Journal of Sustainable Solutions
ISSN : 3048-6947 | Vol. 2 | Issue 1 | Jan - Mar 2025 | Peer Reviewed & Refereed

Data Governance & Security: Protecting Business-Critical Information

N V Rama Sai Chalapathi Gupta Lakkimsetty
Independent Researcher, USA.

Accepted: 19/01/2025 Published: 21/01/2025 * Corresponding author

How to Cite this Article:

Sharma, A. (2025). Data Governance & Security: Protecting Business-Critical Information, *Journal of Sustainable Solutions*, 2(1), 19-28.

DOI: https://doi.org/10.36676/j.sust.sol.v2.i1.55

Check for updates

Abstract

The growing dependence of organisations on data for operational efficiency and decision-making has made protecting sensitive data a top issue. Instead of seeing security as an afterthought, the "Security by Design" approach promotes incorporating security measures into data systems' architecture and design from the beginning. The integration of security and governance into data systems is examined in this study, with a focus on the function of the governance of data in guaranteeing data protection, privacy, and compliance. Organisations may reduce the risk of data breaches, unauthorised access, and abuse by implementing clear governance structures that guarantee data security procedures are regularly followed. Layers of product-specific regulations and standards form the foundation of this structure. To satisfy a product's needs and meet the cutting-edge specifications of its field, the layers might be combined into a particular set. The deployment of eGovernment systems, which are often backed by middleware-based integration platforms, is a result of governments' increasing usage of information technology. Specifically, the necessity for government organisations to exchange information more often has spurred the adoption of provided Master Data Management (MDM) systems. However, these systems must adhere to data protection laws, which might make it more difficult for the government to reuse a lot of information. The challenges of implementing Data Protection (DP) laws in e-Government MDM system are discussed in this study. Specifically, it examines the demands that DP problems place on these systems and suggests ways to enforce these rules while taking into account various MDM architectural styles. These solutions make use of middleware-based capabilities and conventional MDM systems.

Keywords: - Decision-Making, Operational Efficiency, Growing Adoption, E-Government, Leverage Middleware-Based, MDM Systems, Data Protection (DP), Clear Governance, Data Breaches, Risk, Proposes Solutions, Compliance.

I. INTRODUCTION

Data is becoming one of the most important resources for businesses in all sectors in the current digital era. There has never been a greater pressing need to safeguard data, whether it is consumer personal information, intellectual property, or information that is essential to corporate operations [1]. Businesses must implement strong security measures to safeguard their data systems and guarantee their integrity in light of the growing frequency of data breaches, cyberattacks, and stricter data privacy laws. The idea of "Security by Design," which stresses incorporating security into the data system design from the beginning rather than implementing security measures after the system has been implemented, is a crucial component of this protection [1,2]. Integrating thorough governance frameworks is one of the best strategies to guarantee data system security. The procedures, guidelines, and standards that guarantee data security, consistency, accuracy, and accessibility are together referred to as data governance [2, 3]. In addition to ensuring that data is handled sensibly and morally, effective governance also makes sure that it is shielded against loss, corruption, and unwanted access.

Organisations may guarantee that data is continuously safeguarded throughout its lifetime, from collection to preservation, processing, and sharing, by including safety precautions into the architecture of the data system via governance [2, 3]. Typically, governance frameworks consist of a mix of procedures, instruments, and regulations that uphold data security standards.

These consist of data labelling and classification [3, 4], access control policies, data encryption, auditing procedures, and adherence to industry rules like the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR) in Europe, and the Healthcare Insurance Portability and Accountability Act (HIPAA) in the United States (US). These frameworks assist organisations in demonstrating compliance with these requirements, which has grown more crucial given the growing dangers of data breaches, in addition to protecting sensitive data [4].

Adopting security by design for data systems entails a comprehensive strategy in which security is integrated across the whole data lifecycle [4, 5]. Security precautions must be taken proactively from the moment data is collected until it is stored, analysed, and finally shared or deleted. Organisations should, for instance, use encryption to safeguard data while it is being sent, enforce strict access control procedures, and guarantee that only authorised people have access to sensitive information [5, 6]. In order to trace data access and change and detect any risks and breaches instantly, organisations also need to set up transparent audit trails.

Furthermore, the significance of security by design is increased with the growing use of based on the cloud data systems. Nowadays, a lot of businesses depend on cloud providers to store and process their data, therefore they need to collaborate closely with these providers to make sure that the necessary safety protocols are in place [6, 7]. This shared responsibility paradigm, nevertheless, sometimes causes misunderstandings about who is in charge of certain security measures. Because of this, businesses need to be vigilant about security and make sure that their cloud-based systems for data are just as safe as their on-premise systems [7, 8].

According to recent studies, both the frequency of security events and the financial impact of each data breach have grown over time. 47% of Finnish organisations were the most affected by data breaches in 2009, with 25% of EU organisations reporting such incidents [7, 8]. As a consequence, the European economy has lost billions of euros per year (source: Europol). The proliferation of data (Big Data), social media engagement, and the rise in cybercrime are the primary causes of security events [8, 9].

According to a 2010 study, 39% of the businesses under investigation had an average security maturation of 2 out of 5 [8, 9]. Companies mostly prioritise operational security (such as firewalling and anti-virus technology) and less on governance (such as compliance, rules, and business continuity management), according to empirical (measurements) study conducted inside organisations in 2012 and 2013 [8, 9]. Therefore, based on these research, security of information maturity has decreased over the last three years, mostly due to the "complex and generic" nature of the present frameworks. [9, 10]. Regulatory regulations are the driving force behind the data confidentiality dilemma [10, 11]. Information is becoming more and more regulated across a number of industries as it is essential to oversee data custodians' operations via legal frameworks.

Examples include the General Data Protection Regulation (GDPR) law, the Payment Card Industry (PCI) Security Standards, the Public-Sector Information (PSI) Directive, the PII, or personally identifiable information Privacy Act 5 u.s.c. 552a 2020 edition, and anonymisation standards such as the Health Insurance Portability and Accountability Act, or European Medicines Agency Policy 0070.

Fines of up to 4% of the yearly worldwide revenue may result from these regulatory actions, which might have an instantaneous financial effect [14]. The most recent instance is Facebook, which has been fined $5 billion and might face further penalties of €56 million based on the results of continuing GDPR investigations. Since all of these laws and regulations create a very complex legal and compliance framework that businesses must adhere to [16], data confidentiality is a candidate for further automation due to the Data Loss Prevention (DLP) risk [15].

Value has been included as one of the key V's of big data as a result of the growing dependence on data-driven data analysis and visualisation, which has been validated by academics and the business community [17]. The usage of data will rise in an effort to create value via big data, which will raise the possibility of sensitive information being shared without the appropriate safeguards in place [18]. It becomes clear why privacy of data is seen as the most crucial component of big data safety when this danger is coupled with the Variety impact of big data [19].

Organisations are concerned about how to effectively manage and prevent related risks as a result of the growing usage of data and changing regulatory frameworks. An opportunity for standardisation and automation has been found in relation to this demand. In order to create the necessary policies and procedures, the majority of organisations have started a journey with their Information Security Office (ISO), Chief Data Office, and Information Technology departments [19, 20]. With this in place, businesses need a framework to automate the process and reduce human involvement, which may result in bias or mistakes. According to the adoption of the Big Data Era, the corporate cost of not sharing and using the data may restrict the competitive advantage of the company. Therefore, after determining the need and related expenses, the possibility of automation was examined.

Even though combining security and governance is crucial, many organisations still find it difficult to put these ideas into practice. Instead of being a fundamental component of the system's design, security is sometimes seen as an afterthought or an add-on [20]. Organisations may therefore have to deal with issues including uneven data protection procedures, insufficient security measures, and trouble fulfilling regulatory obligations. In order to overcome these obstacles, this study investigates how businesses may successfully include governance frameworks into their data system architecture, guaranteeing that security is ingrained from the very beginning [21].

E-Government systems have been increasingly implemented to improve the quality of public services by providing relevant information and self-services to citizens as well as by enabling a more effective inter-organizational coordination among public agencies and partners [21]. These systems are usually based on middleware platforms providing capabilities to interconnect agencies. Information sharing is at the root of eGovernment as it is required to achieve a consistent systems' interoperability as well as to promote efficiency by reducing duplication of effort in collecting and storing information.

This has motivated the inclusion of an "Information dimension" in e-Government architectures. Furthermore, ensuring the quality of shared data and the application of rigorous management practices have motivated the adoption of Master Data Management (MDM) as a key component in eGovernment. Briefly, [22], MDM systems consist of Information Systems on core business data enriched with tools and management practices. In this way, MDM systems provide an integration and quality assurance tier between business components implementing public services and data distributed in organizations connected through the e-Government system.

In response, the implementation of Data Protection (DP) along with additional privacy-related laws, which are now enacted in many nations, poses a significant obstacle to inter-organizational data exchange. According to some empirical research, this characteristic may prevent a government from reusing information extensively since they must carry out many validations on the data's sources, purpose, and consents before sharing it [11].

In order to address the challenges of implementing Data Protection laws in e-Government MDM systems, this study analyses the needs that these problems provide and suggests enforcement strategies that take into account the various MDM architectural styles [12]. The suggested solutions make use of widely used standards (like XACML) and the capabilities of conventional MDM systems and middleware-based integration platforms (such data transformation).

II. RELATED WORK

2.1 Master Data Management Master

The unified, [13], comprehensive, and accurate picture of business-critical Master Data (MD) inside an organisation or business sector is provided by data management (MDM). MDs are made up of ideas and characteristics like "person" with "name" and "birthday" or "product" with "colour" or "size." Because MD is a strategic organisation, quality and dependability must be guaranteed. As a result, MD establishes clear Data Management & Governance procedures, which form the foundation of MDM.

The repository model entails keeping all of the data in a single database, including all MD characteristics used in all software programs [14]. A central MDMS handles client data requests without contacting source systems (application software information providers). Based on where MD is preserved, this style comes in three different variations (i.e., produced, updated, and destroyed):

i) Consolidation;

ii) The centralisation of; and

iii) Living together.

In the consolidation type, local source systems handle all MD maintenance tasks, and data updates are sent from those systems to a central MDMS. In the centralised variation, the MDMS handles all MD maintenance tasks, and data updates are sent from the MDMS to the target systems [15]. Lastly, data changes go both ways in the coexistence version, which combines the earlier ones.

2.2 E-Government Platforms Integration

In many nations, platforms have emerged as a crucial instrument for advancing e-government. In order to provide economies of scale and promote the growth of multi-agency services, they often offer the resources and infrastructure needed to make it easier for agencies to interact with one another [16]. Common features include interoperability (e.g., via using standards), security (e.g., authentication), connection, and mediation services that leverage Enterprise Integration Patterns (EIP), such as data transformation [16]. Enterprise Service Bus (ESB) and SOAP Web Services, a position are two examples of traditional middleware technologies that typically offer mediation and interoperability features. Furthermore, security features often depend on established standards like XACML.

2.3 Data Protection Regulations

Governments often manage very sensitive personal data (Wu, 2014). In fact, combining and aggregating data might make their analysis quite intrusive. Because of this, the majority of nations have created some kind of Data Protection (DP) law, although with somewhat diverse methods [17]. They primarily address the reuse of information in different settings for which it was originally intended. In many nations, people must specifically provide their approval before authorities may use or distribute their personally identifiable data [19, 20]. According to Figure 1, under these regulations, individuals grant agencies permission to use or share sensitive data with other agencies for a specific purpose and during a certain time frame.

2.4 Relevant Standards

The ISO/IEC 8000-1X0:2009 series of standards addresses the need for applications to communicate MD and their quality level, Fig. 1, using a predefined format. Specifically, the ISO 8000-120:2009 section outlines how details about the MD provenance are provided in the messages that are transmitted. As an example, attributes are established to identify the kind of event conducted over data, the date of the event, the organisation that supplies the MD, and the organisation that owns the MD, among other things [19, 20].

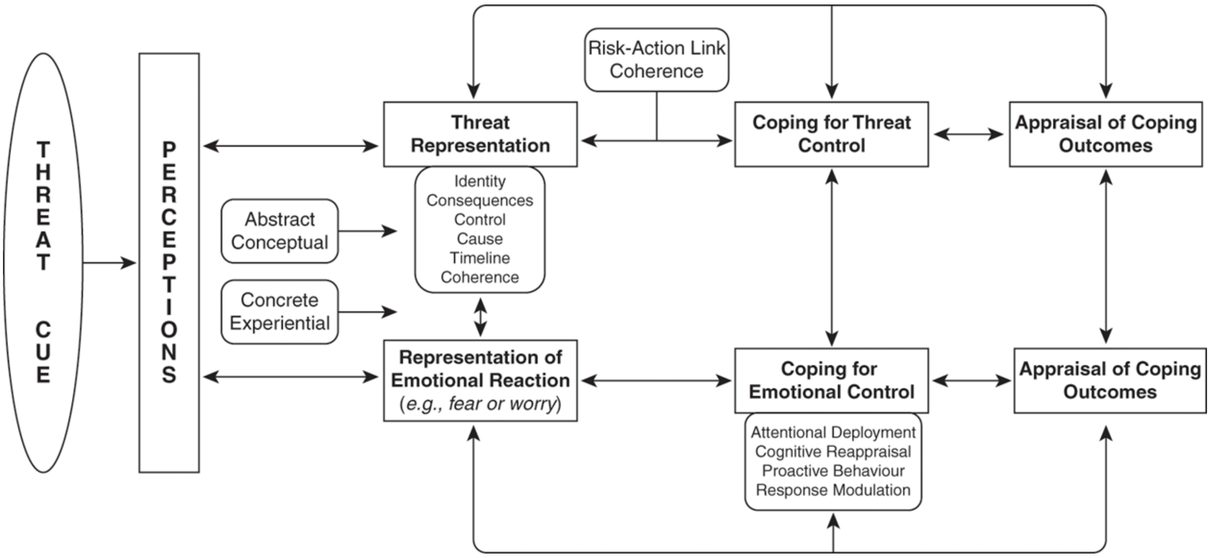

Fig. 1 Common ideas found in the DP Regulations. [20]

The possibilities and difficulties of MDM in e-Government or extensive collaborative systems have been discussed by a few writers. Additionally, it has been discussed how to enforce DP requirements in cross-organizational data transfers [11]. To the best of our knowledge, however, neither solutions that use middleware-based capabilities to handle the problems of DP and internet-based government MDM Systems nor approaches that jointly address them exist. Lastly, although some MDM systems address data privacy, they concentrate on less abstract solutions (like data encryption) than our strategy (like managing citizen consents) [5].

III. REQUIREMENTS FOR ENFORCING DP

The e-Government MDM framework that this work is built on is established in this part, along with the criteria for DP regulatory enforcement inside it. [5, 9].

3.1 E-Government MDM Context

The following traits are typical of e-government systems:

i) Interaction between organisations;

ii) Citizens' data must be distributed; [10],

iii) Consents about the shared information's arrangement of data;

iv) Regulatory organisations (oversight and performance. agency, for example); and

v) The application of integration platforms.

The MDM eGovernment setting used as a foundation for this study is shown in Figure 2 [18].

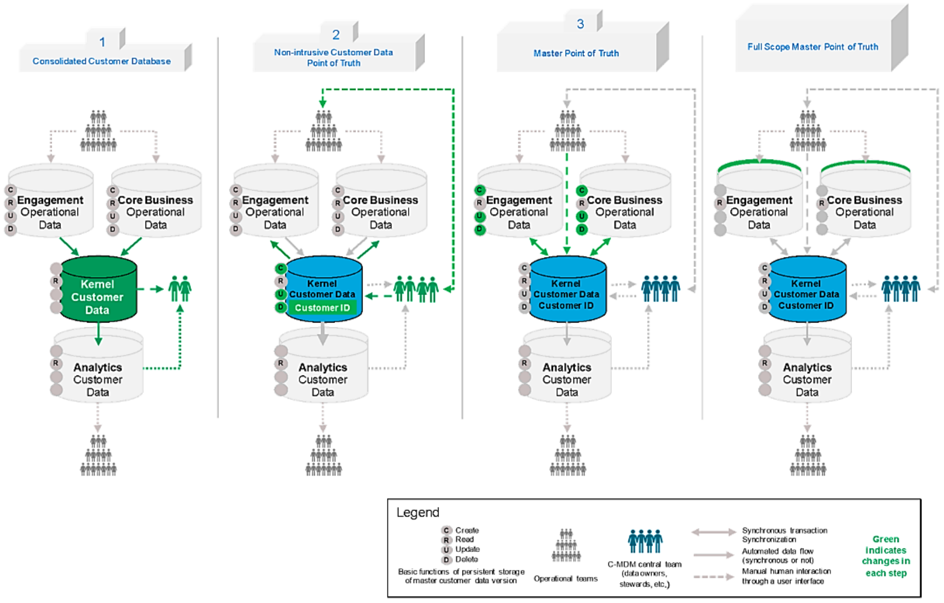
1
Consolidated Customer Database
2
Non-intrusive Customer Data Point of Truth
3
Master Point of Truth
Full Scope Master Point of Truth
Engagement Operational Data
Core Business Operational Data
Kernel Customer Data
Kernel Customer Data Customer ID
Analytics Customer Data
C
R
U
D
Legend
C Create
R Read
U Update
D Delete
Basic functions of persistent storage of master customer data version
Operational teams
C-MDM central team (data owners, stewards, etc.)
Synchronous transaction Synchronization
Automated data flow (synchronous or not)
Manual human interaction through a user interface
Green indicates changes in each step

Fig. 2 Context of Generalised MDM e-Government. [19]

An Integration Platforms (In-P) run by a supervising agency facilitates all communications between public entities [18, 20]. This platform offers security services like authentication as well as basic mediation features like data transformation. Additionally, it is in charge of hosting the MDM system, which specifically manages citizen data. When MD is maintained (if done at the In-P, for example, using a centralised repository style), synchronised (between the In-P and public agencies), or requested (for example, by other agencies or partners), MDM interactions that go via the In-P occur [22].

Public agencies use the IaaS strategy (i.e., via services) and a state-wide approved data model, which is an a superset of the MD schema, to exchange citizens' data [28]. Specifically, the MDM system sends and receives messages (such as SOAP messages) over a platform in order to get and transmit MD characteristics for citizens. Because they include provenance information, these messages adhere to the ISO/IEC 8000-1X0:2009 family of standards.

A citizens' MD schema [1], used as a case study throughout the remainder of the work, and the format of messages transmitted and received using throughout-P to exchange data are shown in Figure 2. It should be noted that the communication contains information about its origin, destination, sender, and provenance in addition to the citizens' data.

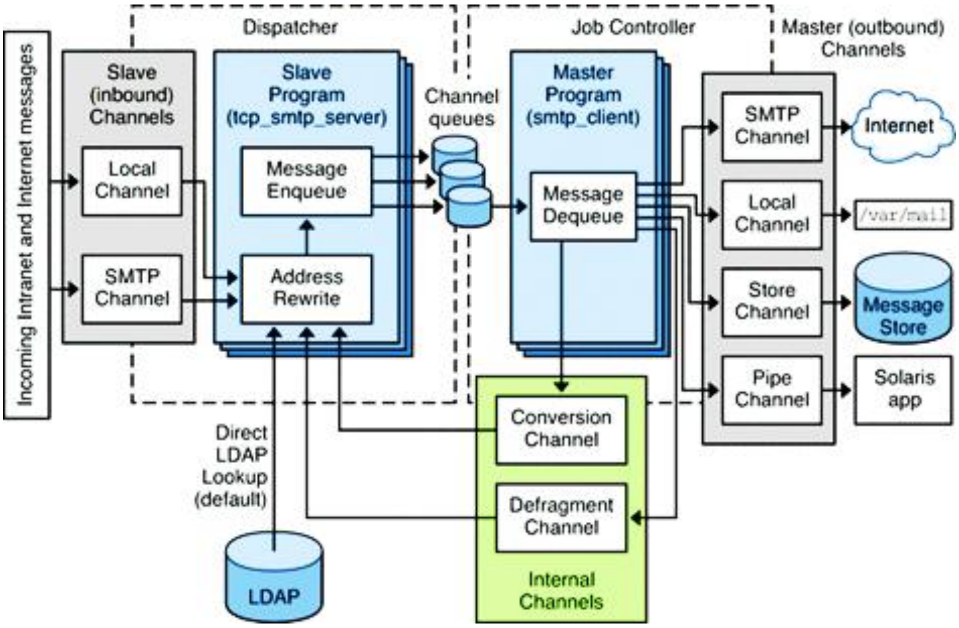

Fig. 3 Message Structure and the Master Data a schema. [14, 16]

3.2 Analysis of Requirements

Four basic conditions must be met by a system that enables a supervising agency to ensure that all [28], MDM contacts adhere to DP laws in the context that is being provided:

RQ1: Through components housed in the InP, it must keep an eye on and implement DP requirements. This is due to:

i) The supervisory the agency must have complete authority over the methods of enforcement and the sanctions that will be applied in cases in which a rule is broken, and

ii) It's possible that certain government organisations lack for the construction necessary to house the necessary elements.

RQ2: All MDM interactions carried out inside the In-P, such as during requesting, maintaining, and synchronising MD, must be observed and enforced by it [18].

RQ3: It must permit the preservation of each MD attribute's categorisation (sensitive or public), citizen permission, and existing DP regulations. This is required to know if a given interaction is compliant with the regulations [29].

RQ4: It must be able to manage and gather the additional data needed to confirm that the interactions are compliant. This comprises:

i) Details that must be included in requests (such as the reason the MD is being sought); and

ii) Data that may be needed to confirm the interaction' conformance but is not covered by the MD model, such as nation of origin [16].

IV. PROPOSED APPROACH

The suggested approach's a high-level architecture, the expanded MD design process, and the enforcement of DP requirements in the many MDM connections are all covered in this part. [19].

4.1 High Level Architecture

The high-level design of the suggested solution, which consists of many specialised components housed in the In-P [19, 20], is shown in Figure 4. First, as per Figure 4's conceptual model, the consent management system Management System (CMS) is responsible for upholding people' consents. A user interface based on the internet would be ideal so that individuals could control their own consents.

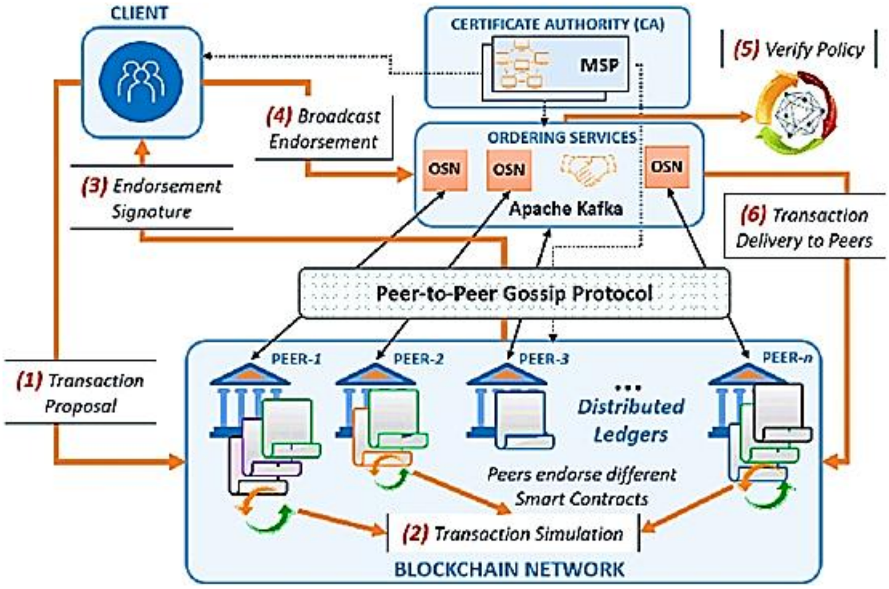
CLIENT
CERTIFICATE AUTHORITY (CA)
MSP
(5) Verify Policy
(4) Broadcast Endorsement
ORDERING SERVICES
OSN
OSN
OSN
Apache Kafka
(3) Endorsement Signature
(6) Transaction Delivery to Peers
Peer-to-Peer Gossip Protocol
PEER-1
PEER-2
PEER-3
PEER-n
(1) Transaction Proposal
Distributed Ledgers
Peers endorse different Smart Contracts
(2) Transaction Simulation
BLOCKCHAIN NETWORK

Fig. 4 High Level Proposal Architectural. [26]

4.2 Extended MD Design

The following phases make up the procedure to expand MD, which uses the original MD & DP policies as input:

1) Determine the necessary information to make authorisation judgements and specify whether or not the MD should include it, [28]
2) Find sensitive information in both the original MD or the extra information found in the step before, and [29],
3) Give each sensitive property a provenance attribute [28].

The outcome of applying the aforementioned procedures to the example shown in Figure 3 [28] is shown in Figure 5. Nationality is an extra necessary characteristic in this instance that is added to the initial MD.

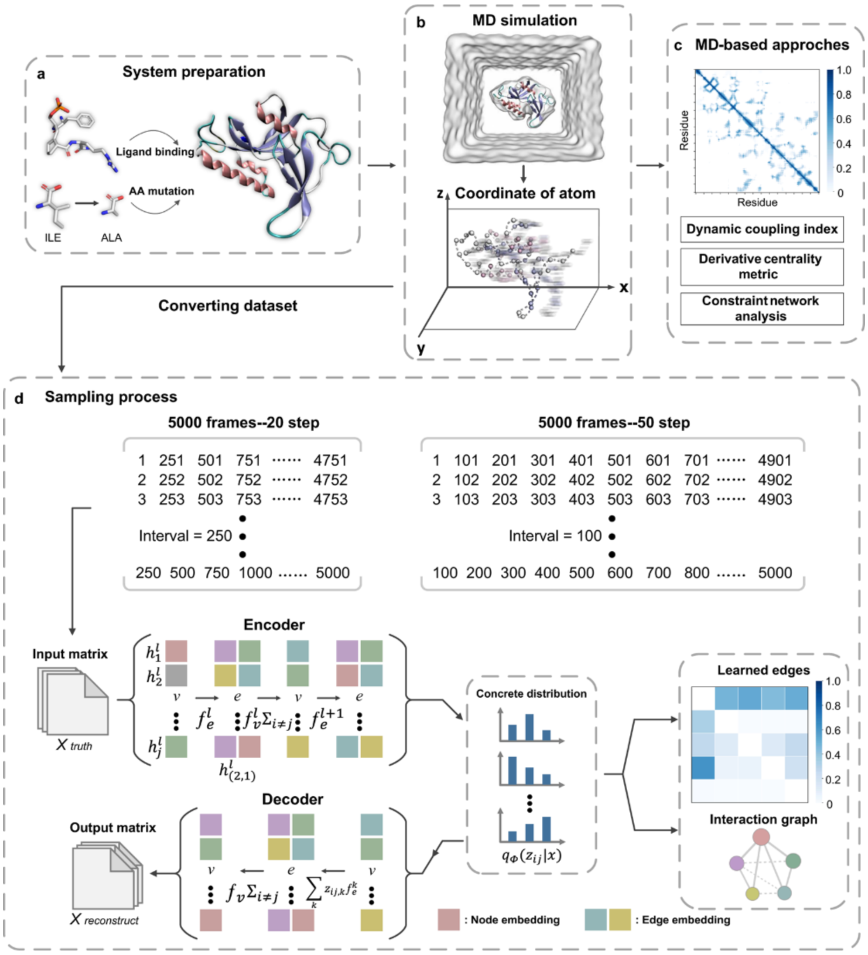

Fig. 5 Extra Steps in MD Design. [29]

4.3 Enforcing DP in MDM Interactions

This section explains how, in light of the various architectural types, the suggested solution enforces DP requirements within MDM interaction (maintenance, synchronisation, and requests). Coexistence or centralised versions of the repository architecture allow MD maintenance interactions to go via the In-P. The interactions in these situations must contain a goal with the value "MDM-maintain" [28, 29]".

V. CONCLUSION

In order to ensure that Master Data interactions adhere to these standards, this paper evaluates the needs for enforcing protection of data in e-Government-based Master Data systems & presents solutions. The overarching objective is to use common MDMS and e-Government platforms to implement effective DP enforcement in inter-organizational scenarios.

The suggested methods include leveraging the e-Government the platform as a shared component to enforce rules and regulate DP compliance by altering data and operational flows. In addition to using established standards (such as XACML and ISO/IEC 8000), these solutions make use of the mechanisms of popular middleware technologies and MDM systems. This continuing work's primary contributions are:

i) Determining the prerequisites for an MDM eGovernment system that is DP aware,

ii) Outlining a standard design for such systems in order to ensure DP, and

iii) Outlining enforcement strategies (like the MD filter). Additionally, this study advances the discussion of compliance with regulations concerns in eGovernment systems.

VI. REFERENCES

[1] W. Van Grembergen and S. De Haes. Implementing Information Technology Governance; Models Practices and Cases. Hershey. United States: IGI Publishing. 2008.

[2] W. v. Grembergen. Strategies for Information Technology Governance. United States: Idea Group Publishing. 2004.

[3] ISACA. Cobit5: for Information Security. ISACA. 2012.

[4] G. Vreede. D. Vogel. G. Kolfschoten and J. Wien. "Fifteen Years of GSS in the Field: A Comparison Across Time and National Boundaries." in Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03). 2003.

[5] R. Newby. G. Soutbar and J. Watson. "Group Support System Approach." International Small Business Journal. vol. 21. no. 4. pp. 421- 433. 2003.

[6] S. Asch. "Effects of group pressure upon the modification and distortion of judgment." In H.Guetzkow (ed.) Groups. leadership and men. vol. Carnegie Press. p. Pittsburgh. 1951.

[7] A. Rutkowski. B. Van de Walle and G. van den Eede. "The effect of Group Support Systems on the Emergence of Unique Information in a Risk Management Process: A Field Study." in Proceedings of the 39th Hawaii International Conference on System Sciences. Hawaii. 2006.

[8] Yao, L., & Liu, W. (2020). Privacy-preserving governance models for data security in healthcare systems. IEEE Transactions on Industrial Informatics, 16(10), 7012- 7023.

[9] Zhou, X., & Wei, Y. (2018). Integrating security and compliance into enterprise data governance. IEEE Transactions on Data and Knowledge Engineering, 30(9), 1842- 1854.

[10] Choudhary, P., & Sharma, P. (2019). Governance in data security: Challenges and solutions. IEEE Transactions on Cloud Computing, 7(4), 1011- 1023.

[11] Li, J., & Zhang, H. (2020). Implementing data governance in blockchain-based systems for enhanced security. IEEE Transactions on Industrial Informatics, 16(8), 4706- 4718.

[12] Gupta, A., & Rathi, N. (2018). A framework for integrating data security and privacy in data governance. IEEE Access, 6, 30584-30595.

[13] Cheng, W., & Liu, H. (2019). Governance and security integration for scalable data systems: A design approach. IEEE Transactions on Cloud Computing, 8(2), 498- 509.

[14] Feltus, C., Grandry, E. and Fontaine, F.X., 2017. Capability-driven design of business service ecosystem to support risk governance in regulatory ecosystems. Complex Systems Informatics and Modeling Quarterly, (10), pp.75-99.