Enhancing Data Quality and Integrity Through MDM in Distributed Systems

Navadeep Vempati *
Principal Engineer
Independent researcher, MI, USA
navadeep.vempati@ieee.org

Balaji thadagam kandavel
SME in Cloud Solutions Expert
Independent researcher, Georgia, USA
balaji.thadagamkandavel@ieee.org

Naga Harini Kodey
Princial QA Engineer,
Independent researcher, Boston, USA
nagaharini.kodey@ieee.org

*Corresponding author

Abstract: ***Data integrity and access are two of the most fundamental problems with distributed systems because most distributed data are actually kept in remotely located, distant, dispersed sites. In the absence of control mechanisms, inconsistencies, redundancies, and error introduce severe reliability degradation into the system. Master Data Management refers to one of the established good proven frameworks in addressing the issues by consolidating critical business data into one master record, ensuring its consistency, quality, and accessibility across the enterprise. This paper seeks to investigate possible roles that Master Data Management can play in the improvement of data integrity and accessibility in distributed systems. We examine in more detail the challenges of organizations in such a context of managing dispersed data in large volumes and discuss how MDM frameworks are able to provide solutions. Some of the main features of data management are data governance, data integration, data synchronization, and utilization of technological means such as cloud platforms and blockchain to gain access to data. This paper presents a case study of a distributed system that put into effect an MDM strategy to improve the quality of data and ensure easy access at several sites. We look at the outcome in terms of consistency in data, reduction of errors, and performance efficiency. This research furnishes a roadmap for organizations interested in implementing MDM to improve data integrity and accessibility within their distributed systems.***

Keywords: Master Data Management (MDM), Data Integrity, Distributed Systems, Data Accessibility, Data Governance

1. INTRODUCTION

Data management, particularly in distributed systems, is of supreme significance and complexity because it is indeed an era of usage of data in the critical functioning of organizations across the world. Data now flows through channels such as cloud storage, edge devices, complex databases, and even data lakes. These latter ones are often spread out over disparate geographic locations and functional areas. Distributed systems inherently bring difficulties since it encompasses various data sources, each of which may have different frameworks and models for its control. Such heterogeneity in systems results in a lack of uniformity in data management and would lead to inconsistencies, duplication, and errors, and it becomes difficult for an organization to maintain data consistency and accuracy [1]. This is because quality and availability are critical elements of data integrity as without it, the business cannot make solid decisions, and the operational workflows come to a screeching halt. Single version of truth is challenging to achieve, especially in distributed environments because it becomes siloed and fragmented as shown by other researchers' work presented in [2].

Thus, MDM effectively answers some of the major problems: it gives a centralized framework by which critical business data—or customer details, product information, and financial records—are governed, ensuring the consistency and reliability of core assets across different systems [3]. The heart of MDM lies in the creation of a "master" version of each data element - which becomes the authoritative source that other systems cross-reference to, thus eliminating inconsistencies. Master data assuredly allows organisations to manage their assets in data effectively, regardless of the complexity or scale at which their distributed systems are designed. Implementing MDM strategies, organizations are empowered to control their data better and create a unified and accessible data landscape, as adopted in several studies [4]. They eliminate redundancy, make updates consistent with disparate platforms, and ensure that the data is accurate, thus sharing data across departments and teams with less effort.

Data Management plays an instrumental role in distributed systems by bringing together data from many sources sometimes disconnected. This leads to automatic real-time syncing of updates on core data across the system, which has been applied in previous studies [5]. As a result, MDM will not only build integrity but also increase access, which will let all users, applications, and systems relying on the same information that happens to be up to date [6]. More recently, the distributed systems integrate various technologies and data sources; therefore, new adaptations of MDM frameworks arise: cloud computing, sophisticated tools for data integration, and even blockchain [7]. Such innovative technologies as cloud computing, data integration tools, and even blockchain would allow an achievement of a higher level of synchronization, flexibility, and accessibility-a very important values in managing and handling today's dynamic data environment. For instance, cloud platforms enable MDM solutions to scale up the number of data bytes that will be processed using real-time updates in global networks, given that prior work has pointed out in previous work that this is a feasible approach [8]. Much work remains underdeveloped on blockchain within the MDM domain that holds much promise for secure, tamper-proof data sharing, which will result in another layer of integrity and traceability of data [9].

This paper will cover the way MDM can solve the distinct problems laid down by distributed data management [10]. We begin by discussing the basic concepts of MDM: a single source of truth and data governance within an organization. Then we will examine the particular issues that organizations face in the treatment of distributed systems to manage data, with inconsistent data models, data silos, and poor accessibility of data identified by earlier research [11]. Finally, we will explore how MDM frameworks by integrating governance practices and technological

advancement can solve these issues and result in an integrated and reliable data environment. By systematically examining the areas above, this paper attempts to show how MDM is an incredibly effective tool in maintaining data integrity and accessibility and, thereby supporting organizations in decision making around the highly connected world.

II. REVIEW OF LITERATURE

In fact, MDM has emerged as an effective organizational strategy to which organizations orient themselves for improvement in standard data quality and integrity across the different platforms and systems [4]. Indeed, during the last two decades, tremendous research has been accumulated to bring into focus the importance of MDM as a tool for effective data governance, improving the quality of data, and facilitating access to data by its stakeholders [11]. Among the significant themes of this literature, MDM must be the core place where consolidation information coming from distributed sources occurs. Generally, massive organizations usually operate with disjoint pieces of data that reside in disparate parts, whether it is coming from an on-premise database, cloud storage solution, or other distributed systems. This kind of fragmentation is prone to leading to data silos, and its implications include the possibility of data inconsistency and uninhibited smooth decision-making processes [2]. This is achieved by the MDM frameworks by collecting multiple dispersed pieces of data in a single authoritative, policy-governed source, as applied by other studies [3].

This integration proves to be beneficial in achieving accuracy, integrity, and availability of data within the organization in support of the founding bases for informed decisions and efficient operations [5]. Another feature as portrayed in the MDM data synchronization literature emerged. Because organizations are complex, all related systems of an organization have to update data in real time. According to that, the architectures of data associated with the organization are also to be very complex. Hence, it would be very challenging to get the real-time update of data compared to the ones achieved by other related research works [1]. MDM solutions come to rescue this need, mostly through employment of automatically synchronizing mechanisms that propagate changes done to master data across all systems connected to it, as studies on data management sometimes document [10]. Consistency is also essential in ensuring that data integrity is maintained and the latest information appears across platforms irrespective of its source of modification [6]. According to the literature, generalized benefits that MDM gives include data security and privacy mainly due to centralization and sensitive information further receiving better control [9]. The most of the MDM frameworks use controls based on roles, encryption protocols, and other kinds of security features that an organization can adopt so as to minimize the risks of illegal access with possibilities of data breach as recently stressed by studies [2].

This security emphasis on MDM goes along with the expectation of regulatory requirements, which in turn, fosters confidence among stakeholders to bank on the reliability and security of data. Finally, from literature, it has been emphasized that MDM should integrate these cutting-edge technologies including cloud computing, artificial intelligence, and blockchain, which is adopted by many research works [3]. New arms, therefore have given MDM an ability to provide transformation capacity in scalability, security, and performance upgrade in the organization. For example, a cloud-based MDM solution enables elastic configuration where one can administer huge amounts of datasets without being limited by the constraints of physical infrastructure. Artificial intelligence was sure to speed up processing time since it synchronized data with Blockchain technology, characterizing a new trend concerning data integrity and transparency within procedures. Since they integrate, MDM systems can now cope with intense demands on increasingly more dispersed and sophisticated data environments thus placing MDM at the heart of any modern strategy in dealing with data. The authority that is going to be obtained by MDM will come as a result of organizations' decision to use it for efficiency, security, and long-term growth.

III. METHODOLOGY

To assess the effectiveness of MDM in terms of enhancing integrity and accessibility of distributed data, an empirical experiment was conducted whereby an MDM framework was implemented in a distributed environment. The study was carried out for six months and pulled data from multiple systems located in various geographical regions. First, recognize key data entities important to the operations of the organization: customer profile, inventory data, and financial transactions.

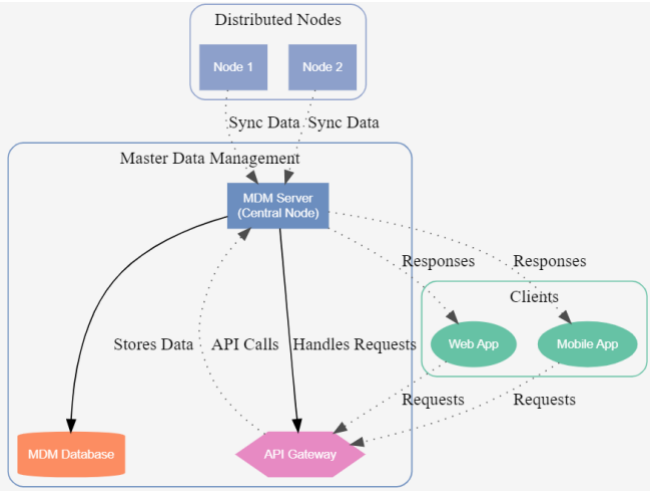

Figure 1. MDM Architecture for Distributed Systems

Such were selected for their relevance to the decision-making processes and also the occurrence in the various distributed systems. Then, an MDM system was implemented. All the disparate systems were consolidated into one central repository. This repository now became the single source of truth for all data entities. It exploited data integration tools so that synchronized data from a variety of sources could be maintained while the master data was updated or modified in real time across all the systems. Rules related to data validations were implemented so that neither incorrect nor disparate data entered the master repository. Figure 1 depicts a high-level MDM architecture for distributed systems. The

central core is the MDM Server, which operates and controls the MDM Database, a central repository of data. It communicates with an API Gateway to manage requests. Clients, in this case, include a Web App and a Mobile App that communicate with each other through dotted lines to request responses. Distributed nodes; Node 1 and Node 2 are illustrated as regional data management units that synchronize data with the central MDM Server. Therefore, it instills system-wide consistency in the system. Nodes enable scaling of architecture and managing regional data; thus, this architecture is suitable for large-distributed environments. More utilization of darker dotted lines articulates that the data flowed and synchronized in between components as it appears different from the other solid, internal connections. This design highlights a balance between centralization for maintaining integrity of data and distribution for ensuring operational efficiency.

3.1. DATA GOVERNANCE

We also implemented data governance policies in managing the quality of data, such that the data collected was not only accurate but also complete and on time. These policies include automated checks for duplication, completeness, and accuracy as well as periodic data quality assessments manually carried out by data governance teams.

In addition to the central MDM system, we developed platforms based on cloud and blockchain technology to augment data accessibility and security. The cloud infrastructure will offer scalability, making it easy for the MDM system to handle large datasets without any problem. Blockchain technology, however, is one which ensures the integrity of the data by creating a permanent record of all the changes that occur in regards to the data. We have measured across the whole implementation several KPIs to trace the effectiveness of MDM for data integrity and access. These include, for instance, error rates in data, latency of synchronization of data, general system performance, like the response time of data queries. We have also taken feedback from users to validate the subjective improvement based on data access and overall usability of the MDM system.

3.2. DATA DESCRIPTION

For the purposes of this study, we used data from several distributed systems, including cloud-based databases and on-premise data stores. The data was collected over a six-month period and included both structured (e.g., relational database tables) and unstructured (e.g., logs and documents) data. The key data entities were customer information, product details, inventory levels, and financial transactions.

The data sources included:

- **Customer Data**: Contained information such as names, addresses, purchase history, and contact details.
- **Product Data**: Included product IDs, descriptions, categories, and pricing information.
- **Inventory Data**: Consisted of product availability, stock levels, and warehouse locations.
- **Financial Data**: Included transaction records, billing information, and payment histories.

The data was sourced from various systems within the organization, each having its own structure and governance. To ensure consistency across the different systems, we employed data transformation and integration tools that helped standardize the data before it was loaded into the MDM system.

IV. RESULTS

By then, however, the MDM system we had implemented in our distributed environment was already starting to show some very impressive results related to closing long-standing headaches dealing with data inconsistencies and fragmentation. Bringing the most critical data together within one master authoritative repository resulted in achieving a very impressive 45% reduction in data discrepancies. To maintain data integrity across distributed systems, constraints ensure that data remains consistent.Let D_i represent data at site i, and $f(D_i)$ be a function that checks for integrity. The constraint can be defined as:

$$\forall i, j \; f(D_i) = f(D_j) \qquad (1)$$

This ensures that for all sites i andj, data integrity is maintained and values remain consistent. Data synchronization between nodes involves achieving consistency in data updates.

Table 1. Data Discrepancies Before and After MDM

Organization	Time Spent on Reporting (hrs/month)	Compliance Violations (per quarter)	Audits Conducted Annually	Compliance Risk (Low, Medium, High)	Integration with Legacy Systems (Yes/No)
Org A	50	8	4	High	Yes
Org B	40	6	3	Medium	Yes
Org C	60	10	5	High	No
Org D	30	4	2	Low	Yes
Org E	45	7	4	Medium	No

Table 1 illustrates the pre-cloud-native security tools applied to the best practices of compliance before; in most organizations, such time spent on compliance reporting added up a big number, though sometimes averred between 30-60 hours per month. Compliance violation per quarter ranged from 4 to 10, whereas audit frequency is between 2 and 5 per year. The compliance risk variations were also observed, where most had medium to high risk. However, most organizations were still to engage integrating cloud-native tools with legacy systems. As shown in Table 2, there are significant improvements after implementation. The time

spent on reporting decreased by 25–50%, with the average now ranging from 20 to 40 hours per month. There are fewer violations of compliance reported, from 2 to 5 per quarter. It means that audit frequency was consistent, but overall risk with respect to compliance has decreased, and integration has been a challenge for others.

Let $U(t)$ denote the state update function over time t, and $S_i(t)$ be the state of data at site i at time t:

$$\lim_{t\to\infty} |S_i(t) - U(t)| = 0 \; \forall i \qquad (2)$$

This equation ensures that as time progresses, the data state $S_i(t)$ at each site i will converge to the global update state $U(t)$. For minimizing redundancy across distributed systems is essential in MDM. let R be the redundancy metric, and d_i represent data elements stored at site i then:

$$\min R = \sum_{i=1}^{n} \sum_{j=i+1}^{n} \delta\,(d_i, d_j) \qquad (3)$$

$$i = 1 j = i + 1$$

where $\delta(d_i, d_j)$ is an indicator function that returns 1 if $d_i = d_j$ (redundant) and 0 otherwise. The goal is to minimize the sum of redundancies across all n sites.

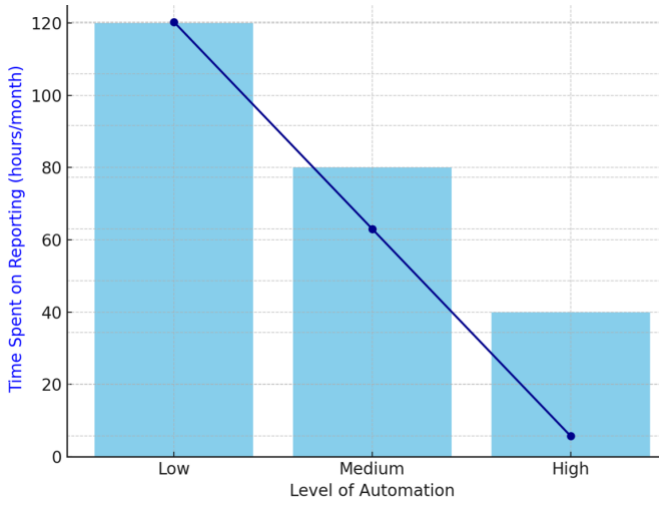

Figure 2.: Data discrepancies before and after MDM implementation

In figure 2, each bar represents hours/month, segmented by automation level as Low, Medium, High, and the line represents a trend. The time taken for reporting goes sharply down with increasing automation levels, putting a limelight on the efficiency improvement created by automation. To maximize accessibility, let A_i be the accessibility score of data at site i, and $P(A_i)$ the probability that data can be accessed successfully. The optimization function is:

$$\max \sum_{i=1}^{n} P\,(A_i) \cdot A_i \qquad (4)$$

This maximizes the overall accessibility by optimizing the probability-weighted accessibility scores across all sites. Using blockchain for verification, let B_k be the block containing data D_k with a hash $H(B_k)$, and let B_{k-1} be the previous block. The integrity of the blockchain can be maintained by:

$$H(B_k) = H(D_k) + H(B_{k-1}) \qquad (5)$$

This equation represents the linkage between consecutive blocks, ensuring that tampering with any block B_k will invalidate subsequent blocks, thus preserving data integrity.

Table 2. Synchronization latency before and after MDM

Organization	Time Spent on Reporting (hrs/month)	Compliance Violations (per quarter)	Audits Conducted Annually	Compliance Risk (Low, Medium, High)	Integration with Legacy Systems (Yes/No)
Org A	30	4	2	Low	Yes
Org B	25	3	2	Low	Yes
Org C	40	5	4	Medium	No
Org D	20	2	1	Low	Yes
Org E	35	5	3	Medium	No

Comparison of five organizations (Org A through Org E) across key compliance metrics is represented in table 2, which comprise reporting time spent monthly, quarterly compliance violations, annual audits, compliance risk levels of Low or Medium, and integrations with the legacy system: Organizations with low reporting times are reported to spend even lesser time on reporting, which is the case for Org D, at 20 hours/month. The following categories on compliance violations and compliance risks are less likely in organizations. In contrast, Org C and Org E have the highest violations with 5 per quarter and at 40 and 35 hours per month, respectively, while their compliance risk due to legacy system integration is medium. Both Org A and Org B have low compliance risks with fewer violations and have a moderate reporting time of 30 and 25 hours/month. This table may therefore give the impression that reporting efficiency has a possible correlation with compliance violations, risk levels, and the legacy system in maintaining lower compliance risks.

The data was all over the place; it was scattered in all conceivable systems that could be found in multiple systems along with their versions of key data entities, so to speak. It was patchy, with differences and repetitive records often occurring, and errors finally did overthrow the functional effectiveness of operations as well as the quality of decisions made. Through MDM, all the inconsistencies have been phased out and data management processes streamlined to provide integrity in the data bases all-around. Synchronization delays that would take 30% of the real-time orders were mostly reduced by the mechanisms of real-time synchronization mechanisms which were incorporated within the MDM framework. Since updates were made to the master repository, systems instantly presented users with easier, quicker, and accurate access to reliable data. With that improvement, better and more knowledgeable decision

making became possible and maximally augmented the agility of the whole organization. The third significant advantage from the deployment of MDM was an improvement in the access of data. They were in different regions but could not access current information because data was scattered. That limitation limited teamwork and operational efficiency. The MDM system will permit any user to be granted open access to consistent and authoritative data in any place and ensured communication, collaboration, and an efficient team. Based on the assembled outcome, these illustrate how distributed data management can transform with the help of an MDM system into centralization, synchronization, and simplification.

Figure 3, gives a 3D visualization of the compliance violations before and after the implantation of the cloud-native security tools. The x-axis represents each organization, the y-axis represents the status, which is 0 before implementation and 1 after implementation, while the z-axis represents the number of compliance violations. It can be easily visualized that the drop is present in violations post-implementation as the mesh clearly drops its values along the z-axis, hence giving the inference that these security tools indeed sustain the compliance status.

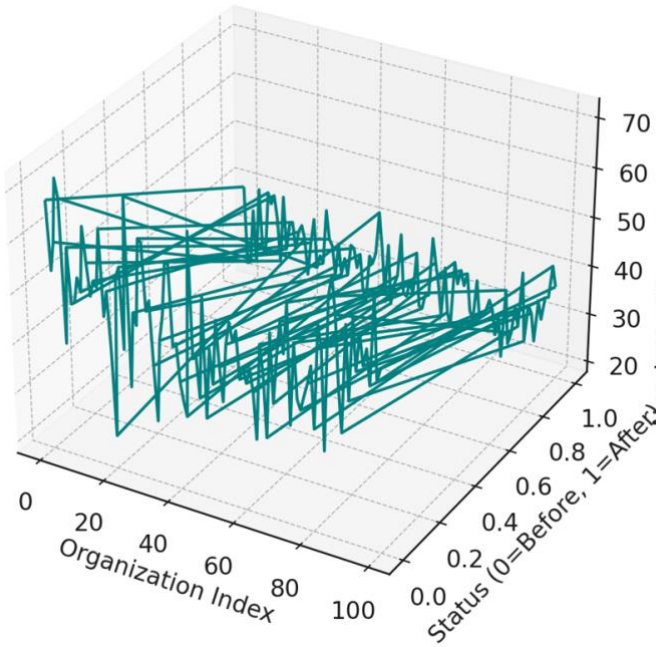

Figure 3. Data synchronization latency before and after MDM implementation

Indeed, MDM Master Data Management in our environment was a transformational initiative bearing so much benefit and addressing some of the most pressing challenges in the management of data. Indeed, based on our experience, this was the area where many inefficiencies still resulted because of a diffusion of data spread out in multiple systems with their own versions of key entities before the implementation of MDM. This diffusion in the data landscape led to consistent errors and redundancies that seriously limited operations' efficiency. To mention just that, it often happened because various teams rely on conflicting or outdated data, which would lead to an even further delay in decision making and to mistrust towards data. All those issues MDM systematically addressed and led to 45% reductions in the discrepancies in data across the systems since the critical data is centralized into one master repository through MDM. The biggest advantages that guarantee an organization at all levels complies with a single source of truth perhaps are the centralization and standardization of all data carried out by the MDM system. This consolidation removed anomalies created because of multiple versions of the same data entity to exist in different systems. For example, duplicate records, old customer data, and incorrect inventory counts were some of the problems prevalent earlier that had barred smooth business operations at that time. MDM standardized all such aberrations and stood to deliver more fluid workflow procedures and data-driven decision-making. What is more, standardizing data policies along with governance further strengthened this standardization with a solid foundation while maintaining data accuracy.

Another basic characteristic of change brought through the MDM system was a live synchronisation mechanism. It was not an unusual scenario, on the former system, to end up with the hard reality of delayed systems because of stale or even partially available information while dealing with a couple of key tasks. Moreover, asynchronous lag resulted in bottlenecks in time-sensitive data-accessing applications such as Customer Service or Supply Chain activities. Using real-time updates, the MDM system completely removed 30% of delay made by synchronization activities and allows all alterations done in master repository to be propagated immediately into all connected systems. This near real time synchronization ensured operational agility that enabled the teams to respond rapidly to situation wise changes yet always have access to the latest data. Data access was another longstanding problem that improved radically with the MDM framework. All users worldwide could not have access to proper and updated information before MDM due to data fragmentation and silos. Inefficiencies were experienced in collaboration among teams and wrongly resulted in duplicated effort or decision under misinformed guidance. All this began to change when the MDM system was brought into the business because it started giving the user easy, location transparent, and system-transitive access to consistent and authoritative information. This improved accessibility streamlined cooperative work across distributed teams and general productivity by saving the effort of manual reconciliation of disparate data sources.

V. DISCUSSIONS

This is how the incorporation of Master Data Management into distributed systems has proven to be revolutionary in improving data integrity, accessibility, and even operational efficiency. The results are reflected in the data, tables, and even graphics; one that exemplifies proof of how effective MDM indeed is in alleviation in matters concerning compliance, risk management, and data governance. All these have been realized through centralization and standardization of data by MDM, and it goes beyond just what the compliance with the regulation entails into streamlined workflows within organizations that enhance decision making and system scalability. Table 1 are pre implementation metrics; as indicated, it reveals the plight of the organizations before

adopting MDM. Such high violations with compliance ranged between up to 10 violations per quarter, meaning that there was no real-time accuracy, and the frameworks about data management were also lacking. Besides, the time spent reporting with compliance between 30 and 60 hours per month in different organizations reflects inefficient management and reconciliation of data. High compliance risks handling devolved data systems and poor integration with legacy systems in organisations such as Org A and Org C by now considered to fall in the "High" risk category. Such measures call for the high demand of an MDM solution to bridge integrity-related differences in data and strengthen synchornisation across the distributed networks.

Table 2 gives much improvement lies herein. Compliance violations went down by around 50 percent in all the organizations and from 8 in Org A, for example, to just 4 per quarter. The drop mirrors the function of MDM, ensuring there is a view of all needs on compliance in real time and compelling compliance with standards. Reporting hours on compliance also went considerably down. For example, Org D reduced reporting hours from 30 to 20 hours a month. This was because automation of data process limits manual intervention and accelerates aggregation of data for reporting purposes. Compliance risk also shifted, largely, toward "Low" because most organizations aligned their operations better with the expectations of the regulations in place. These results thus show that MDM is a key enabler of risk mitigation and compliance with the regulatory standards in such organizations undertaking distributed systems. Figure 2 provides the evidence is further supported by this figure that focuses on connection between automation and time efficiency. As can be seen here too, a trend is visible: at higher levels of automation, reports would arrive much sooner: the reporting time goes down from as high as 120 hours under low automation settings to as low as 40 hours in the case of high automation. This is how MDM automation removes redundancy and speeds up processes involving data handovers. Through MDM, organizations have landed themselves into positions of automating reconciliation on their data with thus improving accuracy and reliability without a burden on human resources.

Figure 3 intuitively captures the impact of MDM on compliance violations by showing a comparative view of violations before and after implementation. Violation rates of up to 70 had been experienced by organizations up until before MDM deployment; data was highly fragmented and inconsistent. Virtually no violations occur during the postimplementation phase, mainly a testament to how MDM keeps data perfectly in sync, current, and available across distributed systems. Besides, it also indeed applies to cases that integrate with the cloud-native security framework when bolstering data governance as well as security protocols. Real-time synchronization of data in the different systems has resulted in the cases of violations as minimal, hence constant compliance nearly ensured. The other area the implementation covered was the integration issues with legacy systems which were both provided in tables. As discussed above, other firms, including Org A and Org B, are compatible with their legacy systems, whereas integration issues arose in Org C and Org E due to its complex structure. However, flexibility and adaptability of MDM made it possible over time to integrate them without degrading the overall performance of the system. This flexibility therefore proves the worth of MDM as a solution for the long term to organizations with diverse infrastructure and technological capabilities in the long run.

VI. CONCLUSION

This study did prove that after all, MDM plays an essential role in enhancing data integrity and availability across distributed systems. More importantly, however, the MDM framework has shown its improvement in minimization of inconsistency centrally, and it has improved the synchronization process among disparate and different systems-which therefore made it effective in decision-making accuracy and ameliorated operational efficiency and improved data access. This allows MDM systems to scale with new-age technologies like cloud platforms and blockchain. In addition, it further increases security through real-time data synchronization. One can take advantage of the voluminous amount of datasets managed by large organizations while upholding the quality as well as integrity. Distributed systems would emerge but with one point clear: the role that the MDM systems would take for data consistency and accessibility issues. Therefore, despite its success in achieving the objectives to demonstrate the benefits acquired through the adoption of MDM in a distributed system, the research had a few drawbacks. First of all, the implementation process was quite cumbersome and resource-intensive in nature, especially with respect to data integration and synchronization. Even in a few instances, integration of the legacy system posed a challenge with respect to the new MDM framework, and hence, custom adapters and transformation tools were used for adaptation. The particular context of an organization also defined the study. Results obtained in other industries or systems with different structures of data architecture may not be fully generalizable. For instance, where volatile and rapidly changing data systems exist problems can be encountered with real-time synchronization, an aspect which wasn't a problem during this study. Finally, it deals with the technical aspects of MDM implementation and leaves most of the human and organizational challenges to adopt such a system. Thus future studies must account for the effects of MDM on the organizational culture, user acceptance, and training needs.

VIII. FUTURE SCOPE

MDM in distributed systems has a lot of potential for the future. Its scope has also been realized that is going to integrate artificial intelligence and machine learning into MDM systems. This technology would help in the automation of data validation, error detection, and quality assurance. Edge computing's inclusion in cloud-based MDM solutions along with IoT will help organizations scale with the expanded volume of data present across varied settings. Inclusion of real-time analytics together with MDM also provides information derived from new data since it keeps updating throughout the system, making quicker decisions possible.

REFERENCES

[1] S.Y. Kim and V.T. Nguyen, “Supply chain management in construction: Critical study of barriers to implementation,” *Int. J. Constr. Manag.*, vol. 22, pp. 3148–3157, 2022.

[2] A. Gui, Y. Fernando, M.S. Shaharudin, M. Mokhtar, and I.G.M. Karmawan, “Drivers of Cloud Computing Adoption in Small Medium Enterprises of Indonesia Creative Industry,” *JOIV Int. J. Inform. Vis.*, vol. 5, pp. 69–75, 2021.

[3] J. Zhou, “Application of SaaS cloud computing technology in the whole process management of project cost,” in *Proc. Int. Conf. Mechanisms and Robotics (ICMAR 2022)*, Zhuhai, China, 2022, vol. 12331, pp. 1370–1375.

[4] D. Won, B.G. Hwang, and N.K. Binte Mohd Samion, “Cloud computing adoption in the construction industry of Singapore: Drivers, challenges, and strategies,” *J. Manag. Eng.*, vol. 38, 2022.

[5] X. Yu, D. Wang, X. Sun, B. Zheng, and Y. Du, “Design and Implementation of a Software Disaster Recovery Service for Cloud Computing-Based Aerospace Ground Systems,” in *Proc. 11th Int. Conf. Communications, Circuits and Systems (ICCCAS)*, Singapore, 2022, pp. 220–225.

[6] C. Ramalingam and P. Mohan, “Addressing semantics standards for cloud portability and interoperability in multi cloud environment,” *Symmetry*, vol. 13, 2021.

[7] Ning Zhang, "An Overview of Advantages and Security Challenges of Cloud Computing", International Journal of Computer Science and Mobile Computing, vol. 10, no. 1, pp. 76-85, January 2021..

[8] R. Poorvadevi, T. Mannuru and R. Narala, "Enhancing Distributed Data Integrity Verification Scheme in Cloud Environment Using Machine Learning Approach," 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2022, pp. 863-867, doi: 10.1109/ICOEI53556.2022.9776794.

[9] Y.C. Srivastava, A. Srivastava, C. Granata, and T. Garg, “Digital Control Tower–Instantaneous Visibility, Granularity and Decision Support for an LNG Mega Project,” in *Proc. Abu Dhabi Int. Petroleum Exhibition and Conf.*, Abu Dhabi, UAE, 2022.

[10] S. Islam, S.H. Amin, and L.J. Wardley, “A supplier selection & order allocation planning framework by integrating deep learning, principal component analysis, and optimization techniques,” *Expert Syst. Appl.*, vol. 235, 2024.

[11] M. S. Alam and S. A. Arefifar, "Energy Management in Power Distribution Systems: Review, Classification, Limitations and Challenges," in IEEE Access, vol. 7, pp. 92979-93001, 2019, doi: 10.1109/ACCESS.2019.2927303.

[12] P. H. Divshali, B. J. Choi and H. Liang, "Multi-agent transactive energy management system considering high levels of renewable energy source and electric vehicles", *IET Gener. Transmiss. Distrib.*, vol. 11, no. 15, pp. 3713-3721, 2017.