconfiguration, dan brute force login.	Menunjukkan efektivitas OWASP untuk mendeteksi kerentanan website dan memberikan rekomendasi peningkatan keamanan sistem.

6	Raffles Agustinus Supit, Yeremia Alfa Susetyo (2026)	Implementasi JSON Web Token untuk Autentikasi dan Otorisasi pada Sistem Pembayaran Digital Menggunakan Framework Flask	Meningkatkan keamanan autentikasi dan otorisasi pada sistem pembayaran digital.	Implementasi JWT pada API menggunakan framework Flask, pengujian black-box, keamanan API, dan concurrency.	JWT berhasil diterapkan, seluruh pengujian keamanan dan transaksi lulus, serta konsistensi data tetap terjaga.	Menunjukkan JWT dan Flask efektif meningkatkan keamanan akses API pada sistem pembayaran digital
7	Febri Dolis Herdiani (2021)	Penerapan Oracle Enterprise Architecture Development (OADP) Dalam Perancangan Arsitektur Sistem Informasi Manajemen Aset Properti: Studi Kasus PT. Pos Properti Indonesia	Merancang arsitektur sistem informasi manajemen aset properti yang terintegrasi.	Oracle Architecture Development Process (OADP), observasi, wawancara, studi pustaka.	Menghasilkan blueprint enterprise architecture berupa business context, architecture vision, current state, future state, roadmap, dan governance.	Menunjukkan bahwa metode OADP dapat digunakan sebagai dasar perancangan sistem informasi terintegrasi untuk mendukung pengelolaan aset perusahaan secara lebih efektif.

Berdasarkan penelitian terdahulu pada tabel 1, keamanan login merupakan salah satu aspek penting dalam perlindungan sistem informasi. Berbagai penelitian menyatakan bahwa penerapan autentikasi dan otorisasi yang mampu meningkatkan keamanan akses pengguna. Selain itu, penggunaan teknologi tambahan seperti Virtual Private Network (VPN), Multi-Factor Authentication (MFA), dan One-Time Password (OTP) terbukti dapat memperkuat perlindungan terhadap akses tidak sah. Hasil penelitian tersebut menunjukkan bahwa keamanan sistem tidak hanya bergantung pada penggunaan username dan password, tetapi juga memerlukan lapisan keamanan tambahan untuk mengurangi risiko serangan siber. Meskipun penelitian sebelumnya telah membahas keamanan login, autentikasi, otorisasi, VPN, dan MFA secara terpisah, sebagian besar penelitian masih berfokus pada implementasi teknologi keamanan pada sistem informasi secara umum. Belum banyak penelitian yang mengkaji bagaimana kombinasi berbagai mekanisme keamanan tersebut diterapkan secara bersamaan pada sistem Oracle Unified Inventory Management (UIM). Selain itu, masih terbatas penelitian yang menganalisis proses login Oracle UIM dari perspektif keamanan berlapis (layered security) yang melibatkan VPN, autentikasi pengguna, captcha, dan kode verifikasi (OTP) sebagai satu kesatuan mekanisme pengamanan akses sistem. Kebaruan penelitian ini terletak pada analisis keamanan login pada sistem Oracle UIM dengan meninjau penerapan keamanan berlapis yang terdiri dari penggunaan VPN, autentikasi pengguna, captcha, dan kode verifikasi (OTP). Dengan demikian, penelitian ini diharapkan dapat memberikan gambaran mengenai kontribusi setiap lapisan keamanan dalam melindungi akses pengguna terhadap sistem Oracle UIM. Berdasarkan hal tersebut, penelitian ini bertujuan untuk menganalisis mekanisme keamanan login yang diterapkan pada sistem Oracle UIM, mengkaji peran VPN dalam mendukung keamanan akses sistem, serta mengevaluasi penerapan keamanan berlapis yang digunakan untuk melindungi proses autentikasi pengguna.

METODE PENELITIAN

1. Jenis Penelitian. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif. Penelitian ini bertujuan untuk menganalisis mekanisme keamanan login pada sistem Oracle UIM yang meliputi akses melalui VPN, proses autentikasi pengguna, serta penerapan mekanisme keamanan tambahan seperti OTP dan layered security.
2. Lokasi dan Objek Penelitian. Penelitian ini dilakukan pada sistem informasi berbasis Oracle UIM ialah mekanisme login pengguna, termasuk proses autentikasi dan sistem keamanan yang diterapkan.
3. Metode Pengumpulan Data. Pengumpulan data dilakukan melalui observasi dan studi literatur. Observasi dilakukan dengan mengamati langsung proses login pada sistem Oracle UIM, mulai dari akses VPN hingga autentikasi pengguna. Studi literatur dilakukan dengan mengkaji jurnal, buku, dan referensi ilmiah terkait keamanan sistem informasi, autentikasi, dan keamanan jaringan.
4. Teknik Analisis Data. Data dianalisis menggunakan metode deskriptif dengan membandingkan hasil observasi dengan teori keamanan sistem informasi seperti CIA Triad, authentication, VPN security, dan layered security. Analisis dilakukan untuk mengidentifikasi tingkat keamanan dan potensi kerentanan sistem login.
5. Indikator Analisis. Indikator yang digunakan meliputi mekanisme autentikasi, penggunaan VPN, penerapan OTP/MFA, serta potensi risiko keamanan seperti brute force dan akses tidak sah.
6. Alur Penelitian. Alur penelitian pada Gambar 1 merupakan tahapan yang dilakukan dalam menganalisis keamanan login pada sistem Oracle UIM. Tahapan penelitian diawali dengan studi literatur untuk mengumpulkan referensi terkait keamanan sistem informasi, autentikasi, VPN, dan konsep layered security. Selanjutnya dilakukan observasi terhadap sistem login Oracle UIM, khususnya pada proses akses melalui VPN dan mekanisme autentikasi pengguna. Setelah itu, dilakukan identifikasi terhadap mekanisme keamanan yang digunakan dalam sistem tersebut, seperti penggunaan username dan password, VPN, serta penerapan OTP atau MFA jika tersedia.

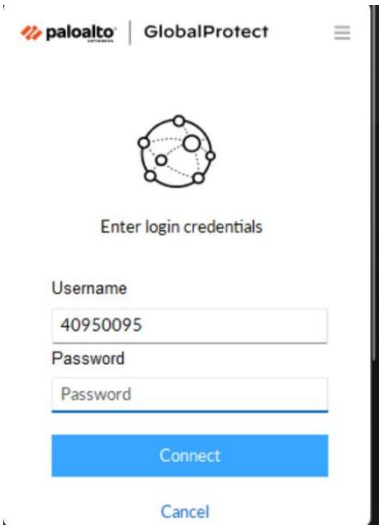


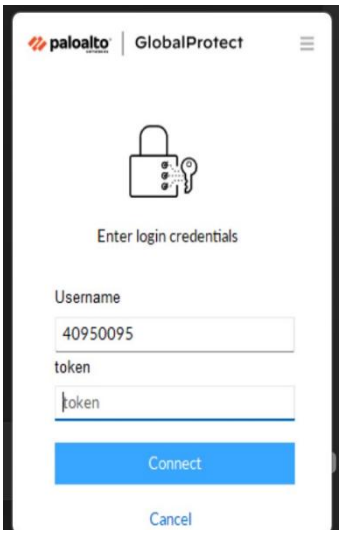
Gambar 1. Flowchart Alur Penelitian

HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian

Penelitian ini dilakukan pada sistem Oracle Unified Inventory Management (UIM) yang digunakan di lingkungan perusahaan. Berdasarkan hasil observasi, proses login pada sistem Oracle UIM diawali dengan akses melalui VPN GlobalProtect dari Palo Alto Networks. Proses akses VPN terdiri dari dua tahap autentikasi. Pada tahap pertama, pengguna memasukkan username dan password seperti pada Gambar 1. Setelah kredensial tersebut diverifikasi, sistem meminta token OTP sebagai autentikasi kedua seperti pada Gambar 2.





Gambar 2. Tampilan Login VPN Global Protect Tahap 1 (Username dan Password)

Gambar 3. Tampilan Login VPN GlobalProtect Tahap 2 (Token/OTP)

Setelah berhasil melewati VPN, pengguna mengakses halaman login Oracle UIM seperti pada Gambar 3. Sistem menerapkan autentikasi berbasis username dan password. Halaman login tidak mengizinkan auto-completion, password ditampilkan dalam bentuk masked input, dan jika kredensial salah, sistem menampilkan pesan "Invalid Credentials".

Gambar 4. Tampilan Halaman Login Oracle

Setelah pengguna berhasil login, sistem menampilkan dashboard utama Oracle UIM seperti pada Gambar 4. Dashboard menampilkan berbagai menu yang dapat diakses berdasarkan role pengguna, antara lain Tasks, Services, Inventory, Work Management, Service Management, dan NFV Orchestration.

Gambar 5. Tampilan Halaman Dashboard

Berdasarkan hasil observasi dan wawancara dengan system administrator, mekanisme keamanan login yang diterapkan pada Oracle UIM dapat dilihat pada Tabel 1.

Tabel 1. Identifikasi Mekanisme Keamanan Login pada Oracle UIM

No	Mekanisme Keamanan	Diterapkan	Keterangan
1	Username & Password	Ya	Dikelola WebLogic Server dengan embedded LDAP
2	VPN	Ya	Palo Alto GlobalProtect dengan MFA
3	MFA pada VPN	Ya	Token OTP setelah username dan password
4	MFA pada Oracle UIM	Tidak	Hanya username dan password
5	Single Sign-On (SSO)	Tidak	Belum diterapkan
6	Session Timeout	Ya	30 menit (default)
7	HTTPS untuk Login	Ya	Menggunakan kanal HTTPS
8	Digest Authentication	Tidak	Belum diterapkan untuk web services API

Pembahasan

Hasil penelitian menunjukkan bahwa sistem Oracle UIM menerapkan autentikasi berbasis username dan password yang dikelola melalui WebLogic Server dengan embedded LDAP. WebLogic Server menggunakan JAAS (Java Authentication and Authorization Service) sebagai framework standar untuk autentikasi dan Principal Validation Provider untuk perlindungan tambahan terhadap serangan CSRF. Hal ini sesuai dengan dokumentasi Oracle UIM Security Guide yang menyatakan bahwa autentikasi pada Oracle UIM dikelola secara eksternal melalui WebLogic Server. Hal ini juga diperkuat oleh penelitian Adicandra et al. (2026) yang menyatakan bahwa autentikasi merupakan proses verifikasi identitas pengguna sebelum diberikan akses ke dalam sistem, dan otorisasi merupakan proses penentuan hak akses pengguna setelah autentikasi berhasil dilakukan.

Penelitian ini menemukan bahwa akses ke Oracle UIM dilindungi oleh VPN GlobalProtect yang menerapkan Multi-Factor Authentication (MFA) berupa token OTP setelah username dan password. Temuan ini menunjukkan bahwa organisasi telah menerapkan konsep layered security atau defense in depth, di mana lapisan keamanan pertama (VPN dengan MFA) melindungi akses ke sistem Oracle UIM yang berada di jaringan internal. Hal ini sejalan dengan penelitian Heriyanto et al. (2022) yang menyatakan bahwa metode keamanan two-factor authentication (2FA) diusulkan untuk mengatasi isu penanggulangan sisi server untuk mencegah pencurian kata sandi. Penelitian tersebut juga menegaskan bahwa model perlindungan keamanan berlapis dapat meminimalisir akses orang yang tidak memiliki wewenang terhadap akun pengguna. Namun, berbeda dengan penelitian Heriyanto et al. (2022) yang menerapkan 2FA pada sistem utama dengan kolaborasi bot Telegram untuk

pengiriman kode OTP dan autentikasi kalkulasi, pada penelitian ini MFA hanya ditemukan pada lapisan VPN dan tidak diterapkan pada halaman login Oracle UIM.

Berdasarkan analisis kesesuaian dengan prinsip CIA Triad, aspek confidentiality sudah cukup baik karena password disimpan di embedded LDAP WebLogic Server dengan kebijakan minimal 8 karakter dan kombinasi alfanumerik, proses login menggunakan kanal HTTPS, dan REST API menggunakan token header. Namun, web services API belum menerapkan digest authentication sehingga berpotensi mengirimkan password dalam bentuk cleartext jika menggunakan HTTP. Oracle merekomendasikan penggunaan digest authentication untuk menghindari pengiriman password dalam bentuk cleartext pada web services over HTTP. Temuan ini sejalan dengan penelitian Pahlawansah et al. (2025) yang mengidentifikasi bahwa kelemahan konfigurasi keamanan seperti pesan error yang terlalu detail dapat membocorkan informasi internal aplikasi dan mempermudah penemuan celah lain. Penelitian tersebut juga menekankan bahwa komponen usang dan kesalahan konfigurasi menciptakan permukaan serangan yang terus meluas seiring waktu. Aspek integrity pada sistem ini tergolong baik karena WebLogic Server menggunakan JAAS sebagai framework standar untuk autentikasi dan Principal Validation Provider yang memberikan perlindungan tambahan terhadap serangan CSRF. Hal ini sejalan dengan temuan dari penelitian Supit dan Susetyo (2026) yang menyatakan bahwa penggunaan token dengan algoritma HMAC SHA-256 memberikan kejelasan mengenai hak akses pengguna, yang secara efektif menutup celah keamanan yang rentan terhadap eksploitasi oleh pihak yang tidak berwenang. Penelitian tersebut juga membuktikan bahwa mekanisme validasi token yang konsisten dengan teori bahwa sistem yang memanfaatkan klaim terstruktur dan verifikasi kriptografi dapat mengurangi peluang penyalahgunaan token dan akses ilegal.

Aspek availability ditemukan memiliki kelemahan pada tidak adanya account locking setelah percobaan login gagal. WebLogic Server sebenarnya menyediakan fitur User Lockouts yang dapat dikonfigurasi untuk membatasi jumlah percobaan login gagal sebelum akun dikunci. Namun, berdasarkan informasi dari system administrator, fitur ini belum diaktifkan. Kondisi ini meningkatkan risiko serangan brute force. Penelitian Jaelani et al. (2025) menemukan bahwa kerentanan username enumeration pada halaman login terjadi ketika sistem memberikan respons yang berbeda antara kesalahan kredensial akibat kata sandi yang tidak sesuai dan kondisi akun yang tidak terdaftar. Perbedaan respons tersebut mengindikasikan bahwa sistem secara tidak langsung mengungkapkan keberadaan username yang valid dalam basis data, sehingga berpotensi dimanfaatkan untuk mendukung serangan brute force. Penelitian tersebut merekomendasikan penerapan rate limiting untuk membatasi jumlah percobaan login yang dapat dilakukan dalam rentang waktu tertentu, serta penggunaan pesan kesalahan yang sama untuk semua kasus agar tidak mengungkapkan apakah username atau password yang salah.

Temuan penting lainnya adalah tidak diterapkannya MFA pada halaman login Oracle UIM, meskipun MFA telah diterapkan pada VPN. Penelitian Pahlawansah et al. (2025) menunjukkan bahwa halaman administrator yang tidak memiliki proteksi terhadap serangan brute-force menjadi target terbuka untuk serangan tebak kata sandi otomatis. Penelitian tersebut juga menegaskan bahwa tanpa mekanisme rate limiting atau penguncian akun, keberhasilan serangan brute force seringkali hanya masalah waktu. Penelitian Heriyanto et al. (2022) menambahkan bahwa autentikasi kalkulasi merupakan bagian penting yang tak terpisahkan dalam pengembangan metode 2FA untuk menghindari serangan bruteforce yang sering terjadi terhadap sistem informasi. Hasil penelitian ini berbeda dengan temuan Megananda et al. (2024) yang menemukan bahwa implementasi ERP Oracle di PT Ultrajaya berhasil meningkatkan efisiensi operasional dan analisis data secara real-time, namun belum secara

spesifik membahas penerapan MFA pada sistem utama. Role default uimuser pada Oracle UIM memberikan akses super user ke semua halaman dan aksi. Berdasarkan dokumentasi Oracle, peran ini sebaiknya tidak diberikan kepada semua pengguna karena risikonya yang tinggi. Penelitian Jaelani et al. (2025) menemukan bahwa kerentanan Insecure Direct Object Reference (IDOR) memungkinkan pengguna yang telah terautentikasi untuk mengakses atau memodifikasi data yang bukan menjadi kewenangannya hanya dengan memanipulasi parameter permintaan. Hal ini sejalan dengan temuan Adicandra et al. (2026) yang menyatakan bahwa Role-Based Access Control (RBAC) mendukung prinsip keamanan least privilege, di mana pengguna hanya diberikan akses sesuai kebutuhan, sehingga dapat meminimalkan risiko penyalahgunaan sistem. Penelitian tersebut juga menekankan bahwa RBAC mempermudah pengelolaan hak akses tanpa perlu konfigurasi kompleks dan mendukung pengembangan sistem yang lebih scalable. Temuan pada penelitian ini menunjukkan bahwa prinsip least privilege belum sepenuhnya diterapkan.

Session timeout pada sistem ini dikonfigurasi selama 30 menit (default). Penelitian Adicandra et al. (2026) menyatakan bahwa session digunakan untuk menjaga status autentikasi pengguna selama berinteraksi dengan sistem, memberikan efisiensi karena pengguna tidak perlu melakukan login ulang pada setiap permintaan akses. Namun, sistem juga harus memastikan bahwa session dikelola dengan aman untuk mencegah serangan seperti session hijacking. Penelitian Supit dan Susetyo (2026) menambahkan bahwa pengujian keamanan API berdasarkan standar OWASP menunjukkan bahwa sistem mampu menangani berbagai potensi kerentanan dengan penerapan rate limiting yang efektif dan validasi input yang benar. Berdasarkan temuan dan analisis yang telah dilakukan, terdapat beberapa kebaruan yang dihasilkan dari penelitian ini. Secara teoritis, penelitian ini memperkaya literatur mengenai analisis keamanan login pada sistem Oracle UIM yang masih terbatas, khususnya dalam konteks penerapan layered security melalui VPN dengan MFA. Secara praktis, penelitian ini memberikan rekomendasi perbaikan yang spesifik bagi organisasi yang menggunakan Oracle UIM, terutama pada aspek penerapan MFA pada sistem utama, pengaktifan account locking untuk mencegah brute force, penerapan digest authentication untuk web services API, serta penerapan RBAC dan prinsip least privilege dalam pengelolaan role pengguna. Rekomendasi ini sejalan dengan penelitian Pahlawansah et al. (2025) yang menekankan bahwa keamanan siber harus dipandang sebagai elemen fundamental dari manajemen risiko institusi, bukan sekadar tugas teknis departemen IT.

KESIMPULAN

Berdasarkan hasil observasi dan analisis pada sistem Oracle UIM, penelitian ini menyimpulkan bahwa mekanisme keamanan login yang diterapkan masih memiliki beberapa kelemahan. Sistem telah menerapkan autentikasi berbasis username dan password melalui WebLogic Server dengan embedded LDAP serta didukung VPN GlobalProtect dengan MFA sebagai lapisan pertama. Namun, MFA tidak diterapkan pada halaman login Oracle UIM, tidak ada mekanisme account locking untuk mencegah brute force, web services API belum menerapkan digest authentication, dan role uimuser memberikan akses super user yang bertentangan dengan prinsip least privilege. Penelitian ini menghasilkan model analisis keamanan login pada Oracle UIM yang mencakup enam lapisan keamanan yaitu jaringan, autentikasi, transmisi data, manajemen sesi, otorisasi, dan audit logging. Penelitian memiliki keterbatasan karena hanya berfokus pada aspek login dan belum melakukan pengujian penetrasi. Penelitian selanjutnya disarankan melakukan pengujian penetrasi langsung, memperluas cakupan analisis, dan mengimplementasikan MFA pada Oracle UIM.

DAFTAR PUSTAKA

Adicandra, E., Yulindon, Dewi, R., & Rifka, S. (2026). Implementasi Autentikasi dan Otorisasi pada Sistem Informasi Berbasis Web. JIPM (Jurnal Ilmiah Pendidikan dan Manajemen), 4(2), 289-298.

Herdiani, F.D. (2021). Penerapan Oracle Enterprise Architecture Development (OADP) Dalam Perancangan Arsitektur Sistem Informasi Manajemen Aset Properti: Studi Kasus PT. Pos Properti Indonesia. Jurnal Ilmiah Ilmu Terapan Universitas Jambi, 5(1), 31-36.

Heriyanto, Y., Qalban, A.A., & Mukaromah, I.A. (2022). Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik. Journal of Innovation Information Technology and Application (JINITA), 4(2), 142-150. doi.org/10.35970/jinita.v4i2.1637

Jaelani, W.L., Primianjani, Y.A., Fathulloh, M.I., Monellia, I., Diputra, A.I.E., & Khilaq, A.R. (2025). Pengujian Kerentanan pada Sistem Informasi ABC untuk Peningkatan Keamanan. NARATIF: Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika, 7(2), 154-162.

Megananda, S., Mogensyah, T., Ramadhanty, N., & Rudiyono, H. (2024). Integrasi Sistem MRP ke Sistem ERP Oracle pada PT Ultrajaya Milk Industry di Bandung Barat. PENG: Jurnal Ekonomi dan Manajemen, 2(1b), 1909-1922. doi.org/10.62710/j1rpnr03

Pahlawansah, H., Basmar, M.F., & Yusuf, M. (2025). Analisis Kerentanan Website SMK Muhammadiyah 2 Bontoala Makassar Menggunakan Metode OWASP (Open Web Application Security Project). BIOS: Jurnal Teknologi Informasi dan Rekayasa Komputer, 6(2), 92-99. doi.org/10.37148/bios.v6i2.180

Supit, R.A., & Susetyo, Y.A. (2026). Implementasi JSON Web Token untuk Autentikasi dan Otorisasi pada Sistem Pembayaran Digital Menggunakan Framework Flask. JATI (Jurnal Mahasiswa Teknik Informatika), 10(3), 5188-5194.