IJCISR
INTERNATIONAL JOURNAL OF COMPUTING, INTELLIGENCE, AND SECURITY RESEARCH

INTERNATIONAL JOURNAL OF COMPUTING, INTELLIGENCE, AND SECURITY RESEARCH (IJCISR)

Available Online @
ijcsir.fmsisndajournal.org.ng
IJCISR 2(1) 2023
Original Research

AN ANALYSIS OF DATA PROTECTION REGULATION COMPLIANCE MONITORING AND ENFORCEMENT

[1]Joshua J. Tom, [2]Adigwe Wilfred, [3]Nlerum P. Anebo, [4]Bukola A. Onyekwelu
[1,4]Department of Cyber Security, Elizade University, Ilara Mokin, Nigeria,
[2]Department of Computer Science, Delta State University of Science and Technology, Ozoro, Nigeria,
[3]Department of Computer Science, Federal University Otuoke, Nigeria

Abstract

Organizations using customer data have the obligation to protect privacy of personal data in their databases. The assurance of customers' data privacy is subject to sound data protection policies. These policies are drawn by government and its agencies to achieve adherence to respecting the data privacy rights of citizens. Data protection regulation is not an end but a means to achieving protection of data privacy of customers. There are several data protection regulations like the European General Data Protection Regulation (GDPR), HIPAA, SOX, Payment Card Industry Data Security Standard (PCI DSS), California Consumer Privacy Act (CCPA), and in Nigeria the Nigeria Data Protection Regulation (NDPR). For these regulations to be of impact there must be mechanisms to ensure adherence to the data protection regulations. This mechanism must provide for the monitoring of data controllers' regulatory compliance with data regulations. In this paper, we analyze data protection compliance and enforcement model based on semantic web ontology and discuss how the NDPB can seamlessly monitor and enforce compliance of data protection regulation. The contribution of this paper is conceptualizing a model for checking the compliance of data processing agreements with NDPR to ensure maximum compliance checking with minimum effort and help to identify companies and organizations with low compliance. The modelling of data protection regulation compliance monitoring has promising results in ensuring compliance with relevant laws and regulations governing the handling of sensitive data. The model can facilitate effective tracking and monitoring of data usage, alerts the appropriate authorities in case of breaches, and generates reports for audits and compliance verification. Based on the analysis in this paper, there is promising possibility of fully developing an automated system to reduce the margin of error and increased the efficiency of the monitoring process, allowing organizations to better safeguard sensitive data and avoid hefty fines for non-compliance.

Keywords: Data Privacy, Compliance Enforcement, Data Protection Regulation, Automation, Ontology, Semantic Web

INTRODUCTION

Data protection regulation is very important to ensure the protection of individuals' data privacy as they access critical internet-based services. These services are offered by both private and government owned companies and organizations such as hospitals and other health providers, banks and other financial institutions, online loans, online shops, online payment providers, etc. All these services are vital to the survivability of an individual in the modern society; hence an individual has no alternative, but to embrace and leverage the abundant benefits brought by the internet technology. Arguably, this technology has caused a shift from the industrial revolution to the age of information revolution (Odusote, 2021), but not without its attendant challenges as private data are collected, processed, stored, and transmitted across the internet characterized as an insecure communication channel. Abuse or misuse of private data can cause severe harm to the data owners if proper measures are not put in place by the data holders to safeguard the security and privacy of the data owners. For example, data abuse, misuse or breach can lead to grave consequences including the data owner suffering depression, discrimination, loss of self-dignity, stigmatization, etc. On the other hand, companies and organizations that collect and use customer data also stand a risk as a result of litigation, loss of revenue, loss of trust and reputation, for example, Facebook and Cambridge Analytica faced severe plague in 2019 as a result of data misuse and failure to protect confidential information. Therefore, government whose responsibility is to protect the fundamental rights of all citizens including privacy of information must ensure that the activities of those in the business of customer or consumer data use are monitored and controlled. Such monitoring and control require effective regulations and policies to be put in place to ensure that the data users (companies and organizations) only use such data ethically. The regulations and policies help to point out accepted ethical standards governing the handling of customer data depending on the industry. Regulations specify obligations and prohibitions (Esayas and Mahler, 2015) for companies and organization. Obligations consist of actions which companies and organizations must carry out in order to comply with regulations and prohibitions consist of actions that should never be performed. For instance, there are obligations and prohibitions for companies and organization in the financial sector that collect, process, transmit and store user credit card payment information. These obligations and prohibitions are spelt out in the PCI DSS. Similarly, companies and organizations in the health sector are to adhere to and comply with obligations and prohibitions as spelt out in the Health Insurance Portability and Accountability Act (HIPAA). Compliance refers to the set of norms, rules, and regulations that a business process must adhere to. These include obligations such as legal or contractual duties, prohibitions that dictate what actions should be avoided, and recommendations that offer best practices and guidelines. Failure to comply with these normative positions can result in legal consequences and financial penalties. Therefore, it is crucial for businesses to understand and implement compliance measures to ensure their adherence to industry standards and regulations.

OVERVIEW OF NIGERIA DATA PROTECTION REGULATIONS (NDPR)

NDPR was the brain child of the National Information Technology Development Agency (NITDA) which came into effect on January 25, 2019 as a subsidiary legislation with its root from the NITDA Act 2007 section 6. Before this time, Nigeria never had any policy instrument focused on data privacy and protection. However, issues on data protection were only sparingly mentioned in section 37 of the Nigerian constitution 1999 as amended, the National Identity Management Commission (NIMC), National Human Rights Commission (NHRC), etc. Data protection was not the primary concern of any of the bodies mentioned. Hence, the realization of the huge deficiency in data protection in Nigeria creation of the NDPR as a Nigerian version of the General Data Protection Regulation (GDPR) created to address data privacy issues by the European Union. To again acceptance of the international community of Nigeria's data protection law, the Federal government of Nigeria on February 4, 2022 established the Nigeria Data Protection Bureau (NDPB), an independent authority saddled with the responsivity of ensuring that Nigeria has a principal legislation for enabling data protection and privacy. By virtue of section 64 of the Nigeria Data Protection Act 2023 signed into law on June 12, 2023 by President Bola Ahmed Tinubu, the NDPB is expected to metamorphose into an independent (powered by Section 7) National Data Protection Commission (NDPC), which will be responsible for enforcement of rules and regulations set out in the Act, regulation of the processing of personal information, and other related matters. The Governing Council of the NDPC has been charged with formulation and provision of overall policy direction of the affairs of the NDPC. The Act provides a legal framework for the regulation of personal data in Nigeria. The objectives of the Act include (1) safeguarding of fundamental rights, freedoms and interests of data subjects as guaranteed under the Constitution of the Federal Republic of Nigeria and regulation of processing of personal data to ensure that it is processed in a fair, lawful and accountable manner and protecting data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subjects' rights.

In order to ensure effectiveness in administering the rules of NDPR and manage compliance of the data protection regulations, the NDPB is empowered by a provision in the NDPR to appoint and license Data Protection Compliance Organizations (DPCO) in Nigeria. These organizations are to monitor, audit, conduct training, and provide data protection compliance consulting to all Data Controllers in Nigeria.

NDPR PROCESSING OF PERSONAL DATA

As specified in the NDPR, the processing of personal data of Nigerians by any organization operating within Nigeria is governed by clear general principles (NITDA, 2020) that 'personal data' must be:

i. collected and processed in accordance with a specific, legitimate and lawful purpose consented to by the data subject
ii. adequate, accurate, and without prejudice to the dignity of the human data subject
iii. store only for the period within which it is reasonably needed; and
iv. secure against all foreseeable hazards and breaches such as theft, cyberattacks, viral attack, dissemination, manipulation of any kind, and damage by any natural elements.

The above provisions for the processing of personal data gathered by organizations in Nigeria is synonymous with the European GDPR data protection principles which include lawfulness of data processing, data minimization, accuracy and adequacy of data processing, personal data storage and retention, and confidentiality and security of personal data as specified in Article 2 of the regulation. Details of the specification of the data processing principles can be obtained in NDPR (2020). The NDPR also made provision for the rights of the data subjects including right of the data subject to be informed of the processing activities, right to objecting to the processing of personal data, right to be forgotten, etc. A novel effort by the NDPR is its provision for compliance and enforcement through the NDPR compliance framework, which resulted in the creation of Data Protection Compliance Organization (DPCO). The NDPR compliance framework is the cornerstone or the main motivation for developing compliance enforcement model in this paper. This framework ensures proactive monitoring and evaluation through analytics of the huge personal data to identify patterns that reflect any non-compliance.

DATA PROTECTION COMPLIANCE ORGANIZATIONS IN NIGERIA

DPCO is an entity duly licensed by the Nigeria Data Protection Bureau (NDPB) for training, auditing, consulting, and rendering services and products for compliance with the NDPR or any foreign Data Protection Law or Regulation having an effect in Nigeria as in Article 1.3 subsection xiii of the NDPR. The 2023 Nigeria Data Protection Act signed into law by Tinubu-led administration in Nigeria empowers the NDPB to register and license suitable DPCOs to monitor, audit, conduct training and offer data protection compliance consulting to data controllers. Organizations qualified to be registered as DPCOs include law firms, IT service providers, and professional service consultancy firms. The DPCOs are saddled with strategic responsibilities such as providing data protection compliance and breach services for data controllers and administrators, data protection training and awareness, data privacy breach impact assessment amongst other roles. In furtherance of the importance of compliance with the NDPR by organizations and companies doing business in Nigeria, data controllers are compelled to read and understand the provisions of the NDPR, develop and implement an NDPR-consistent privacy policy, notify employees, customers, and visitors to its web sites of its privacy policy and appoint staff member(s) as data protection contacts points. Failure to adhere to these requirements may render the defaulter liable to fines by NDPB in line with the provisions of the NDPR and such companies or organization may also risk not being included in the National Data Protection Adequacy Programme (NaDPAP) whitelist. DPCOs carry out compliance obligations on behalf of the data controller. The strategic role played by the DPCOs in the data cycle is inevitable and as such organizations and companies must prioritize leveraging DPCOs' services where they cannot appoint Data Protection Officers or comply with the provisions of the NDPR by themselves.

SEMANTIC WEB BASED MODELS

Introduced by Tim Bernes-Lee and Tim O'Reilly, semantic web is an extension of the current web going one step further to give information well defined meaning (Berners-Lee et al., 2001). Semantic Web is the web of connections between heterogeneous data forms with the capability of allowing the data to be machine-readable. Hence, this advantage of the semantic web can be leveraged to link the disparate and heterogeneous data schemas into a unified structure which can permit access to dissimilar databases distributed across different companies and organizations with business interests. The Semantic Web provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries. The semantic web provides an extension of the traditional web with the capabilities of giving well defined meaning to information, which enables machines to work in synergy with humans (Berners-Lee et al., 2001). An interesting advantage of the semantic web technology is data integration and task automation (Cho and Lee, 2006). This allows possible viewing of databases maintained at different locations across the internet as a unified database. The different forms of semantic technologies constituting building blocks of a semantic web as shown in figure 1.

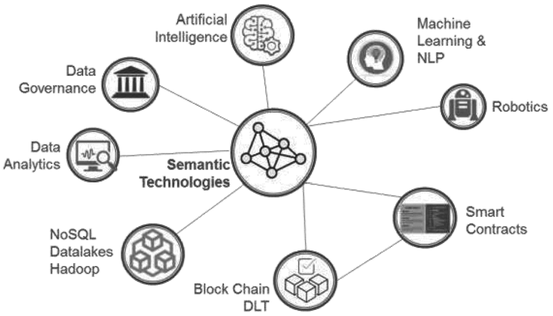

Fig. 1: Components of Semantic Web Technologies. (Adapted from the W3C)

A semantic web is made up of Resource Description Framework (RDF), some Data Interchange Format, notations, and the Web Ontology Language (OWL). These components are collectively providing resources to make a formal description of concepts, terms, and relationships as it applies to a given domain. Figure 2 shows the hierarchical structure of a semantic web.

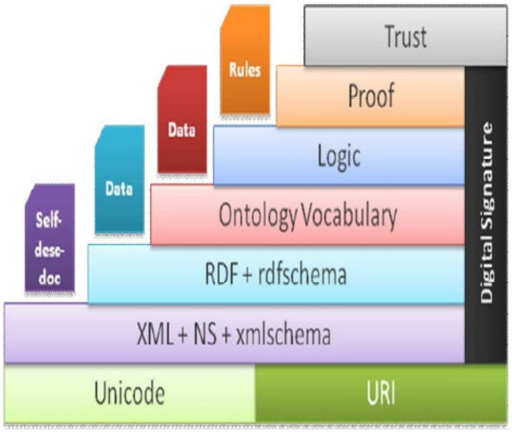

Figure 2: Architectural Structure of Semantic Web

The structure has the uniform resource identifier (URI) and the Unicode as the foundation of the semantic web architecture. On top of the foundation is the data interchange format (e.g., XML, NS, XMLSchema. This level is followed by the RDF and the RDFSchema, which is later followed by the Ontology vocabulary, etc. This architecture provides software platforms with machine-interpretable metadata of user collected data stored in varied databases by different organizations. With this capability, a semantic web-based model enables systems to make meaningful representations in way similar to human information processing, where meaningful inferences could be made out of data.

NDPR COMPLIANCE ENFORCEMENT MECHANISM (N-CEM)

The goal of NDPR enforcement is to encourage compliance with the NDPR rules concerning the handling of customers' personal data collected for a variety of reasons and purposes. Instituting an effective compliance model with adequate efficiency in dealing with the many forms of expected or unexpected non-compliance often requires different options or a combination of options. A better approach is combining options to take advantage of their respective strengths. Forms of enforcement as provided for in the NDPR include surveillance, compliant filling, investigation, serving notice of enforcement/administrative penalties and criminal prosecution. An automated means of monitoring compliance falls in the surveillance category. Surveillance is a specific and deliberate approach to monitoring compliance to identify breach of the NDPR requirements. Conducting routine surveillance is informed by the believe that there may be a deliberate or non-deliberate breach of the provisions of NDPR by parties who have the legal obligations to perform specific tasks in accordance with NDPR requirements with respect to the data subjects. The basic principles which embody the main ideas of the NDPR include (i) lawfulness, fairness, and transparency; this entails having valid reasons for collecting and processing data and obtaining consent from data subjects before their personal data could be processed. (ii) purpose limitation, this requires that data should be collect and processed only for the specified, explicit, and legitimate purpose (iii) data minimization specifies that data processors collect adequate and relevant data that is limited to what is necessary for the purpose of data processing (iv) data accuracy requiring that collected data is accurate and updated. Others include storage limitation specifying the need for the data controllers to hold personal data only for specified duration, integrity, confidentiality and accountability.

REVIEW OF RELATED WORKS

Misuse of customer data and data theft can lead to breach of data privacy especially as the internet has gained a tight grip on operations of most companies and organizations due to their embracing online presence through adopting online operations and the cloud. Odusote (2021) examines data misuse and date theft with regards to data protection regulation in Nigeria including areas that are yet to be taken care of by legislation and makes recommendations for a way forward. Odusote drew attention to the fact that, even though very laudable initiatives have been put forward and encouraged by government for the betterment of the citizens, enough has not been done to protect the data privacy of the stakeholders (data owners) especially as these initiatives elicit and store user data in its repositories for services to the users. The author enumerated several challenges of NITDA's and later NDPB's data protection efforts in Nigeria to include the restrictiveness of the NDPR in addressing data privacy concerns, inadequate legislative provisions against cybercrime practices, little or no awareness to the sensitivity of user data and the need to protect such data, data breaches and cyber incidence non reportage, and low compliance as result of data protection regulatory enforcement and supervision. Among the recommendations made in the paper, is the setup of body to ensure that companies and organizations doing business in Nigeria comply with the data protection regulation requirements without which the regulations would be as useless as a toothless lion.

Using the Unified Modelling Language (UML) and Object Constraint Language (OCL), Torre et al. (2021) built a model-based representation of the European's GDPR, a first attempt at creating an automated model based GDPR compliance solution. In the paper, the authors developed a two-tiered description of the GDPR, made up of a generic GDPR model and a well-defined strategy for specializing this model. The generic tier consisted of GDPR concepts and principles of GDPR as applicable to different contexts, while the specialized tier describes how the generic tier is localized to a specific concept. This serves as a first step towards the design of automated methods for checking GDPR compliance. The GDPR model is built with machine analytic capability using a model driven engineering (MDE) to provide effective communication between IT experts and domain professional.

Kammueller (2018) investigated the implications of GDPR on IoT enabled healthcare system design. This investigation was triggered by the expected data breaches in the system. To enable the proof of compliance to the GDPR, the work proposed a solution based formal modeling and analysis using interactive theorem proving. The paper demonstrated the use of logical modelling and machine assisted verification supporting data protection by design.

Though data stored in a blockchain enabled system is immutable, situations exist where data owners should have the right to change or delete their data and probably must consent to how their private data are processed and used. This consideration in protecting data is necessary requirement to ensure individual's right to rectification and the right to be forgotten after a transaction in an information system. Based on this realization, Gonçalves et al. (2023) gave a description of the design of a system to use and process survey data to comply with the GDPR requirements. Their propose design employs an Hyperledger Fabric blockchain and an InterPlanetary File Systems, the former serving to ensure no tampering of data, while the latter is for storage. The use of the blockchain technology provided immutability without contravening the GDPR regulations.

With the GDPR enforcement of regulations to protect user data, has been a significant study in the area of data protection and attendant technical challenges created by GDPR's articulation of data protection by design. Chhetri et al. (2022) presents a scalable design tool for automating data protection regulation compliance. The tool allows compliance checking and carrying out audits of data handling based on the data owners' consents modelled using knowledge graph. In the design, compliance checking is achieved by implementing a regulation-to-code process. This translates GDPR regulations to technical and organizational measure and source code. The authors demonstrate the effectiveness of their design in the context of smart cities, insurance, and highlight ways in which the tool can be adapted to other domains.

With the data protection drive by data protection regulatory agencies extended to Online Social Networks (OSN) due to recent scandals of abuse of users' personal data, GDPR presents OSN providers with a stream of data protection compliance requirements to protect against user data abuse and misuse. Ahmed et al. (2020) investigates the link between GDPR provisions and the use of the blockchain technology in solving the content management problem in OSN and identified key characteristics of the blockchain technology that facilitate regulatory compliance. The main focus of the paper is the opening up of research directions in the use of blockchain disruptive technology to achieve regulatory compliance in the domain of OSN.

Zhou et al (2022) proposed a natural language processing (NLP)-based semantic framework to implement rules-based automated compliance checking for modelling building information at the design stage. In their model, semantic-based information was extracted and analyzed using NLP methods to generate conceptual ontology objects collectively enabling rule classification through its corpus basis. With this model, cross operation from varied data sources is improved by the isomorphic nature of the information from these sources due to semantic integration of the differentiated data.

PROPOSED COMPLIANCE MONITORING ARCHITECTURE

Uncontestably, the framework for the EU's GDPR enforcement of compliance provides the highest standard of data protection for European countries and in some countries worldwide where the GDPR is adopted for regulating data protection (Hoofnagle et al., 2019). This is because GDPR give very high priority to compliance and enforcement. Based on this high premium placed on enforcement by the GDPR, this paper finds it a necessity to model an automated approach to monitor and enforce compliance of data protection regulations in Nigeria. The idea behind this modelling is predicated on the need for the NDPB to be in a pivotal position, which provides a centralized platform for assessing and monitoring the web content and databases of data controllers. This need for a centralized monitoring requires an implementation of a federated database architecture wherein the individual enterprise databases are coordinated into a single repository with regular updates for assessment and compliance checking by the regulators. The federated data governance approach provides an avenue for achieving data privacy, compliance, and security, which is essentially one area that screams out for centralization. This way, the NDPB can simultaneously discover noncompliant data across companies and organizations and apply sanctions immediately. With federated data, information from the different companies' databases collected by the DPCOs are combined and integrated into a single virtual repository eliminating storage duplication. This brings all the data together while the control of the respective enterprise databases still resides with the data controllers. This allows us to define data protection regulations centrally, while not disturbing the autonomy and resources of the local domain. The architecture gives the NDPB access to customer data collected by different data controllers on the fly eliminating the need to run after data controllers, while trying to find out whether a data controller adheres to the data protection regulation. In this section, we show the main components of our model in figure 3.

The conceptualized model as shown in figure 3 is fully explained here. The structured processing of rules component aims to ensure that organizations comply with the regulations and guidelines set by data protection authorities by using a set of predefined rules to monitor and assess an organization's compliance level regularly. The output of this process provides insights into areas where the organization needs to improve and helps them take corrective action before any violations happen. Compliance checking also need a way of getting relevant regulatory information. In order to establish an accurate model, it is necessary to extract relevant information from data. In this process, reliable and consistent regulations must be put in place to ensure the accuracy and integrity of the data. This information extraction requires careful consideration of the type of data being analyzed, as well as the goals of the model. By establishing a clear understanding of the relevant data and regulations, a robust and reliable model can be developed to provide insights into the underlying trends in the data. During the rule execution phase of data regulation compliance monitoring, the defined rules are applied to the relevant data to determine whether any violations have occurred. This involves analyzing data from various sources and comparing it against the rules set forth by the regulatory frameworks. If any violations are detected, they are flagged for further investigation, and corrective action can be taken to remedy the situation and bring the organization back into compliance. The rule execution phase is an essential part of ensuring that organizations adhere to regulatory requirements and protect sensitive data from unauthorized access or misuse. Finally, the compliance checking results phase is a crucial part of data regulation compliance monitoring. In this phase, the monitoring team analyzes the data collected in the previous phases to determine whether the organization is compliant with data regulations. This includes reviewing policies and procedures, assessing data security measures, and evaluating the organization's procedures for responding to data breaches. Based on the results of the compliance checking, the monitoring team will provide recommendations for any necessary changes or improvements to the organization's data management practices. This phase ensures that the organization is aware of any compliance risks and is taking active steps to mitigate them.

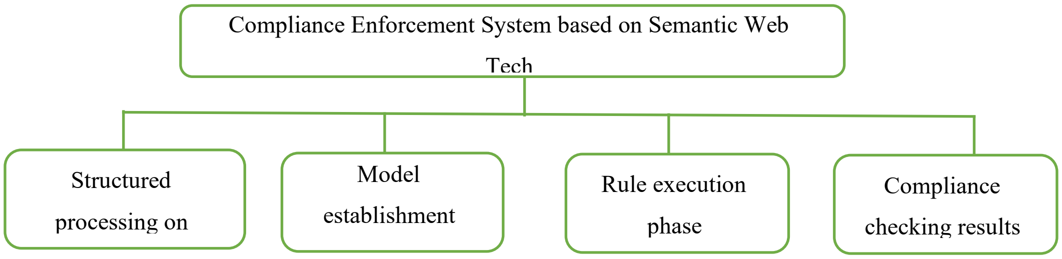
Compliance Enforcement System based on Semantic Web Tech
Structured processing on
Model establishment
Rule execution phase
Compliance checking results

Fig. 3: Phases of the Conceptualized Model

RESEARCH METHODOLOGY

This study proposes a methodology for automating compliance monitoring using semantic web and ontology. The approach uses ontologies to represent compliance regulations and policies, and semantic web technologies such as SPARQL queries to extract data from regulatory documents. The proposed methodology is designed to improve the efficiency and effectiveness of compliance monitoring by reducing manual labor and time spent on traditional compliance monitoring methods. The study shows that the automation of compliance monitoring using semantic web and ontology can lead to more accurate and timely compliance monitoring, making it possible for organizations to avoid legal and financial penalties. To achieve this, we first create of a knowledge base that captures regulations and compliance requirements which are then transformed into formal semantic representations for automated reasoning and consistency checking against the regulatory knowledge base. The compliance checking algorithm scans and analyzes this knowledge base to ensure compliance with relevant laws and regulations as stipulated by NDPR. Using semantic web and ontology, the algorithm assesses data security measures, identify potential gaps and vulnerabilities, and recommend appropriate actions to address them. The architecture for our automated compliance checking algorithm for data protection regulation is as shown in figure 4 and consists of a set of rules or criteria based on the specific regulations in question. The algorithm scans data sets and processes to identify any potential violations of the regulations and flag them for review. This could involve machine learning and natural language processing to interpret complex legal language and adapt to changing regulations.

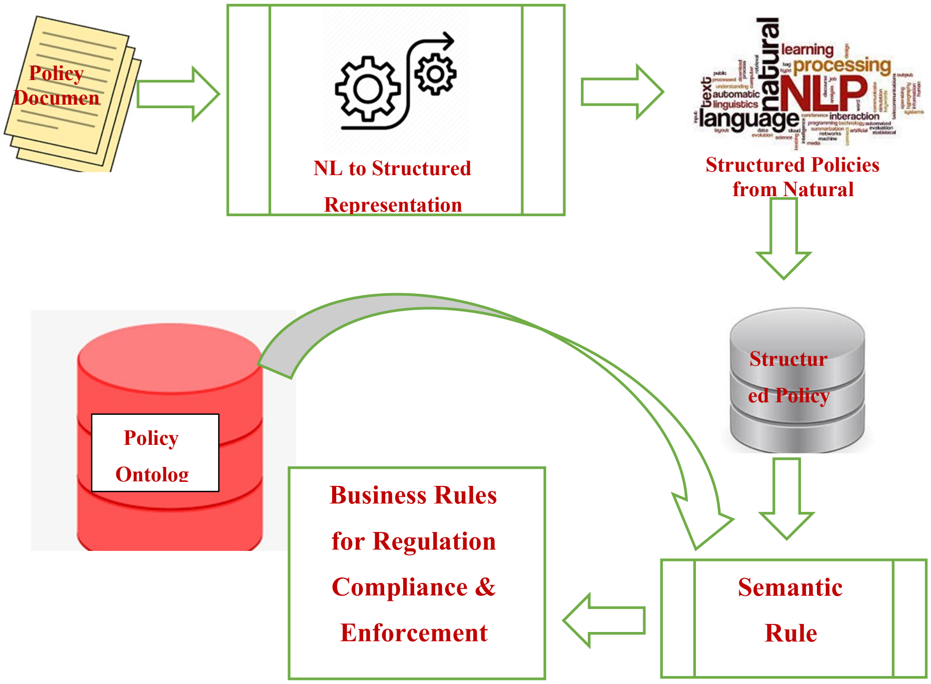

Fig. 4: Proposed Regulation Compliance and Enforcement Model

Ontology for Data Protection Regulation Compliance

An ontology for data protection regulation compliance is a structured representation of the concepts, entities, and relationships involved in complying with regulations governing the protection of data. It includes definitions of key terms, models of the regulatory framework, and rules for interpreting and implementing regulations. The ontology provides a framework for understanding and managing compliance obligations, including requirements for data processing, data subject rights, and data protection impact assessments. It also supports the development of automated compliance systems, enabling organizations to manage and monitor compliance more effectively and efficiently.
Ontology can be used to define relevant regulations, rules and policies in a machine-readable format by creating a formal vocabulary that represents the concepts and relationships of these rules. This vocabulary can then be used to create an ontology that models the domain of regulations and policies. The ontology can specify the rules in a structured and consistent format, making it easier for machines to process and understand the regulations. By standardizing the representation of regulations, rules and policies, ontology can facilitate the automatic detection and enforcement of compliance, reducing the burden on human intermediaries

The Nigeria Data Protection Regulation (NDPR) is a set of legal and regulatory requirements aimed at protecting personal data in Nigeria. Some of the concepts outlined in the NDPR include the definition of personal data and sensitive personal data, the obligations of data controllers and processors, the rights of data subjects, the requirement to obtain consent for the processing of personal data, the need for adequate security measures, and the penalties for non-compliance. The Nigeria Data Protection Regulation (NDPR) states that any natural person or legal entity that processes personal data in Nigeria is subject to the regulation. This includes data controllers, data processors, data subjects, and data protection officers. Additionally, the NDPR applies to entities involved in cross-border data transfer, such as data exporters and data importers. Other relevant entities include law enforcement agencies, government agencies, and other public authorities that process personal data, as well as data protection agencies responsible for enforcing the NDPR.

The Nigeria Data Protection Regulation outlines various relationships between stakeholders involved in data processing activities. It establishes the relationship between data subjects and data controllers, the relationship between data controllers and data processors, and the relationship between data processors and sub-processors. It also highlights the relationship between data controllers and the National Information Technology Development Agency (NITDA) as the regulatory authority responsible for enforcing the regulation. Additionally, it establishes the relationship between data controllers and data subjects' rights to access and control their personal data. These relationships are critical to ensuring compliance with the regulation and protecting the privacy rights of data subjects in Nigeria.

Our methodology outlines three deontic concepts, which refer to ethical principles or duties that individuals should follow. These concepts include obligations (the actions individuals must do), permissions (the actions individuals are allowed to do), and prohibitions (the actions individuals are not allowed to do). By categorizing actions in this way, we can more effectively assess and analyze the ethical implications of different behaviors

An ontology for obligations, permissions, and prohibitions in data protection regulation would include a structured representation of the legal requirements placed on data controllers and processors. It would define the types of personal data that can and cannot be collected, processed, and shared, as well as the rights of the data subjects. The ontology would also specify the obligations and duties of both the controller and the processor, as well as the sanctions and penalties for non-compliance. Such an ontology would help organizations to better understand and comply with data protection regulations and could also facilitate automated compliance monitoring and auditing. The ontology policy is designed to formalize NDPR's regulatory context to aid sharing and reuse of synthesized knowledge for future decision making. We present an ontology with a number of NDPR concepts grouped in three subcategories (permission, obligation, and prohibition) and equal number of relationships.

Technologies for Implementation

The semantic web ontology-based compliance monitoring model in this paper comprises three main components: a compliance ontology, a monitoring engine and a compliance dashboard. The compliance ontology defines the relevant regulations, rules and policies in a machine-readable format using Web Ontology Language (OWL). This ontology consists of concepts, categories, and relationships that define compliance requirements and standards. The system utilizes this ontology to model NDPR compliance. The monitoring engine uses semantic reasoning to evaluate compliance against the ontology and identify non-compliant areas and generates alerts for non-compliance as earlier shown in figure 4. Semantic involves using logic and rules to interpret data and identify compliance issues. By analyzing the meaning and context of information, the model can detect potential violations and alert organizations to take corrective action. The model is designed to ensure that data processing activities are carried out in accordance with the applicable regulations and standards, and safeguard the privacy and security of personal information. The compliance dashboard provides a user-friendly interface for visualizing compliance status and detail. Together, these components enable effective and efficient compliance monitoring and management in complex regulatory environments.

SPARQL is a standardized language used for querying Linked Open Data and databases that use RDF (Resource Description Framework). It serves as a protocol for accessing data and allows users to specify complex queries across data sources. SPARQL enables users to access and manipulate data using standardized syntax and semantics, making it a valuable tool for enterprises or organizations that require advanced data access and utilization. The use of SPARQL based database for data protection regulation compliance monitoring model is crucial towards ensuring the protection of personal data. The database allows for effective tracking and monitoring of compliance with data protection laws and regulations, providing organizations with the necessary tools to ensure they are fully compliant. The use of SPARQL enables efficient querying and retrieval of information, facilitating compliance monitoring through the identification of non-compliance issues. The database will promote transparency and accountability, safeguarding the rights of individuals and enhancing trust in organizations' handling of personal data. SPARQL can be used in a data protection regulation compliance monitoring model to query and analyze data. It can be used to retrieve and filter data from different sources, enabling organizations to assess their compliance with data protection regulations. SPARQL queries can be designed to check if personal data is being processed lawfully, if consent has been obtained, if data subject rights are being respected, and if appropriate technical and organizational measures are in place.

DISCUSSION

It is extremely important that NDPB (Data Protection Regulators in Nigeria) be able to automatically check data protection regulatory compliance by the various data controllers and data processors in Nigeria. This would facilitate trust between the data owner, data controllers, and regulators. For this to be achievable, the DPRB must have real-time access to data processor' and controller' systems. In this paper, the use of semantic web and ontology were proposed which provide a joint language and standard for monitoring compliance by mining customers' personal data across heterogeneous platforms and systems. Semantics has to do with the linguistic and philosophical meaning of concepts and constructs in languages (be it human language or programming language), formal language, and semiotics. An ontology uses triplets to show relationships between concepts in a particular knowledge domain (Elluri and Joshi, 2018). Semantics web and ontology are important building blocks of a semantically based regulatory compliance system. The inferential intelligence of semantic technologies and ontology of regulatory concepts was leverage on to build an automated system for NDPR compliance checking. We acknowledged that there are several challenges in building a semantic web ontology-based system to automate data regulation compliance monitoring in this paper. These challenges included the lack of standardized compliance regulations, the difficulty in mapping different regulations to ontologies, the need for constant ontology maintenance, the complexity of integrating multiple regulatory requirements, and the dynamic nature of data compliance regulations. Furthermore, we suggested that integrating natural language processing techniques and machine learning techniques could improve the chances of developing an automated model with high efficiency and ability to handle unstructured data. The implementation of an automated approach to data protection regulation compliance monitoring may be hindered by various factors such as the complexity and ambiguity of regulations, the lack of standardized guidelines and requirements, limited data interoperability and integration across systems, and the need for expertise and resources to develop and maintain the systems. Additionally, privacy concerns and ethical considerations may also arise when using automated monitoring tools, requiring careful attention to ensure transparency and accountability. These challenges may require a collaborative effort among stakeholders in the legal, regulatory, technical, and ethical domains to overcome and enable effective automated compliance monitoring.

CONCLUSION AND FUTURE WORK

The data protection regulatory domain using a systematic and innovative approach made up of (i) semantic analysis of legal texts and rules in the NDPR, (ii) translation of the semantically analyzed rules into a structured natural language, and (iii) mapping this data protection regulatory rules into machine readable representation using ontology engineering was analyzed. This regulatory ontology development would help NDPB to monitor the level of regulatory compliance as well as aid data controllers and processors to assess and apply regulation within the regulatory domain. To the best of our knowledge, our paper is the first attempt towards conceptualizing NDPR compliance enforcement automation which will eventually contribute to the development of smart regulation compliance enforcement models.

In the future, an automated approach can be developed to streamline the enforcement of NDPR compliance, which integrates data privacy regulations with monitoring and reporting mechanisms. The system should be able to scan websites and applications for possible violations, generate real-time alerts, and provide actionable insights for remediation. Additionally, the automation system should provide a centralized dashboard for tracking compliance progress, conducting audits, and generating reports. Implementation of such a system would help organizations ensure NDPR compliance while minimizing the risk of possible penalties and data breaches. We also recommend combing existing ontology building methodologies such as LOT (2022), Methontology (1997), Ontolingua, and the Enterprise model approach, etc. for more efficient compliance and enforcement management.

REFERENCES

Odusote, A. (2021) *Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation*. Beijing Law Review, **12**, 1284-1298. doi: 10.4236/blr.2021.124066.

Esayas, S. Mahler, T. (2015). *Modelling Compliance Risk: A Structured Approach*. Artificial Intelligence Law **23**, 271–300 https://doi.org/10.1007/s10506-015-9174-x.

Torre, D., Alferez, M., Soltana, G. et al. (2021). *Modeling data protection and privacy: application and experience with GDPR*. Software and Systems Modeling, 20, 2071–2087. https://doi.org/10.1007/s10270-021-00935-5.

Kammueller, F. (2018) "*Formal Modeling and Analysis of Data Protection for GDPR Compliance of IoT Healthcare Systems*" 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, pp. 3319-3324, doi: 10.1109/SMC.2018.00562.

Martins Gonçalves, R., Mira da Silva, M., &Rupino da Cunha, P. (2023). *Implementing GDPR-Compliant Surveys Using Blockchain*. Future Internet, 15(4), 143. https://doi.org/10.3390/fi15040143.

Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). *Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent*. *Sensors*, *22*(7), 2763. https://doi.org/10.3390/s22072763.

Ahmed, J., Yildirim, S., Nowostawski, M., Abomhara, M., Ramachandra, R., Elezaj, O. (2020). *Towards Blockchain-Based GDPR-Compliant Online Social Networks: Challenges, Opportunities and Way Forward*. In: Arai, K., Kapoor, S., Bhatia, R. (eds) Advances in Information and Communication. FICC 2020. Advances in Intelligent Systems and Computing, vol 1129. Springer, Cham. https://doi.org/10.1007/978-3-030-39445-5_10.

Godyn, M., Kedziora, M., Ren, Y. *et al.* (2022). *Analysis of solutions for a blockchain compliance with GDPR*. *Sci Rep* **12**, 15021. https://doi.org/10.1038/s41598-022-19341-y

Hoofnagle C. J. Bart van der S. and Frederik Z. B. (2019): *The European Union General Data Protection Regulation*. What it is and What it Means '28(1) ICTLJ 65.

Petkova, T. (2016). *"A Web of People and Machines: W3C Semantic Web Standards.*" Ontotext, March 24. Accessed 2018-05-25.

Zhou, Y., She, J., Huang, Y., Li, L., Zhang, L., & Zhang, J. (2022). *A Design for Safety (DFS) Semantic Framework Development Based on Natural Language Processing (NLP) for Automated Compliance Checking Using BIM: The Case of China*. *Buildings*, 12(6), 780. MDPI AG. Retrieved from http://dx.doi.org/10.3390/buildings12060780.

Berners-Lee, T., Hendler, J., and Lassila, O., (2001). *The semantic web*. Scientific American, 284 (5), 34–43.

Nam-deok C. and Eun-ser L. (2006). *Design and Implementation of Semantic Web Search System Using Ontology and Anchor Text*. Workshop on Approaches or Methods of Security Engineering (AMSE 2006, Sess. B).

Marwane E. K. and Elke P. (2009). *A Semantic Framework for Compliance Management in Business Process Management*. Conference: Business Process, Services Computing and Intelligent Service Management, Leipzig, Germany.

Elluri, L. and Joshi, K. P. (2018). "*A Knowledge Representation of Cloud Data Controls for EU GDPR Compliance*," 2018 IEEE World Congress on Services (SERVICES), San Francisco, CA, USA, 2018, pp. 45-46, doi: 10.1109/SERVICES.2018.00036.

NITDA, (2020). *Nigeria Data Protection Regulation 2019*: Implementation Framework, July 2020.

Poveda-Villalón, M., Fernández-Izquierdo, A., Fernández-López, M., & García-Castro, R. (2022). *LOT: An industrial oriented ontology engineering framework*. Engineering Applications of Artificial Intelligence.

Fernández-López, M., Gómez-Pérez, A., & Juristo, N. (1997). *Methontology: from ontological art towards ontological engineering*.