International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 8382-8389
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Geographic Access Audit Dashboard: Monitoring Oracle HCM Cloud Authentication Events via RESTful API Integration

Manivannan Ramar*

MSG Entertainment Holdings, LLC, USA
* **Corresponding Author Email:** manivannanramars@gmail.com- **ORCID** 0000-0002-5247-8850

:

Article Info:

DOI: 10.22399/ijcesen.4230
Received : 22 September 2025
Accepted : 01 November 2025

Keywords

Oracle HCM Cloud,
RESTful API Integration,
Access Auditing,
Oracle Integration Cloud,
Security Monitoring

Abstract:

Cloud-based human capital management systems have revolutionized workforce data management while simultaneously introducing complex security challenges that extend beyond traditional perimeter-based protection models. This article presents a comprehensive framework for implementing external access auditing capabilities for Oracle HCM Cloud through RESTful API integration with Oracle Access Management. The article examines Oracle HCM Cloud's multi-layered security architecture, including role-based access controls, job-level privileges, and data-level security mechanisms, while analyzing the strategic trade-offs between restrictive IP whitelisting approaches and comprehensive audit logging methodologies. A detailed technical specification of the two-tier audit data extraction process is provided, demonstrating how statistical count retrieval followed by paginated event data collection optimizes bandwidth utilization and processing efficiency. The article evaluates Oracle Integration Cloud as an enterprise-grade middleware orchestration platform, comparing its capabilities with those of alternative tools and justifying its selection for mission-critical automation workflows. Implementation best practices are established for scheduling automated data collection cycles, designing dimensional data warehouse schemas to support temporal and geospatial analysis, and developing visualization dashboards that enable anomaly detection and compliance reporting. The integration of audit data with security information and event management systems is discussed as a mechanism for elevating isolated access logs into comprehensive security intelligence. This framework enables organizations to maintain visibility into geographic and temporal access patterns occurring outside native application boundaries, supporting proactive threat detection, forensic investigation capabilities, and regulatory compliance requirements in distributed enterprise environments.

1. Introduction

Cloud-based human capital management systems have fundamentally transformed how organizations manage their workforce data, enabling unprecedented accessibility and operational efficiency across geographically distributed enterprises. Oracle HCM Cloud represents a comprehensive suite of applications that centralizes employee information, payroll records, talent management processes, and sensitive demographic data within a unified cloud infrastructure. As organizations increasingly migrate critical HR functions to cloud platforms, the imperative to maintain robust security postures has intensified proportionally. The transition from on-premises data centers to cloud environments introduces a paradigm shift in security considerations, particularly concerning access control, data sovereignty, and audit trail maintenance [1].The storage of sensitive demographic data in cloud environments presents multifaceted security challenges that extend beyond conventional IT security frameworks. Employee records typically contain personally identifiable information, including social security numbers, financial account details, health insurance information, performance evaluations, and compensation structures. The aggregation of such sensitive data creates high-value targets for malicious actors, necessitating comprehensive security architectures that address both internal and external threat vectors. Traditional perimeter-based security models, which operated on the assumption of trusted internal networks and

untrusted external networks, prove insufficient in cloud contexts where the perimeter becomes nebulous and access patterns are inherently distributed. The conventional castle-and-moat approach fails to account for legitimate access requirements from mobile devices, remote work locations, third-party integrators, and global business operations that characterize modern enterprise environments.Oracle HCM Cloud incorporates sophisticated native security features designed to protect data integrity and confidentiality at multiple layers. The platform implements granular role-based access controls that enable organizations to define precise permissions at the job function level, ensuring users access only information pertinent to their responsibilities. Data-level security mechanisms further restrict visibility based on organizational hierarchies, geographic regions, or custom-defined segments. Authentication protocols leverage industry-standard frameworks, including Security Assertion Markup Language and OAuth implementations, to verify user identities. Additionally, the platform provides encryption for data at rest and in transit, alongside comprehensive audit logging capabilities that track user activities within the application boundary [2].Despite these robust internal security controls, organizations require visibility into access patterns that occur outside the application's operational perimeter. Understanding the geographic origins of authentication attempts, temporal patterns of system access, and correlations between unusual access behaviors and potential security incidents becomes essential for comprehensive security monitoring. While Oracle HCM Cloud secures data within its architectural boundaries, supplementing these controls with external access monitoring provides an additional defensive layer. This approach enables security teams to detect anomalous authentication patterns, identify potential unauthorized access attempts from unexpected geographic locations, and maintain detailed forensic trails for compliance and incident response purposes. The integration of external audit data collection through RESTful API interfaces represents a pragmatic strategy for extending visibility beyond native application controls, facilitating proactive threat detection, and supporting regulatory compliance requirements in increasingly complex digital environments.

2. Access Control Paradigms in Cloud HCM Systems

Oracle HCM Cloud's security architecture fundamentally relies on role-based access control as its primary authorization mechanism, representing a mature implementation of the principle of least privilege. The RBAC framework operates through a hierarchical structure where roles aggregate specific privileges, and these roles are subsequently assigned to users based on their job functions and organizational responsibilities. Each role encapsulates a collection of function security privileges and data security policies that collectively define what actions a user can perform and what information they can access. The granularity of Oracle's RBAC implementation extends to individual page components, enabling administrators to control visibility and editability of specific fields within user interfaces. This fine-grained control mechanism ensures that sensitive information such as compensation details, disciplinary records, or confidential performance and assessments remains accessible only to authorized personnel with legitimate business needs [3].Job-level privileges in Oracle HCM Cloud provide an additional dimension of access control that intersects with traditional role assignments. These privileges enable organizations to define access permissions based on employment attributes, including job codes, positions within organizational hierarchies, departments, legal entities, and geographic locations. The job-level security model becomes particularly valuable in multinational organizations where regulatory requirements mandate strict data residency and access restrictions. For instance, European operations subject to General Data Protection Regulation requirements can be isolated from access by personnel in other jurisdictions unless explicit business justification exists. Data-level security mechanisms further refine access boundaries by implementing row-level and column-level restrictions within database structures. Security profiles can be configured to filter data based on complex criteria, including reporting relationships, cost center affiliations, union membership status, or custom-defined attributes. This multi-layered security approach ensures that even users sharing common functional roles may encounter different data sets based on their specific organizational context and responsibilities.The comparison between IP whitelisting and comprehensive audit logging represents a fundamental strategic choice in cloud security architectures. IP whitelisting operates as a preventive control that restricts application access exclusively to predetermined network addresses, effectively creating a digital perimeter around the cloud application. This approach offers simplicity and provides strong assurance that access originates only from known locations, making it suitable for organizations with centralized operations and limited remote work

requirements. However, IP whitelisting introduces significant operational constraints in contemporary business environments characterized by mobile workforces, mergers and acquisitions, temporary workers, and third-party service providers requiring system access. Comprehensive audit logging, conversely, functions as a detective control that permits broader access while maintaining detailed forensic trails of all authentication attempts and system interactions [4].The trade-offs between restrictive access policies and business flexibility manifest most acutely in distributed work environments where employees, contractors, and business partners require system access from diverse geographic locations and network contexts. Overly restrictive policies may impede legitimate business operations, forcing users to adopt workarounds that potentially introduce greater security risks. Conversely, permissive access policies increase the attack surface and complicate threat detection efforts. Organizations must carefully calibrate their security postures to balance risk mitigation with operational requirements, often implementing layered approaches that combine preventive controls for high-sensitivity functions with detective controls and behavioral analytics for routine operations.

3. RESTful API-Based Audit Data Extraction

Oracle Access Management provides a comprehensive RESTful API framework designed to facilitate programmatic access to authentication and authorization audit data through standardized HTTP methods and JSON-formatted responses. The OAM REST API architecture adheres to contemporary web service design principles, implementing resource-oriented endpoints that expose audit events, statistical summaries, and configuration metadata through intuitive URI structures. The audit data retrieval endpoints specifically target the extraction of authentication events, session management activities, and access policy evaluations that occur at the perimeter of Oracle HCM Cloud instances. These APIs serve as critical integration points for security information and event management systems, enabling organizations to consolidate access logs from multiple cloud applications into centralized monitoring platforms. The technical implementation leverages OAuth authentication protocols to ensure that only authorized clients can retrieve sensitive audit information, maintaining the confidentiality and integrity of security-relevant data throughout the extraction process [5].The two-tier query approach represents an optimized strategy for managing large-volume audit data extraction while minimizing network overhead and processing latency. The initial tier involves invoking a statistical summary endpoint that returns aggregate metadata about available audit records within a specified temporal window. This preliminary query provides essential planning information, including the total count of events matching the filter criteria, enabling client applications to allocate appropriate resources and implement effective pagination strategies before requesting the actual event data. The statistical endpoint accepts temporal boundary parameters defining the audit window of interest and returns counts without transferring the complete event payloads, significantly reducing bandwidth consumption during the discovery phase. Following the statistical assessment, the second tier executes detailed event retrieval requests that return comprehensive audit records, including timestamps, source IP addresses, authentication methods, user identities, session identifiers, and outcome status codes. This bifurcated approach proves particularly valuable when dealing with high-traffic environments where audit repositories accumulate substantial event volumes over relatively short timeframes.Query parameters within the OAM audit API provide flexible filtering and pagination capabilities essential for managing distributed data retrieval operations. The temporal parameters utilize ISO standard timestamp formatting with timezone specifications to ensure unambiguous interpretation across geographically distributed systems. The fromDate and toDate parameters establish inclusive boundaries that define the audit window, supporting precision down to millisecond granularity to accommodate high-frequency access patterns in enterprise environments. Pagination mechanisms employ a combination of page number identifiers and page size limits to enable controlled traversal through large result sets without overwhelming client systems or network infrastructure. The pageSize parameter allows clients to specify the maximum number of records returned in a single response, enabling adaptive strategies that balance throughput optimization with memory constraints. Authentication requirements for these API endpoints mandate the presentation of valid bearer tokens obtained through OAuth client credential flows, ensuring that audit data access is restricted to properly authenticated and authorized integration platforms [6].The timestamp formatting conventions employed by OAM audit APIs conform to RFC standards for Internet date and time representation, utilizing UTC-based timestamps to eliminate ambiguities associated with local timezone conversions and daylight saving

time transitions. This standardization proves critical for correlating events across geographically distributed systems and ensuring accurate temporal sequencing in forensic investigations. The pagination strategies must account for potential data insertions occurring during multi-page retrieval operations, implementing consistent snapshot isolation or cursor-based pagination to prevent data inconsistencies that could compromise audit trail completeness.

4. Integration Architecture and Automation Framework

Oracle Integration Cloud emerges as a comprehensive middleware orchestration platform specifically architected to address enterprise-grade integration requirements through a unified cloud-native environment. OIC provides a declarative integration development paradigm that abstracts the complexities of network protocols, data format conversions, error handling mechanisms, and transaction management from integration developers. The platform's architecture encompasses pre-built adapters for numerous enterprise applications, native support for REST and SOAP web services, sophisticated data mapping capabilities through visual transformation designers, and robust process orchestration engines that coordinate multi-step workflows. The selection of OIC for audit data extraction automation leverages its inherent advantages in credential management, where sensitive authentication tokens and API keys are securely stored in encrypted vaults rather than hardcoded within integration logic. Furthermore, OIC's managed infrastructure eliminates operational overhead associated with server provisioning, patch management, high availability configuration, and disaster recovery planning, allowing organizations to focus on integration logic rather than infrastructure maintenance [7].The implementation methodology begins with establishing a REST connection adapter within OIC that encapsulates the technical specifications for communicating with Oracle Access Management audit endpoints. This connection configuration includes base URL definitions pointing to the tenant-specific OAM instance, authentication method specifications utilizing OAuth client credentials, security policy selections defining transport-level encryption requirements, and timeout parameters governing request abandonment thresholds. Following connection establishment, the integration workflow orchestrates sequential API invocations through a carefully choreographed sequence of activities. The workflow initiates by invoking the statistical count endpoint with appropriate date range parameters, capturing the returned count value into a workflow variable for subsequent processing. This count value then parameterizes the second API invocation targeting the detailed event retrieval endpoint, ensuring the pageSize parameter accurately reflects the volume of available records. Data transformation processes intervene between API responses and data warehouse loading operations, converting the JSON-formatted audit events into relational structures compatible with target database schemas. These transformations typically involve parsing nested JSON objects, extracting relevant attributes, applying data type conversions, enriching records with metadata such as extraction timestamps, and formatting outputs according to predefined warehouse table structures.Alternative integration platforms such as SOAPUI and Postman serve valuable purposes within software development lifecycles but exhibit fundamental limitations when applied to production automation scenarios. SOAPUI excels as a testing tool for validating API functionality, exploring endpoint behaviors, and generating sample requests during development phases. Postman similarly provides intuitive interfaces for interactive API exploration and supports basic automation through collection runners and JavaScript-based test scripts. However, these tools lack enterprise capabilities essential for production deployments, including comprehensive error handling frameworks, transaction management, sophisticated scheduling mechanisms, centralized credential management, integration with enterprise monitoring systems, and formal change management processes. Enterprise-grade middleware solutions like OIC provide governance frameworks that enforce security policies, maintain audit trails of integration executions, support versioning and rollback capabilities, and integrate with corporate authentication directories. The operational maturity, vendor support commitments, service level agreements, and compliance certifications associated with OIC justify its adoption for mission-critical audit data extraction workflows where reliability, security, and maintainability supersede the simplicity offered by developer-centric tools [8].

5. Operational Deployment and Applications of analytics.

The automated data collection cycle of audits should be scheduled with a keen eye on the organizational patterns of access, the nature of data, compliance requirements, and latency requirements in the analysis. Best practice recommends daily extraction schedules that are performed during off-

peak hours to have an impact on the performance of production systems as minimally as possible in terms of resource consumption, with adequate temporal granularity to enable security monitoring. Retry mechanisms with an exponential backoff algorithm should be included in the scheduling configuration to reliably tolerate transient network outages, API rate limiting, or temporary service unavailability without data loss. Multi-time zone organizations need to be very keen when it comes to scheduling extraction windows to have full coverage of global access events, and yet on the other hand, not overlap with extraction windows, resulting in data duplication. The extraction timetable must coincide with the data retention policies related to audit repositories, whereby the systematic extraction of the data must precede the automated purging mechanisms, where historical events are erased from the source systems. Also, the scheduling schemes should support peak usage times during month-end financial reconciles, annual performance reviews, or open enrollment periods when there is a massive influx of authentication traffic in comparison to base level [9].The design of the data warehouse schema determines the level of analysis capabilities that can be used in the investigation of the analytical patterns and the generation of security intelligence. Dimensional modelling techniques are especially useful with audit data, where fact tables are used to record the individual authentication events with foreign keys linking them with dimension tables depicting users, geographic area, time, method of authentication, and characteristics of a device. There should be hierarchical structures in the temporal dimension to enable both operational monitoring and strategy trends analysis to be done at different granularities, such as hour, day, week, month, quarter, and year. Geospatial dimensions should be designed with great care and should involve the use of IP address ranges, geographic coordinates based on IP geolocation services, country codes, regional classifications, and organization location mappings to facilitate analysis of their territories' access. The slow-changing dimension techniques capture the transformation of the user attributes, organizational structure, and location classifications over time, but the historical context needed in a longitudinal analysis is maintained. Under schema design, any pre-aggregated summary table that speeds up typical analytical queries investigating daily access volumes, unique user counts, geographic patterns of distribution, and authentication success rates should be built in without having to scan entire table repositories of detailed events.The visualization of access patterns in the dashboard requires user-friendly interfaces that will pass on intricate security data to different stakeholder groups, such as the security operations department, compliance, human resource management, and executive management. Good dashboards use geospatial visualization to plot authentication sources on interactive world maps, which allows one to quickly locate unexpected points of access or unusual geographic patterns. Temporal trend charts will show access volumes over time dimensions, which can identify anomalous spikes that can be caused by credential sharing, automated attacks, or system misconfigurations. The visualizations of the heatmap are associated with the access times and user population to determine the off-hours activities that should be investigated. The capabilities of anomaly detection are based on statistical baselines based on historical trends, and anomalies such as unusual times of logins, first-time access with new locations, quick geographic changes, which physically cannot be made by the legitimate user, and attempts to authenticate after termination of employment are automatically flagged. Dashboard compliance reporting tools consolidate measures of access applicable to regulatory standards such as audit trail completeness, monitoring privileged account activity, segregation of duties violations, and access certification state [10].By integrating with security information and event management systems, the audit data is no longer presented as isolated logs but as a whole security intelligence through correlating HCM access patterns with events observed by network infrastructure, endpoint security solutions and email gateways, and other enterprise applications. Such a correlation allows identifying more advanced patterns of attacks that occur on many systems at once, including credential theft campaigns or insider threat programs.

Table 1: *Access Control Mechanisms in Oracle HCM Cloud [3, 4]*

Security Component	Implementation Approach	Primary Application Context
Role-Based Access Control (RBAC)	Hierarchical structure aggregating specific privileges with granular control extending to individual page components	Foundation for an authorization mechanism across all Oracle HCM Cloud functions, particularly for sensitive data like compensation and performance records
Job-Level Privileges	Access permissions defined by	Multinational organizations requiring

	employment attributes, including job codes, positions, departments, legal entities, and geographic locations	data residency compliance and jurisdictional access restrictions, especially under GDPR requirements
Data-Level Security	Row-level and column-level database restrictions using security profiles based on reporting relationships, cost centers, union membership, or custom attributes	Scenarios where users share functional roles but require different data sets based on organizational context and responsibilities
IP Whitelisting	Preventive control restricting access exclusively to predetermined network addresses, creating a digital perimeter	Organizations with centralized operations and limited remote work requirements, suitable for high-sensitivity functions
Comprehensive Audit Logging	Detective control maintains detailed forensic trails of authentication attempts and system interactions while permitting broader access	Distributed work environments with mobile workforces, contractors, and third-party service providers require flexible access patterns

Table 2: *Technical Architecture of Audit Data Extraction and Query Mechanisms [5, 6]*

API Component	Technical Characteristics	Operational Purpose
RESTful API Framework	Resource-oriented endpoints with standardized HTTP methods, JSON-formatted responses, and OAuth authentication protocols	Programmatic access to authentication and authorization audit data, serving as integration points for security information and event management systems
Two-Tier Query Approach	Initial statistical summary endpoint returning aggregate metadata, followed by detailed event retrieval requests with comprehensive audit records	Optimized strategy for managing large-volume audit data extraction while minimizing network overhead and processing latency in high-traffic environments
Temporal Parameters	ISO standard timestamp formatting with timezone specifications, fromDate, and toDate parameters with millisecond granularity precision	Establishing inclusive boundaries for audit windows with unambiguous interpretation across geographically distributed systems
Pagination Mechanisms	Combination of page number identifiers and page size limits with adaptive strategies for controlled traversal through large result sets	Managing distributed data retrieval operations without overwhelming client systems or network infrastructure
Timestamp Formatting	RFC-compliant UTC-based timestamps eliminate timezone conversion ambiguities and daylight saving time transition issues	Ensuring accurate temporal sequencing and enabling event correlation across geographically distributed systems for forensic investigations

Table 3: *Comparative Analysis of Integration Platforms and Implementation Architecture [7, 8]*

Integration Component	Technical Capabilities	Strategic Value Proposition
Oracle Integration Cloud (OIC) Platform	Declarative development paradigm with pre-built adapters, REST/SOAP support, visual transformation designers, process orchestration engines, and encrypted credential vaults	Comprehensive middleware solution abstracting network protocols, data conversions, and error handling while eliminating infrastructure maintenance overhead through managed services
REST Connection Adapter Configuration	Base URL definitions for tenant-specific instances, OAuth client credentials authentication, transport-level encryption policies, and timeout parameters	Encapsulates technical specifications for secure communication with Oracle Access Management audit endpoints with proper security and performance controls
Integration Workflow Orchestration	Sequential API invocations starting with statistical count endpoint, followed by detailed event retrieval with dynamic pageSize parameters and data transformation processes	Automated audit data extraction through choreographed activities that convert JSON-formatted events into relational structures compatible with data warehouse schemas

Enterprise-Grade Middleware Features	Comprehensive error handling frameworks, transaction management, sophisticated scheduling, centralized credential management, enterprise monitoring integration, and formal change management	Production-ready capabilities, including governance frameworks, audit trails, versioning/rollback support, and corporate authentication directory integration with vendor SLA commitments
Developer-Centric Tools (SOAPUI/Postman)	Interactive API exploration interfaces, endpoint behavior validation, sample request generation, collection runners, and JavaScript-based test scripts	Valuable for development lifecycle testing and API functionality validation, but lacking the enterprise capabilities required for production automation scenarios

Table 4: *Strategic Implementation of Audit Data Collection and Visualization Systems [9, 10]*

Operational Component	**Technical Implementation Strategy**	**Business Intelligence Application**
Automated Data Collection Scheduling	Daily extraction during off-peak hours with exponential backoff retry mechanisms, synchronized with data retention policies and aligned with extraction windows to prevent duplication	Balancing minimal production system impact with adequate temporal granularity for security monitoring while accommodating peak usage periods like month-end reconciliations and open enrollment
Data Warehouse Dimensional Modeling	Fact tables recording individual authentication events with foreign keys linking to dimension tables for users, geography, time, authentication methods, and device characteristics	Enabling analytical pattern investigation through hierarchical temporal structures and geospatial dimensions with IP address ranges, country codes, and organizational location mappings
Slow-Changing Dimension Techniques	Capturing transformations in user attributes, organizational structures, and location classifications over time while maintaining historical context	Supporting longitudinal analysis with pre-aggregated summary tables for accelerating queries on daily access volumes, unique user counts, and authentication success rates
Dashboard Visualization Interfaces	Geospatial plotting on interactive world maps, temporal trend charts, heatmap visualizations of access times, and statistical baseline anomaly detection capabilities	Communicating security intelligence to stakeholders, including security operations, compliance teams, HR management, and executives, through the identification of unusual geographic patterns and off-hours activities
SIEM System Integration	Correlation of HCM access patterns with events from network infrastructure, endpoint security solutions, email gateways, and other enterprise applications	Transforming isolated audit logs into comprehensive security intelligence for identifying sophisticated multi-system attack patterns, including credential theft campaigns and insider threats

4. Conclusions

Oracle HCM Cloud external access auditing by integrating with RESTful API could be seen as a strategic addition to the native security controls that organizations have essential visibility into the authentication patterns that take place outside the boundaries of the customary applications. The paper has shown an extensive structure of technical architecture, implementation methodology, and operational best practices of systematic audit data collection and analysis. The two-level query strategy makes the best use of data extraction performance, and the decision to utilise Oracle Integration Cloud as the middleware orchestration platform makes production deployments enterprise-grade in their reliability, security, and maintainability. The dimensional data warehouse schema design allows advanced temporal and geospatial analysis of the data, whereas purposeful dashboards change raw audit data into actionable security intelligence available to various stakeholder communities. Security information and event management system integration provides audit monitoring at the multiple enterprise systems level of threat detection instead of the isolated application logs level. Organizations using this framework have better access to methods of identifying abnormal access patterns, investigating security incidents, proving regulatory compliance, and forensic audit trails critical to modern

cybersecurity postures. With the rising level of mobility of the workforce and the growing number of regulatory requirements, the capacity to track and evaluate external access patterns is becoming more essential in safeguarding sensitive demographic information held in the cloud-based human capital management systems. This framework offers a viable and scalable framework that is balanced in terms of addressing security needs and providing operational flexibility so that organizations can increase their security monitoring capacity without compromising the accessibility and efficiency benefits that drive cloud HCM adoption.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Oracle Corporation, "Oracle Cloud Infrastructure Security Architecture," 2024. [Online]. Available: https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

[2] Mahesh Sabapathy, Nigel Smith, "Oracle® Human Capital Management Cloud Security Reference," Oracle Corporation, 2014. [Online]. Available: https://docs.oracle.com/cd/E51367_01/commonops_gs/OAWPM/OAWPM.pdf

[3] Dinesh Kumar Venugopal, "Oracle Fusion Cloud Applications," Oracle Fusion Cloud Applications, 2024. [Online]. Available: https://docs.oracle.com/en/cloud/saas/applications-common/24b/facsa/securing-applications.pdf

[4] Vincent C. Hu et al., "Guide to Attribute-Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162, 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf

[5] Gail Flanegin and Nina Wishbow, "Oracle® Access Manager," Oracle Access Manager Developer Guide 10g (10.1.4.3), 2009. [Online]. Available: https://docs.oracle.com/cd/E15217_01/doc.1014/e12491.pdf

[6] D. Hardt, "The OAuth 2.0 Authorization Framework," Internet Engineering Task Force, 2012. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6749

[7] Oracle Corporation, "Public Cloud Machine Using the Oracle Database Adapter," [Online]. Available: https://docs.oracle.com/cloud-machine/latest/intcs_gs/ICSSB/GUID-DF97A9E0-2BC5-42F9-B61F-CBB839DFB26B.htm

[8] Gartner Inc., "Magic Quadrant for Enterprise Integration Platform as a Service," Gartner Research, 2024. [Online]. Available: https://www.gartner.com/en/documents/5198963

[9] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," CSA Guidance. [Online]. Available: https://cloudsecurityalliance.org/research/guidance#

[10] Zhang Xiaolu, "COBIT 2019 Framework: Governance and Management Objectives," ISACA Publications, 2019. [Online]. Available: https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf