

A Metadata-Driven Governance and Data-Quality Framework for Secure Enterprise Information Systems

ROHIT NAGPAL, NAINA GUPTA,
ARJAV PRADEEP KALA, ANKIT PUSHPAM

Abstract: *This study offers a metadata-based framework of governance and data quality for secure enterprise information systems. This framework combines metadata standardisation, automatic data quality verification, role-based access control (RBAC), data lineage tracing, auditing and governance policies enforcement. An evaluation of the framework takes into account data defect identification, metadata completeness, record validity, security enforcement, lineage traceability, compliance with policies and performance. This set of indicators offers an instrument for evaluating information reliability, accountability and security in the enterprise environment. Examples of the outcomes of the evaluation show how this framework can be evaluated, offering possible improvements of data quality and governance in the enterprise. It should be noted that the numbers used are illustrative and not based on experimental results. In order to evaluate the framework performance further work is necessary, using real or representative enterprise data sets. This framework also introduces the following measures to evaluate the effectiveness of governance and reliability of operations: Metadata integrity; Identification of quality defects in data; Enforcement of access control; Lineage tracking; Policy adherence; And processing throughput. Through the integration of these measures, the suggested framework allows for an objective identification of any governance weaknesses and aspects that need to be improved. Due to its modularity, it is possible that the proposed framework can be adapted for use in different enterprise settings with different data types and security needs. However, this framework requires further experimentation using real enterprise data.*

Keywords: Metadata-driven governance, data quality, enterprise information systems, role-based access control, data lineage, policy compliance, audit logging, information security.

Rohit Nagpal (rohitnagpal92@gmail.com) Sr. Data Engineer, Amazon | Bellevue, WA USA
Naina Gupta (ngnaina13@gmail.com) Business Intelligence Engineer, Amazon | Seattle, WA USA
Arjav Pradeep Kala (arjavk@gmail.com) Data Scientist/Student, University of Cumberland | Jersey City, NJ, USA
Ankit Pushpam (pushpam.ankit@gmail.com) Data Engineer, Outcomes Operating Inc. | Seattle, WA USA

Introduction

Enterprise information systems produce huge amounts of data. Therefore, it is important to have proper data governance to ensure data accuracy, consistency, traceability and protection within such systems. The lack of integrated metadata, inadequate data definitions, inconsistencies in validation rules, absence of clear lineage, and incorrect permission levels may affect information governance negatively. It shows that there is a need to integrate the three concepts - metadata management, data quality assessment and information security.

This study will propose a metadata-based framework for data governance and data quality assessment in the context of enterprise information system security. The metadata-based framework will include metadata standardisation, automated rule-based data validation, RBAC, lineage of data, audit log, and policies enforcement. Metadata will contain information about data owner, data classification, data definitions, relationships between datasets, and the requirements on their quality (Sawadogo & Darmont, 2021). Automated validation will help detect missing, redundant, invalid and inconsistent data, and access control will prevent the use of data depending on roles and responsibilities. The proposed framework is assessed using metrics that include defect detection, completeness of the metadata, data quality enhancement, security enforcement, lineage tracking, policy compliance, and processing performance. This metric system creates an objective way to assess the efficiency and possible drawbacks of the framework. Since the numeric results obtained in the current research are illustrative and not validated by experiments, it is essential to perform practical implementation and experimental validation on relevant enterprise data sets (Konatham *et al.*, 2025).

Related work

Enterprise information systems have come to rely more and more on accurate metadata and good data-quality controls in order to maintain security, consistency and traceability of information. Chaudhuri & Rani (2025) provides that metadata-based governance represents a systematic way to deal with data definitions, ownership, data lineage, access permissions and validation requirements within enterprise information systems.

Simuni & Atla (2024) explain that data-quality management is yet another important element of enterprise governance. Lack of complete, accurate, updated and consistent data records may interfere with reporting, decision-making and analytics. Automated validation, identification of anomalies and monitoring of enterprise information systems can help in detecting such problems and taking the necessary measures. Nevertheless, successful governance requires clarity of responsibility and relevant metrics (Vadlamani *et al.*, 2025).

Awodire (2025) highlights that security and privacy have close ties to metadata management. Role based access control, audit trails, and data classification strategies can be used by organizations to keep information secure while being transparent about the utilization of data. However, there are complexities associated with enterprise-level environments, where the use of varying formats, standards, and access control policies is common. In addition, static

governance strategies might not be able to keep pace with dynamic data and related security threats.

The above complexities indicate the necessity of developing a unified approach incorporating metadata management, data quality evaluation, and security controls. The research will concentrate on integration of the three aspects mentioned using metadata standardization, automatic validation, lineage, access, and monitoring.

Method

The technical design-based approach used in the development of a metadata-driven governance and quality framework for secure enterprise information systems. It is most appropriate in this case since the research focus on the combination of governance policies, metadata management, quality validation, and security controls into a framework rather than eliciting user views using interviews or surveys (Uddandaraao et al., 2025).

Requirements analysis involves the identification of the main enterprise problems such as inconsistent metadata, incompleteness, poor traceability, and unauthorized access to the data. Requirements analysis will inform the development of the framework. Secondly, metadata modeling will involve data ownership, classification, data lineage, quality rules and access rules (Gudepu, Jaladi & Gellago, 2023). The use of this method facilitates standardized information management across different enterprise systems.

Table 1: Methods Used in the Proposed Framework

Method	Purpose
Metadata modelling	Defines ownership, classification, and lineage.
Rule-based validation	Detects incomplete, duplicate, and inconsistent records.
Role-based access control (RBAC)	Restricts access according to user roles.
Audit logging	Records governance and data-access activities.
Scenario-based testing	Evaluates framework functionality and compliance.
Quantitative performance evaluation	Measures accuracy, compliance, traceability, and throughput.

Rule-based validation and automated quality assessment employed to test for completeness, consistency, uniqueness and validity of the data. The techniques have been chosen because they will enable systematic detection of data errors. Role based access control will be incorporated to limit access to information based on roles (Uddandaraao, 2026).

Fourthly, scenario-based testing and quantitative assessment evaluate the framework using relevant enterprise data scenarios. Such evaluation criteria could include data quality error detection rate, validation effectiveness, policy compliance rate, process latency and unauthorized access detection. These could determine whether the framework increases information accuracy and security. In summary, the integration of metadata modeling,

automated validation, access control and evaluation is a technical method of evaluating an enterprise governance framework (Anand, 2023).

Results

Framework Evaluation and Data-Quality Performance

The metadata-based governance framework described above has been assessed by using the synthetic dataset of an enterprise and by simulating test cases, since no real enterprise dataset and execution logs have been provided (Sulova & Marinova, 2024). The results presented below represent the illustrative assessment results, which are not the confirmed measurements made on a real system. The aspects of assessment include data quality verification, metadata completeness, anomaly detection, access control enforcement, lineage, governance compliance, performance and effectiveness comparison.

Table 2: Defect Detection Performance Across Data-Quality Rules

Data-quality rule	Records checked	Injected defects	True positives	False positives	False negatives	Precision	Recall	Accuracy
Completeness	6,000	480	446	138	34	76.36%	92.92%	97.13%
Validity	6,000	360	342	101	18	77.20%	95.00%	98.00%
Consistency	6,000	300	267	171	33	60.96%	89.00%	96.60%
Uniqueness	6,000	180	175	70	5	71.43%	97.22%	98.75%
Referential integrity	6,000	240	218	127	22	63.19%	90.83%	97.52%

The simulation results show that the validation rules we propose are able to detect most injected defects. Uniqueness provides the best recall value of 97.22%, with 175 out of 180 defects detected. The validity rule has 95.00% recall, and the completeness rule gets 92.92%. The referential integrity and consistency provide low precision values of 63.19% and 60.96% respectively, which means that they trigger many false positive alerts. The consistency rule generates 171 false positives; hence, it can be claimed that there is some need for more context-dependent validation of relationships between records. Accuracy values vary from 96.60% to 98.75%; however, the high accuracy value can be explained by the fact that there were no defects in most records.

Metadata Completeness and Standardisation

The completeness and standardization of the metadata were evaluated as part of the evaluation of the efficacy of the framework in achieving consistency in enterprise information management. The evaluation was done with regard to 6,000 records in relation to 6 metadata

fields including data ownership, data classification, business definition, lineage information, assignment of quality rules, and access policy mapping (Conrad *et al.*, 2024).

Table 3: Metadata Completeness and Standardisation Assessment

Metadata element	Records assessed	Records meeting requirement	Compliance
Data ownership	6,000	5,640	94.00%
Data classification	6,000	5,760	96.00%
Business definitions	6,000	5,400	90.00%
Lineage information	6,000	5,220	87.00%
Quality-rule assignment	6,000	5,520	92.00%
Access-policy mapping	6,000	5,700	95.00%

The simulation of the assessment reveals differences in the level of metadata readiness among the 6,000 records assessed. Data classification is at 96.00% compliance, access policy mapping at 95.00%, and data ownership at 94.00%. The percentages indicate the possibility of defining standardized data classification and ownership as required fields. Information about the lineage of data demonstrates the lowest level of compliance of 87.00%. It is worth noting that 5,220 records comply with the requirement for lineage information. The low percentage is significant since the lineage of the data allows tracking its sources and further use of it. Business definitions demonstrate the compliance of 90.00% as well, which creates potential for confusion when different departments perceive the data element differently. In practice, missing lineage and unclear definitions should be addressed through metadata discovery, checks on required fields, and data steward responsibilities. Nevertheless, the percentages are simulated, while metadata completeness should be assessed through inventory of enterprise databases and data pipelines.

Comparative Data-Quality Performance

The comparative evaluation highlights the possible impacts of the metadata-based framework on the issues of data validity, duplication, completeness, and consistency (Elouataoui, El Mendili & Gahi, 2024). Comparison is done between baseline and scenario based on the proposed framework, utilizing the same set of quality criteria. The numbers provided herein are not experimentally verified; they are just examples and should be substituted with real figures.

Table 4: Comparative Data-Quality Performance Before and After Framework Application

Quality indicator	Baseline scenario	Framework scenario	Change
Valid records	88.00%	96.00%	+8.00 percentage points
Duplicate records	4.50%	1.50%	−3.00 percentage points
Incomplete records	8.00%	3.00%	−5.00 percentage points

Inconsistent records	6.00%	2.50%	−3.50 percentage points
Records passing all defined rules	82.00%	93.00%	+11.00 percentage points

In the example comparison, one can see how the values of various data-quality characteristics can change once the implementation of the metadata and validation have been introduced. The number of valid records grows from 88.00% to 96.00%; this is an increase of 8.00 percentage points. The number of incomplete records falls by 5.00 percentage points, whereas the numbers of duplicates and inconsistent records fall by 3.00 and 3.50 percentage points, respectively. At the same time, the share of records that pass all quality rules increases from 82.00% to 93.00%. These numbers would be operationally important if achieved through the actual implementation of metadata, but they should be taken with a grain of salt since they are illustrative figures and not the results of empirical study. The correct way to conduct the analysis is to use the same quality rules to measure both the initial dataset and the dataset after implementation.

Access-Control Enforcement and Security Testing

The security analysis evaluates the efficacy of the suggested model in the enforcement of role-based access control, prevention of unauthorised access to data and restricting sensitive information (Zaidi *et al.*, 2023). The analysis looks at read permission to authorised users, unauthorised read requests, write permissions, role segregation and sensitive data restrictions. Below are some of the results that need to be validated through execution.

Table 5: Access-Control Enforcement and Security Testing

Security test	Test cases	Correctly enforced	Incorrect outcomes	Success rate
Authorised read access	500	490	10	98.00%
Unauthorised read access	500	485	15	97.00%
Unauthorised modification	400	392	8	98.00%
Role-permission separation	300	288	12	96.00%
Sensitive-data restrictions	300	294	6	98.00%
Overall	2,000	1,949	51	97.45%

The simulations of the security tests show an average enforcement success rate of 97.45% where 1,949 out of 2,000 test cases exhibit the required outcome of the access-control process. The success rates of authorised read access, unauthorised modification, and restricted sensitive data access are all about 98.00%. Role permission separation shows a lesser success rate of 96.00%, implying that conflicts between user roles and permissions might need further testing. The 15 incorrect outcomes of unauthorised read access are especially significant, considering that improper access may lead to the leakage of sensitive corporate information. The above-mentioned incorrect outcomes should be explored in a production environment via testing of

permission and policy rules along with analysing the system's audit logs (Fritz-Morgenthal, Hein & Papenbrock, 2022). This example proves that one can test the role-based access control framework using test cases. However, even a highly successful simulation does not ensure that such framework is protected against any attacks by hackers or privileged privilege escalation.

Data-Lineage Traceability and Dependency Analysis

The traceability of data lineage was considered to test how effectively the proposed framework is able to track the data lineage from its origin to its destination, perform transformations, find upstream dependencies, evaluate the downstream effect, and document the history of changes. The results are indicative and need verification through a real-world dataset.

Table 6: Data-Lineage Traceability Assessment

Lineage test	Test cases	Successfully traced	Unresolved cases	Traceability rate
Source-to-destination tracing	400	380	20	95.00%
Transformation tracking	350	322	28	92.00%
Upstream dependency identification	300	282	18	94.00%
Downstream impact analysis	250	225	25	90.00%
Change-history reconstruction	200	188	12	94.00%
Overall	1,500	1,397	103	93.13%

The simulated assessment of the lineage yields an overall traceability rate of 93.13% through successful tracing of 1,397 out of 1,500 test cases. Source-to-destination traceability yields the highest success rate at 95.00% meaning that the proposed framework will be able to trace the origins and destination of the records in most test cases. Upstream dependency and change history tracing both yield 94.00% respectively. The least successful is downstream impact analysis which only yields 90.00% with 25 unsolved cases. This constraint is important for organizations as the need to know the impacted reports, processes, and applications before making changes on source data sets or transformation rules exists. If the dependencies of the transformation process are not captured, it might lead to errors in the reports produced and/or service disruptions. An implementation should collect lineage metadata automatically from the data pipeline, use consistent identifiers and verify dependencies each time transformations change (Liu & Meng, 2024).

Governance-Policy Compliance and Implementation

Compliance with the policies of governance was measured in order to determine if the framework presented is able to govern the data ownership, data classification, data retention, data access policies, and audit logs availability. Compliance with these policies ensures that the governance process will remain consistent in enterprise information systems.

Table 7: Governance-Policy Compliance Evaluation

Governance requirement	Policies tested	Correctly implemented	Compliance rate
Data ownership assignment	200	190	95.00%
Classification enforcement	200	194	97.00%
Retention-rule enforcement	180	169	93.89%
Access-policy enforcement	250	243	97.20%
Audit-log availability	170	163	95.88%
Overall	1,000	959	95.90%

The evaluation of the simulated governance results in overall compliance of 95.90%, with 959 out of 1,000 requirements being fulfilled properly. The access policy enforcement complies in 97.20% of cases, whereas classification enforcement is at 97.00%. These figures suggest that there is enough potential in centrally managed metadata and access policies to ensure the governance consistency across enterprise information systems. The lowest level of compliance is observed for the retention rule enforcement (93.89%). This implies that there may be a need for more sophisticated configurations of retention rules. In a real organization, the retention rules will have to comply with legal and operational requirements of the organization and not the universal one. There are 41 failed tests. The reason behind the necessity to pay attention to each failed test is the same – compliance cannot hide a single failure that needs categorization, an owner and proper monitoring till its correction (Ke & Zhang, 2021).

Computational Efficiency and Processing Performance

The performance of the processing workflow was assessed for the analysis of the computational efficiency of metadata validation, data quality rules enforcement, access policy evaluation, lineage processing, and the overall processing workflow itself. The execution time and throughput were chosen as the performance metrics. The provided values are only examples and need to be confirmed with benchmarking.

Table 8: Framework Processing Performance

Operation	Records processed	Illustrative execution time	Throughput
Metadata validation	6,000	2.4 seconds	2,500 records/second
Data-quality rule execution	6,000	4.0 seconds	1,500 records/second
Access-policy evaluation	6,000	3.0 seconds	2,000 records/second
Lineage relationship processing	6,000	5.0 seconds	1,200 records/second

Integrated framework workflow	6,000	8.0 seconds	750 records/second
--------------------------------------	-------	-------------	--------------------

The above performance demonstration example illustrates that the computations needed for each component process are different. Metadata validation process takes 2,500 records per second, whereas the process of enforcing data quality rules takes 1,500 records per second. Lineage relationship process operates at 1,200 records per second, since this process involves dependency and lineage evaluations. The entire process works at 750 records per second. This lower performance rate is understandable in case multiple tests are performed in sequence, though performance would also depend on specific factors. These rates should be seen as a guide to assess operational effectiveness, but not as evidence that the framework satisfies the requirements of a production SLA. Reproducible benchmarks require hardware information, software version, dataset size, warm-up and execution time, along with the median and 95th percentile latencies.

Discussion

The results shown in the previous section are indicative of how the new metadata driven governance and data-quality framework could enhance enterprise information management through the combination of metadata standardisation, automated validation, access control, data lineage and policy enforcement. Nonetheless, it should be noted that the quantitative results are illustrative and cannot be considered experimentally validated (Ruijter *et al.*, 2021). The evaluation of data quality shows that automated validation could assist in finding incomplete, duplicate, inconsistent and invalid records. In the illustrative comparison, the number of valid records rose from 88.00% to 96.00%, whereas the records complying with all quality rules rose from 82.00% to 93.00%. This illustrates potential improvements in data quality management; however, it should be noted that consistent quality rules need to be defined and applied to ensure data quality. Another crucial factor is that of the completeness of the metadata. In terms of the illustrative assessment, the data classification compliance was 96.00%, while ownership information compliance was at 94.00%. The compliance for lineage information was at 87.00%. This means that capturing lineage requires more focus. Metadata discovery automation, standardized naming, and assigned data steward duties can help to tackle this problem. As regards the security assessment, the integration of role-based access control into data governance is a vital thing. The illustrative overall enforcement rate of 97.45% shows how such an approach to measurement can be applied to check access control. At the same time, wrong results due to unauthorized access are very significant as well since any failure may be dangerous for sensitive enterprise information. Thus, permission testing, log audits, and policy assessments must be incorporated into security management process.

In addition, the 93.13% lineage traceability rate implies that lineage tracking is an effective means of source determination, change monitoring, and impact analysis. The lower rate for impact analysis is an indicator that there might be a need to improve dependency mapping. In reality, incomplete lineage would make it more challenging to manage changes and identify impacted reports, applications, and business processes. Evaluation of governance policy compliance rates is another way of proving the usefulness of compliance metrics (Amilineni,

2025). Compliance rate of 95.90% is one way of determining ownership, classification, retention, access policy, and log audit availability. However, compliance rates cannot prove regulatory compliance. Each failed check needs to be investigated, assigned to an owner, and followed through to completion. Finally, the performance estimate of the process reveals that an integrated process may take more time than individual processes because an integrated process involves a number of activities of validation and governance. The throughput estimate of 750 per second must thus be viewed as a suggested benchmark goal, not as a system performance measure. Actual test must involve documentation of hardware and software environment used, multiple runs, and latencies measured (Reddi *et al.*, 2020).

Conclusion

The framework offered within the paper represents an approach based on the use of metadata for governance and evaluation of data quality within enterprise information systems. Through the use of metadata standardization, automatic verification of data quality, access control based on user roles, tracking of the lineage of the data and enforcement of the governance policies, the proposed framework allows creating a systematic approach to managing the enterprise information during all phases of its lifecycle. The example assessments presented show how the indicators such as metadata completeness, defect detection, access control, policy compliance and processing throughput may be used to assess the efficiency of the proposed framework. However, the numerical values presented in the illustration are only illustrative and require empirical verification before any conclusions are made. Further research should include the application of the suggested framework to real enterprise data sets and benchmarking of its performance under varying loads and changing security threats.

Reference List

- Amilineni, M. V. (2025). Audit-Safe Agentic RAG Framework for Regulated Enterprise Systems: A Trustworthy AI Architecture for SAP, Finance, Healthcare, and Government Workflows. *International Journal of Advances in Signal and Image Sciences*, 34-46. <https://xscience.org/index.php/IJASIS/article/download/1849/846>
- Anand, L. (2023). An intelligent AI and ML-driven cloud security framework for financial workflows and wastewater analytics. *International Journal of Humanities and Information Technology*, 5(02), 87-94. <https://ijhit.info/index.php/ijhit/article/view/138>
- Awodire, M. (2025). Data governance and privacy-by-design frameworks (GDPR/HIPAA) in multi-cloud data pipelines. *Journal of Data Analysis and Critical Management*, 1(02), 116-126. <https://jdcam.com/index.php/jdcam/article/download/112/79>
- Konatham, M. R., Uddandaraao, D. P., Vadlamani, R. K., & Konatham, S. K. R. (2025). Federated learning for credit risk assessment in distributed financial systems using BayesShield with homomorphic encryption. *IEEE International Conference on Computing Technologies & Data Communication (ICCTDC)* (pp. 1–6). IEEE. <https://doi.org/10.1109/icctdc64446.2025.11158863>

Chaudhuri, B. G., & Rani, S. (2025). Evaluating Metadata For Governance, Stewardship And Quality Control Architecture In Telecom Data Mining. *International Journal of Environmental Sciences*, 11(21s),
<https://pdfs.semanticscholar.org/08e8/9fc2f9cc510a56783501cb73569ee25a8bb9.pdf>

Conrad, T. O., Ferrer, E., Mietchen, D., Pusch, L., Stegmüller, J., & Schubotz, M. (2024). Making mathematical research data FAIR: Pathways to improved data sharing. *Scientific Data*, 11(1), 676. <https://www.nature.com/articles/s41597-024-03480-0>

Elouataoui, W., El Mendili, S., & Gahi, Y. (2024, April). Active metadata and machine learning based framework for enhancing big data quality. In *Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security* (pp. 1-8).
<https://dl.acm.org/doi/abs/10.1145/3659677.3659707>

Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. (2022). Financial risk management and explainable, trustworthy, responsible AI. *Frontiers in artificial intelligence*, 5, 779799.
<https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2022.779799/full>

Gudepu, B. K., Jaladi, D. S., & Gellago, O. (2023). How data catalogs are transforming enterprise data governance: a systematic literature review. *The Metascience*, 1(1), 249-264.
<http://yuktabuilder.com/index.php/TMS/article/view/256>

Ke, B., & Zhang, X. (2021). Does public enforcement work in weak investor protection countries? Evidence from China. *Contemporary Accounting Research*, 38(2), 1231-1273.
<https://onlinelibrary.wiley.com/doi/abs/10.1111/1911-3846.12652>

Liu, W., & Meng, S. (2024). Data Lineage Tracking and Regulatory Compliance Framework for Enterprise Financial Cloud Data Services. *Academia Nexus Journal*, 3(3).
<http://academianexusjournal.com/index.php/anj/article/view/32>

Reddi, V. J., Cheng, C., Kanter, D., Mattson, P., Schmuelling, G., Wu, C. J., ... & Zhou, Y. (2020, May). Mlperf inference benchmark. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)* (pp. 446-459). IEEE.
<https://ieeexplore.ieee.org/abstract/document/9138989/>

Uddandara, D. P. . (2026). Statistics and the Science of Causal Economics: A New Paradigm for Data Science. Deep Science Publishing. <https://doi.org/10.70593/978-93-7185-895-3>

Ruijter, J. M., Barnewall, R. J., Marsh, I. B., Szentirmay, A. N., Quinn, J. C., van Houdt, R., ... & van den Hoff, M. J. (2021). Efficiency correction is required for accurate quantitative PCR analysis and reporting. *Clinical chemistry*, 67(6), 829-842.
<https://academic.oup.com/clinchem/article-abstract/67/6/829/6247760>

Sawadogo, P., & Darmont, J. (2021). On data lake architectures and metadata management. *Journal of Intelligent Information Systems*, 56(1), 97-120.
<https://link.springer.com/article/10.1007/S10844-020-00608-7>

Vadlamani, R. K., Sundaramoorthy, P., Srinivasagopalan, L. N., Uddandara, D. P., & Bandaru, R. R. (2025). Generative AI and large language models in conversational systems:

Trends and future directions. 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 577–583). IEEE. <https://doi.org/10.1109/aic66080.2025.11212044>

Simuni, G., & Atla, A. (2024). Hadoop in enterprise data governance: Ensuring compliance and data integrity. Available at SSRN 4982500.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4982500

Sulova, S., & Marinova, O. (2024). Metadata management framework for business intelligence driven data lakes. *Business Management/Biznes Upravljenje*,(2).
<https://www.cceeol.com/search/article-detail?id=1257240>

Zaidi, T., Usman, M., Aftab, M. U., Aljuaid, H., & Ghadi, Y. Y. (2023). Fabrication of flexible role-based access control based on blockchain for internet of things use cases. *IEEE Access*, 11, 106315-106333.
<https://scholar.google.com/citations?user=KQ1g3p0AAAAJ&hl=en&oi=sra>

Uddandaraao, D. P., Valiveti, S. S. S., Varanasi, S. R., Rahman, H., & Chakraborty, P. (2025). Data-centric governance models using trustworthy AI: Strengthening transparency, bias control, and policy compliance in welfare management. *International Journal on Engineering Artificial Intelligence Management, Decision Support, and Policies*, 2(4), 29–44.
<https://doi.org/10.63503/j.ijaimd.2025.200>