International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

DevSecOps for Enterprise Ontology Platforms: Continuous Validation, Security, and Compliance of Semantic Knowledge Systems

Itendra Kumar Singh

Independent Researcher, USA

ABSTRACT: Enterprise ontology systems are new platforms that have become the main components of intelligent organizations due to the ability to support semantic interoperability, knowledge integration, and decision-making that is based on AI computing across the heterogeneous enterprise systems. However, with the development of ontologies, and an increase in cybersecurity threats, stringent regulatory imperatives require ontological governance approach to be safe and automated throughout ontology lifecycle. The proposed ontology platform of ontology platforms Secure Semantic DevSecOps Framework (SSDF) in an enterprise is proposed as a stable ontology engineering, automated semantic validation, and security testing, compliance testing and policy-based deployment, which is run as a single pipeline in the proposed paper. It includes ontology version control, automated consistency checking, initial validation in SHACL and subsequent validation in SPARQL, Semantic vulnerability testing, identity and access control, Knowledge graph security, infrastructure as code and continuous compliance auditing, which is consistent with organizational policy and regulatory policy. The AI-based anomaly detection and automated governance systems also maximize semantic integrity, and minimize human effort. By making sure that security and compliance are a critical component of all the software development life, and not an activity performed after the software has been deployed, the ontology model proposed will allow the secure, scalable and survivable development of ontology to be integrated. It may also allow ontology to evolve quickly besides not being able to trade off data quality and semantic consistency or business governance. The framework is a viable platform to establish powerful semantic knowledge systems, that codesigns the digital transformation of organizations, intelligent automation, simplicable AI and interoperable knowledge-based software, which are built upon the cloud-native and hybrid enterprise architects.

Keywords: DevSecOps, Enterprise Ontology Platforms, Semantic Knowledge Systems, Knowledge Graph Security, Continuous Semantic Validation, Regulatory Compliance

I. INTRODUCTION

With the rapid transformation of businesses towards a more digital world, semantic technologies to characterize, merge and manipulate organizational knowledge have experienced very high consumption. Enterprise ontology systems have now become a constituent building block of current information ecosystems semantic interoperability between heterogeneous applications, databases, cloud services, Internet of Things (IoT) devices, artificial intelligence (AI) systems as well as have been created to support semantic interoperability between enterprise knowledge graphs. In contrast with conventional methods of data integration, ontologies offer clear semantic definitions of objects, relationships, constraints, business rules and further semantic reasoning and discovering knowledge and context specific decision-making activities can be carried out. Ontology-based architectures are subsequently constructed as a growing concern in any type of area such as healthcare, finance, manufacturing, government, education, telecommunications and smart cities where a steady understanding of various information is the key to operational performance and planning [1].

The second wave of application of the enterprise ontologies has repainted the future of the enterprise ontologies more than they are felt as the active storehouse of the knowledge, but an ever-changing collection of semantic assets which aid mission-oriented business operations. In many cases, the underlying ontologies are modified according to the new business requirements, the forces of regulation, new technology, and domain forces. Ontology engineering has now evolved into joint domain engineering, ontology engineering, software development and compliance team undertaking to ensure that majority of enterprise knowledge graphs expand in parallel with integration of various types of internal and external data [2]. Though this kind of continuous evolution increases the nimbleness of organizations, it brings about significant issues on the consistency of ontology, semantic accuracy, version control, security threats and regulatory standards.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

The classical processes of ontology development mainly related to conceptual modeling, ontology alignment, the semantic reasoning and knowledge reuse. Despite the significance of such methodologies in aiding semantic engineering, they tend to make security validation and compliance verification as post-development issues. These sequential methods are no longer back-size to the contemporary cloud-native enterprise systems, with semantic models usually changed and pushed into honesty through continuous integration and continuous deployment (CI/CD) pipelines. The level of enterprise knowledge and ontology subject matter organizations to high operational risk and a high legal risk when violated by late semantic detectors and unauthorized manipulation of ontologies, but also more importantly, when poisoned by attacks on ontology, misconfigured access control policies or regulatory policies.

Meanwhile, the widespread adoption of the cloud computing, microservices, containerization and distributed knowledge graphs architectures has expanded the attack space of enterprise semantic systems. Very delicate in enterprise ontologies are business knowledge, customer issues, corporate relations, health-care records, financial institutions, intellectual property and business policies. Ontological changes, such as malicious change to ontology classes, to object properties, to inference rules, or to semantic relationships can propagate erroneous knowledge, and thus propagate erroneous analytics, broken automated reasoning and flawed AI decisions and regulatory non-conformance by enterprise applications. In addition, deforming graph of semantic knowledge which are interconnected with external sources of data by means of attacks to ontology injection and manipulation of inferences, unauthorized querying with SPARQL besides misusing privileges and leaking information will devastate unless proper security is taken on a routine basis [3].

The concept of DevOps has shifted the sentiment of software engineering in the recent years and has placed software development and IT performances in a single, automated software workflow involving continuous integration, continuous testing, continuous deployment, and continuous monitoring. Based on this paradigm, DevSecOps goes a notch higher and adds to the DevOps the notion of implementing cybersecurity measures into the life cycle of the software development and not the verification that occurs at the end of the process. All stages are associated with software delivery, automated vulnerability testing, policy enforcement, infrastructure-as-code security, identity management, and container security and compliance verification are all interconnected. DevSecops can also help organizations construct and publish safe content of software and quick, without impacting the resilience of the applications as well as regulatory compliance.

Although the success of the operation of DevSecOps is certain to some degree in the context of software engineering, the introduction of DevSecOps in the framework of enterprise ontology platforms is in its dawn. The ontological engineering processes as are currently present rarely include the automated semantic validation as a part of an extension of a continuous security test and compliance audit toolchain. Most of the ontology validation techniques have been largely focused on logical consistency by description logic without taking cognizance of cybersecurity threats, governance policies, ontology provenance, version integrity, semantic access control and persistently regulatory verification. With the increasing AI-based semantic automation, and decision making, in enterprise semantic systems, there is an immediate need to bring formal principles of DevSecOps to bear on semantic assets, knowledge graphs and enterprise ontologies.

The other developing problem is the quality of semantics in the fast development of ontologies. The application of ontologies in the context of various organizations, business units, or external partners is more likely to cause the risk of overlapping concepts and incompatible associations in addition to vocabularies and semantics drift mismatch in modern organizations. Using a hand, ontology is inexpensive to revise (time), and it is easy to add errors, and this cannot easily be scaled to large enterprise-sized knowledge graphs, with millions of entities and relationships. SHACL-based semantic validation and SPARQL-based consistency verification operations and ontology reasoners in addition to AI-friendly anomaly detection can make a substantial improvement in functionality of ontologies and allow continuous integration pipelines. The validation schemes can be included with the DevSecOps operations to allow the organization detect the semantic error right after a change has been implemented and later on, costs in maintenance are lowered, system reliability is enhanced generally.

Another hot topic of enterprise semantic platforms is compliance with regulations. Companies operating across the jurisdictions have to conform to the regulations, including the General Data Protection Regulation (GDPR), health insurance portability and accountability act (HIPAA), the ISO/IEC 27001 or SOC 2 and other regulations governing the industries. Enterprise ontologies arrange progressively emerge as a symbol of business procedures in control, individual information, healthcare education, corporate dealings and company planning. Semantic systems, in its turn, are alleged to be constantly proving it conformity with the transformation in legal and organizational standards. Implementing

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

automated compliance checking into DevSecOps pipeline assists organizations to test ontology governance rules, data classification policies, access-control rules, audit trails, and semantic integrity before being released into production environments.

This paper suggests the Secure Semantic DevSecOps Framework (SSDF) of enterprise ontology platform in order to overcome such challenges. The recommendation merges ontology version control, collaborative ontology engineering, automated semantic validation, SHACL, and SPARQL-based verification, AI-assisted anomaly detection, security vulnerability assessment, identity and access management, infrastructure-as-code security, continuous compliance monitoring, policy enforcement and automated deployment into a single DevSecOps pipeline. The framework provides organizations with the chance to build rapidly enterprise knowledge systems without the negative effect on semantic accuracy, cybersecurity or regulatory fidelity as semantic validation, security checks and governance are implemented throughout the entire ontology lifecycle.

By sealing the gap between the state of ontology lifecycle management that currently exists and devsecops, secure semantic engineering will be enhanced with the proposed framework. It enforces continuous updating of ontologies and the guarantee semantic consistency, the integrity of knowledge graphs, secure deployment and compliance-by-design. The framework also provides an environment of credible enterprise semantic ecosystem that can provide explainable artificial intelligence, intelligent automation, shareable knowledge interoperability and data-driven digital transformation. With more business-related applications moving to semantic technologies to drive next-generation AI applications, introducing DevSecOps into ontology engineering is a tactical move towards resilient, scalable and secure semantic knowledge systems.

II. LITERATURE REVIEW

Enterprise ontology platform and semantic knowledge systems have stolen the limelight as the enabler of intelligent cybersecurity analytics, knowledge integration and automatic decision support. The development of ontologies, knowledge graphs, semantic reasoning and ontology engineering has provided the underpinnings to the development of secure enterprise semantic infrastructures. Nevertheless, the prevalent literature is much focused on ontology building and cyber threats intelligence and very little focus has been given to integrate DevSecOps practices to ensure ongoing, security and regulatory compliance throughout the ontology building lifecycle.

One of the first ontology-based cybersecurity knowledge graphs frameworks created by Iannacone et al. formalises the representation of cybersecurity entities, relationships and events [1]. They found that the ontology-built knowledge graphs offer semantic interoperability to the heterogeneous source of the security data and enhanced reasoning over cyber intelligence. The proposed ontology though created a gigantic conceptual scaffolding regarding knowledge representation of the issue of cybersecurity did not respond to the present stage of the development of ontology, to automated verification, and business-safe deployment pipelines demanded by the existing business climate.

Besides standardization in ontology Syed et al. developed the Unified Cybersecurity Ontology (UCO) that merged other cybersecurity standards into a common simulacrum [2]. UCO has transcended far by improving interoperability of efforts in security datasets by providing standardized vocabularies of cyber incidents, vulnerabilities, attacks and defensive tools. The framework increased the knowledge sharing and semantic consistency among organizations. However, the UCO more focused on ontology incorporation and semantic interoperability, without looking into continuous security evaluation and automated compliance validation or ontology lifecycle management built in with DevSecOps.

Jia et al. proposed a powerful process to construct cybersecurity knowledge graphs with the help of a semantic integration of formal and unofficial sources of cyber intelligence [3]. In their architecture, they used ontology engineering and recovery of knowledge to enhance the representation of the cyber threat and logical reasoning. The roles of the knowledge graph in the establishment of intelligent threat analysis and judgment were also developed in the analysis. However, the provided architecture did not include the functionality of continuous semantic validation, ontology handling and test-driven security automation and only offered the creation of knowledge graphs.

SEPSES Knowledge Graph by Kiesling et al. is a full-fledged cybersecurity tool that allows unifying heterogeneous data points into a unified semantic framework and system to enhance semantic integration [4]. The proposed platform enabled members of the semantic query of contents, interoperability and sharing of various cyberspace sectors. However, it also showed you how to put knowledge graphs together simultaneously at a large scale, but it did not tely

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

on how to put ontologies into production, manage policies, and even more to verify or monitor compliance at the enterprise scale of DevSecOps.

The second, the Sikos, brought up the topic of OWL ontologies to model cybersecurity and explained the concern of the concept modeling, semantic reasoning, optimal ontological design concepts, and representation of machine knowledge [5]. The paper has shown the way in which ontology engineering can enhance the faculty to formalize cyber knowledge and reason. Although the work had tremendous impact on the semantic knowledge representation, it never addressed the issue of developing ontology securely like security and vulnerability measurement or continuous integration pipelines as opposed to the scenarios addressing ontology development methodologies.

Credibility is an important factor in a semantic system, Sikos and Philp explored the knowledge representations credibility with provenance awareness and contextualising knowledge graphs with a view to enhance the reliability of the data and semantically transparent knowledge [6]. Their study highlighted provenance modeling as an important tool to ensure the authenticity, auditability, and traceability of data in knowledge graphs. The ontology governance encompasses provenance-sensitive architectures, but did not involve the automated compliance validation and DevSecOps-oriented continual semantic validation during ontology development.

A STIX-based ontology modeling framework of building network security knowledge graph using such a design of standard cyber threat intelligence representations is proposed by Liu et al. [7]. The design reflected in them as they incorporated semantically security intelligence through modeling to ontology and interoperability of cyber defense systems. The framework increased semantic coherence and standard knowledge representation, however, there were no tools of automated testing of ontology, continuous policy evaluation, and safe implementation in distributed enterprise environments.

Drawing inspiration from post-malware after-action reports, Piplai et al. proposed a framework of automated creation of knowledge graphs in cybersecurity to put the tools of natural language processing and semantic extraction into practice [8]. The approach they took provided insights into how knowledge graphs could be automatically created by using artificial intelligence and better threat intelligence representation and reasoning. Despite the framework having greatly decreased manual knowledge engineering efforts, it was more of an automated knowledge acquisition instead of secure ontology lifecycle management, automation governance or regulatory compliance.

R Sarhan and Spruit proposed Open-CyKG and is an open cyber threat intelligence knowledge graph whose aim is to share cybersecurity knowledge on semantic integrators and linked data technologies [9]. Their results examined the fact that the semantic knowledge graphs were not only helpful in unifying the various sources of cyber intelligence but also allowed more complex queries, using SPARQL and knowledge discovery tools. Though it featured input towards semantic interoperability, ongoing ontology validation, enforcing access-control and secure DevSecOps practice towards developing enterprise knowledge systems were all minimal in the framework.

At Mohamed et al. it was suggested to use RDFFrames, a framework to facilitate easy access of RDF knowledge graphs by machine-learned applications [10]. The framework enabled intelligent analysis of enterprise knowledge graphs and the semantic structures were appropriately maintained through the bridging of the semantic technologies and machine learning procedures through the framework. The incorporation of machine learning and a knowledge graph has potential benefits in support of ontology validation using AI in a number of ways, yet the formatting lacks ontology security, mechanism of enforcement of semantic adequacy or automated management in the course of continuous deployment lines.

In the study by Wang et al. a domain ontology and knowledge graph of social engineering attacks in cybersecurity setting is created [11]. These types of semantic structure facilitated the modeling of behaviors of attackers, attack and mitigation methods and the resultant representations facilitated more accurate reasoning and analysis of cyber threats. Even though the practical value of application of ontology based on cybersecurity is defined in the paper, the interpretation of the domain knowledge modeling played the focal point of the paper goals and not enterprise ontology governance, implementation models of semantic validation and secure deployment.

In recent years, there was KRYSTAL by Kurniawan et al. which is an enterprise audit-based knowledge graph framework that uses tactical attack discovery on such data [12]. The frame work was enhanced to semantically reason and use graph analytics in demonstrating attack patterns and presenting the cybersecurity situational awareness. KRYSTAL has demonstrated how it can generate IP knowledge graphs, with the help of enterprise security

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

surveillance and auto logic. However, the framework was somewhat cautious about threat finding as compared to provision of holistic ontology version control, semantic verification, continued compliance auditing and Lifecycle automation of DevSecOps.

All in all, the literature reviewed has proven great advances in cybersecurity ontologies, semantic knowledge graphs, ontology engineering, provenance management, and intelligent cyber threat analysis. The work done so far has been able to come up with standardized ontologies, methodologies of semantic integration, knowledge graph construction methods and AI-assisted reasoning. Nevertheless, a number of research gaps are still there. First of all, the existing ontology engineering systems rarelessly couple a continuous semantic validation, with an automatic security test. Second, the current knowledge graph solutions do not have much support of ontology lifecycle management by DevSecOps. Third, automated compliance check, policy check, ontology version management, infrastructure-as-code security, and continuous deployment is largely not researched in enterprise semantic platforms. Finally, AI-based anomaly detection and continuous semantic quality assurance have not been embraced entirely in ontology engineering procedures. These shortcomings facilitate the suggested Semantic DevSecOps Framework (SSDF) that involves the recurrent checking, protection instruction, management and compliance operations in the general enterprise ontology life-cycle, thus leading to conventional, scaled and dependable semantic knowledge systems of modern internet enterprises.

III. SECURE SEMANTIC DEVSECOPS FRAMEWORK (SSDF) FOR ENTERPRISE ONTOLOGY PLATFORMS

3.1 Framework Overview

To overcome the limitations of the previous ontology engineering models, the analysis is going to propose a model of the Secure Semantic DevSecOps Framework (SSDF) of Enterprise Ontology Platforms. Semantic ontology engineering, continuous validation, cybersecurity testing, regulatory compliance, governance, artificial intelligence and practically automated deployment are all incorporated within the paradigm as an inherent life cycle of DevSecOps. In contrast to the traditional form of ontology development processes which ontology is operationalised prior to undertaking semantic validation, security testing, proposed structure is undertaken with all the ontology development stages with integration of the security and quality assurance process. This allows organizations to detect semantic inconsistencies, security risk and compliance violations at the earliest stage they can possibly in its development, reducing the risk of deployment and enhancing enterprise semantic systems. In line with the DevSecOps of Shift Left Security, the structure incessantly validates ontology artifacts as it assists cloud-native, hybrid-cloud, as well as enterprise on-premise infrastructures. Ten layers make up the SSDF, all linked and sharing ontology metadata, validation reports, security policies, compliance information and deployment artifacts, one of the strengths that ensure long-lasting governance across semantic knowledge lifecycle.

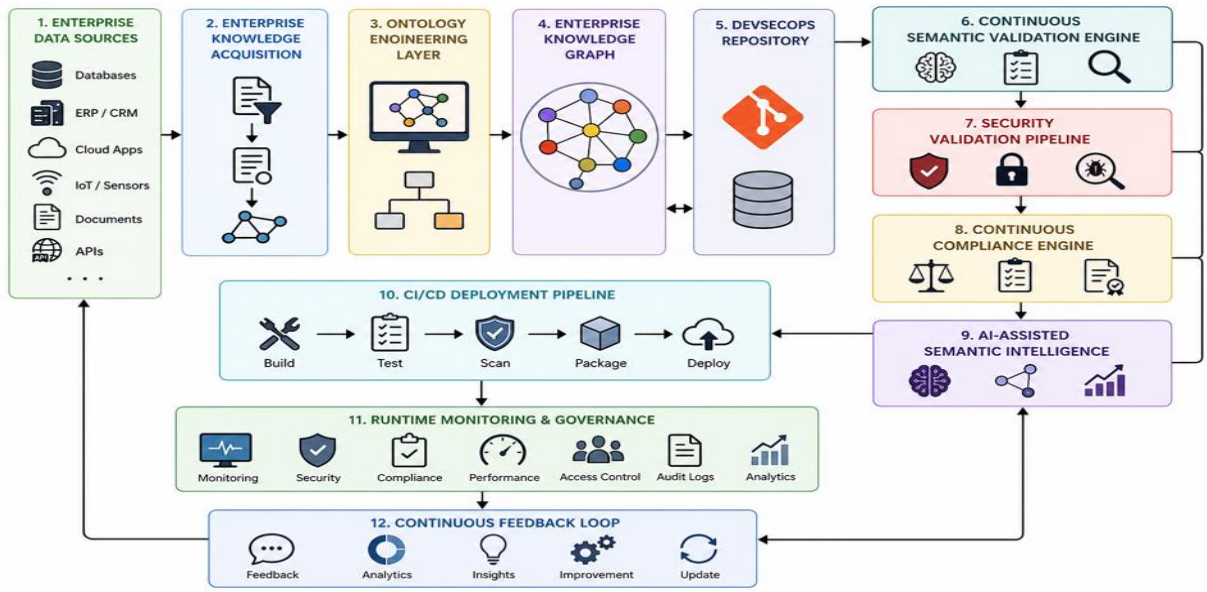

Figure 1- Overall Secure Semantic DevSecOps Framework (SSDF) Architecture

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

3.2 Layer 1: Enterprise Knowledge Acquisition

The first level is the enterprise knowledge which is learnt amidst diverse information infrastructure in the organization. Modern organizations generate vast quantities of structured, semi-structured, and unstructured data stored in business applications, in the cloud or on enterprise databases, in ERP systems, CRM platforms, IoT devices, healthcare systems, financial applications, API resources, XML and JSON repositories, documentation, PDF, data warehouses and third-party sources of threat intelligence. The received data is then sent to preprocessing before the ontology building to metadata extracting, schema mapping, entity recognition, relationship discovery, data normalization and vocabularies. Its processes transform heterogeneous information about an enterprise into standardized semantic representation which can be utilized to come up with ontologies. The main purpose behind this layer is to have a rich knowledge repository where the enterprise concepts, business processes, organizational relationships as well as the domain-specific semantics are well represented. Enterprise metadata repositories, business vocabularies, domain concepts identified and normalized semantic datasets have been produced as the outputs, and are used to create the core of additional ontology engineering endeavors.

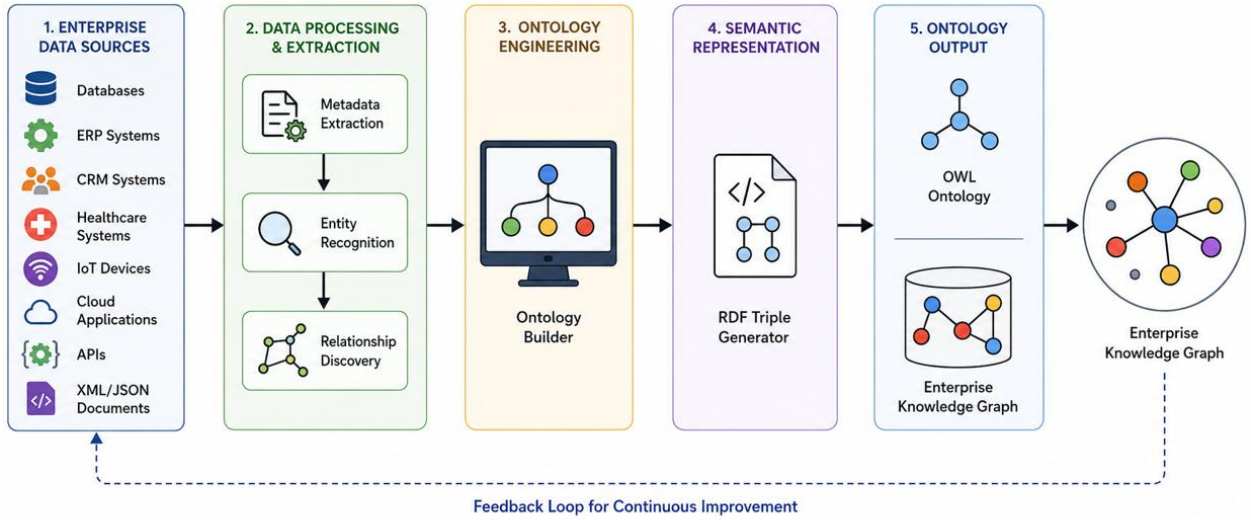

Figure 2- Enterprise Knowledge Acquisition and Ontology Engineering Pipeline

3.3 Layer 2: Ontology Engineering and Semantic Modeling

The second layer moves enterprise knowledge into formal semantic models which can be used to support intelligent reasoning and interoperability. Ontology engineers liaise with the domain experts to create domain ontologies in the OWL, RDF standards in addition to creating the taxonomies, object property, data property, semantic relation, and semantic inference rules. The matched existing ontologies are evaluated to remove semantic redundancy and include interoperability of heterogeneous, enterprise systems by means of ontology matching method. It can also convert organizational entities and relationships into RDF triplets which could be well queried with SPARQL to create knowledge graphs in this step. Semantic metadata repositories become concurrently in order to control, and document ontology. Ontology development tools (protégé ontology) can help ontology engineers designing the ontology, editing and validating the semantic models. Solutions with version control ensure that any ontological change is recorded, thus ensuring that organizations will be aware of the ontology development whilst ensuring semantic integrity of their subsequent releases. The deliverables of this layer are enterprise ontologies, OWL schemas, RDF knowladge graphs and semantic metadata repositories and standardized vocabularies that are primed to be validated and instantiated.

3.4 Layer 3: DevSecOps Source Control and Version Management

The third tier will realize DevSecOps concepts to ontology engineering by having centralized versioning and control. All artifacts of ontology, RDF schema, SHACL constraint, SPARQL query, and semantic configuration file save in controlled version managed repository like Git. Often, the conflicts can be reduced by creating semantic assets in concert by a branch management plan that provides the capability of many ontology engineers. Any change in ontology is automatically recorded with the identity of the people who made the change including time stamp, description of the change, approval and business justification. The ontology integrity is also increased further by the use of the digital signatures and artifact repositories which prevent illegitimate changes and authenticity of artifacts. The ability to

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

manage continual versions of versions of an ontology allows organizations to compare versions of the ontology, determine the differences in the semantics of the ontology and recover the semantic past of the ontology and to obtain the complete ontology lifecycle traceability. Accountability is greatly improved by such governance and, in addition, it promotes the development of enterprise ontology via collaboration.

3.5 Layer 4: Continuous Semantic Validation Engine

The fourth layer is the core of quality assurance of the proposed framework wherein the correctness of ontology is verified on a regular basis whenever a semantic change is done. OWL reasoners automatically check the consistency of ontologies and report logical inconsistencies, inappropriate class hierarchies, concepts that are unsatisfiable and inference errors. Some of the semantic constraints that can be validated in SHACL are cardinality constraints, domain/range constraints, compulsory property, datatype constraint and integrity of relationships. Meanwhile, the validation checks with the help of SPARQL detect duplicate entities, orphan classes, bad object properties, and missing semantic relationships, cyclic relationships, and redundant assertions in the knowledge graphs of the enterprise. Semantic rules in SWRL are automatically intended to analyse the business rules and domain constraints of the organisation. The verification output summary is in the form of semantic quality reports containing of ontology quality scores, error classification and validation report and corrective suggestions. The continuous semantic validation assures that indications of ontology errors are reported as soon as a code is committed and greatly helps in alleviating the issue of semantic errors at deployment.

3.6 Layer 5: Security Validation Pipeline

The fifth layer entrenches cybersecurity in the ontology development life cycle and the security testing is automated in DevSecOps pipeline. An ontology vulnerability scanner is an in-service vulnerability test to ontology poisoning attacks, malicious assertion, semantic injection attacks, rogue modifications of ontologies and integrity attacks. Against ontology repositories and knowledge graph services, access-control verification is done by verifying role-based access control (RBAC), attribute-based access control (ABAC), authentication, authorization policies and identity management rules. RDF services, SPARQL query services, API, measures of encryption to guarantee a secure sharing of semantic information and communication channels are also evaluated in respect to security.

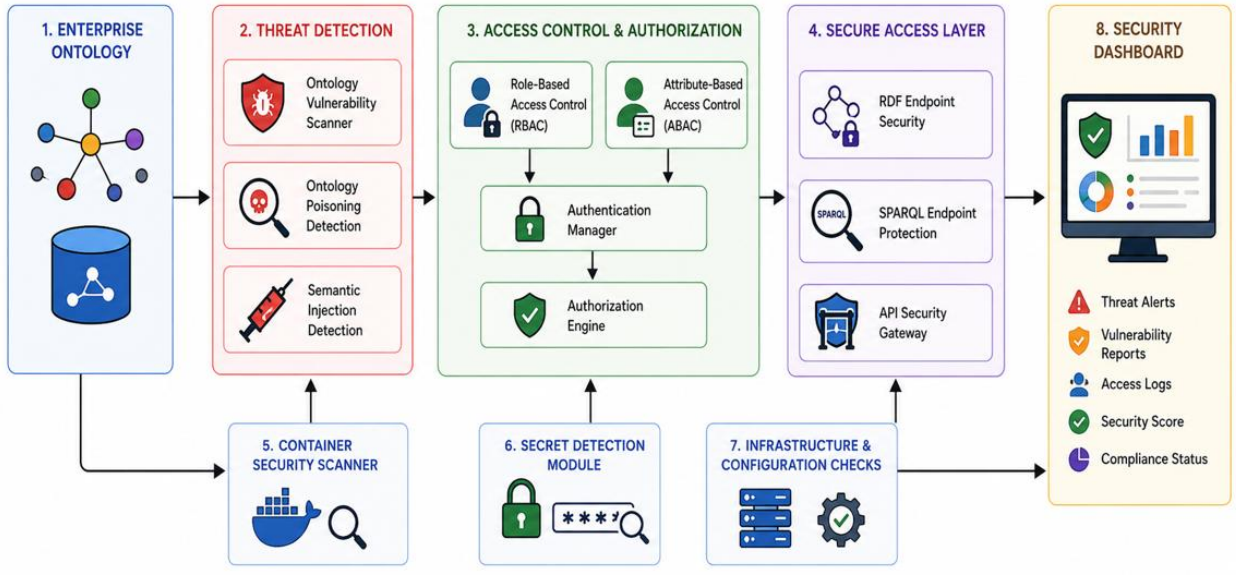

Figure 3- Security Validation Pipeline for Enterprise Ontology Platforms

The software vulnerabilities and configuration flaws are detected by container security scanners checking the Docker images, Deployments in Kubernetes and cloud-based ontology services. The authentication credentials, certificates and cryptography tokens are automatically detected, the secret detection mechanisms will detect the exposed API keys, the certificates, and cryptography tokens before deployment. Extensive security reports include vulnerability ratings, security risk assessment, and suggested solutions to adaptability, making sure that the enterprise ontology platforms are sturdy against changing cyber injustices.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

3.7 Layer 6: Continuous Compliance Monitoring

The sixth layer will validate that the enterprise ontology platforms are crafted to fit the organizational governance policies as well as international regulatory standards. The majority of enterprise ontologies usually contain valuable, sensitive healthcare, financial, governmental, and customer data, therefore, compliance validation should be conducted regularly when developing ontologies. Automatic analysis of ontology artifacts will be based on the following standards: GDPR, HIPAA, ISO/IEC 27001, NIST Cybersecurity Framework, SOC 2 and PCI-DSS. Policy validation is a computerized checking of sensitive data classification, privacy restrictions, consent, retention policies, access permissions, creating audit entries, and governing policy. Potential greater compliance breaches also produce in real-time warnings before the ontology is deployed to make sure that compliance breach regulations do not enter the production facilities. Compliance dashboards include detailed regulatory scores, audit reports, risk assessment and policy compliance scores, which allow administrators of enterprises to conveniently govern compliance governance performance and make it easier to carry out regulatory auditing.

3.8 Layer 7: AI-Assisted Semantic Intelligence

One significant AI use to enhance ontology engineering is to automate governance and semantic analysis. Ontology evolution, semantic structures and enterprise knowledge graph behavior are continually analyzed by machine learning algorithms to detect duplicate concepts, semantic anomalies, inconsistencies in relationships, ontology drift and hidden knowledge patterns. The predictive models propose to ignore relationships, extension of ontology, concept matching and refinements based on the history of ontology evolution. Large Language Models (LLM) are also deployed to support ontology developers with the automatic generation of OWL classes, RDF triples, SHACL constraints, SPARQL queries, semantic documentation and validation explanations. The prescriptions in AI will reduce the manual ontology engineering expenses and improve the semantic correctness, growth efficiency and overall quality of the knowledge. Smart anomaly detection could also be useful in improving governance since suspicious changes in ontology are highlighted before it is deployed.

3.9 Layer 8: Automated CI/CD Deployment Pipeline

Ontology artifacts are automatically sent to the Continuous Integration and Continuous Deployment (CI/CD) pipeline on successfully validation. It is developed as ontology, semantically tested, security tested, compliance tested, packaged into artifacts, containerised and then infrastructure provisioned, orchestrated into Kubernetes on off-the-shelf and deployed to the cloud respectively. It has infrastructure-as-Code technologies that are deployed to work on Azure, AWS, Google Cloud, privately hosted clouds, hybrid clouds, and enterprise Kubernetes.

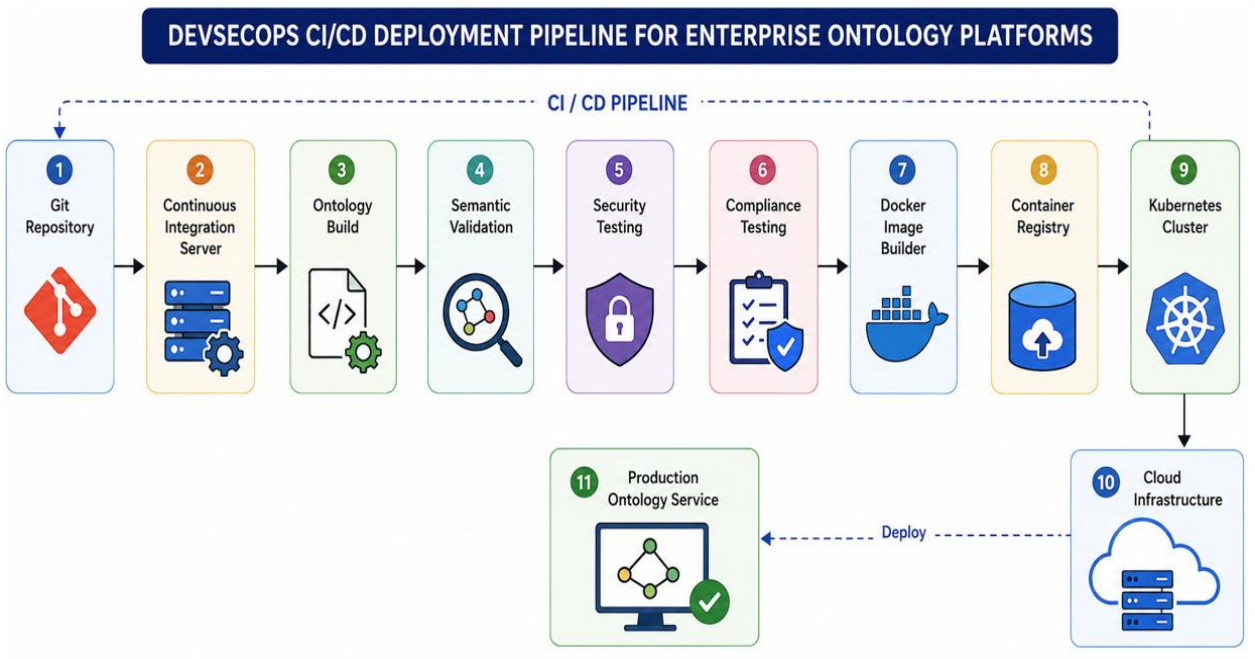

Figure 4- DevSecOps CI/CD Deployment Pipeline for Enterprise Ontology Platforms

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

Each of the deployment phases has automated approval gates to guarantee that semantically sound ontology artifacts that meet the requirement of security- and regulation-related issues are only deployed to production. This will be a deployment pipeline which will run automatically and will reduce the ontology release schedules as well as save numerous man hours in human intervention and deployment bugs.

3.10 Layer 9: Runtime Monitoring and Governance

Monitoring of enterprise ontology platforms is performed continuously after the deployment in order to stabilize operations, semantic integrity and cybersecurity. Services permit health, consistency of ontologies, APIs managed performance, SPARQL endpoint availability, user activities, log of access, query performance, semantic accuracy and usage of infrastructure as well. Intrusion preventing mechanisms thwart suspicious user interactions, realistic edits, suspicious query patterns, and new cyber threats to ontology services. The quality of ontology, semantic consistency and version history, security posture, and compliance state are in real-time displayed to the administrators via governess dashboards. These automated remediation processes can be enabled whenever we notice infra-infra failures or security breached so that we can rollback processes, security alerts or remediation procedures to ensure that we can depend on our systems.

3.11 Layer 10: Continuous Feedback and Improvement

The final layer has a mechanism of constant improvement which allows development of adaptive ontology based on the foundation of operational feedback. Validation failure, runtime failures, compliance, artificial intelligence, responses, use ontology statistics, performance measures, and user surveys are constantly monitored and evaluated. These insights are automatically reported to ontology engineers and can be useful in semantic refinement, ontology optimization, policy change and policy governance. By allowing an operational experience to be linked with the latter ontology building activities via its feedback process, the approach makes possible a continuous educational process. The structure is a constant and continuous bettering procedure since enterprise knowledge proceeds, developing the excellence of ontology, semantic anomalies, enhancing cybersecurity, quickening implementations, meeting regulatory compliance and encouraging economical knowledge controls.

IV. FRAMEWORK EVALUATION

4.1 Evaluation Objectives

Secure Semantic engineering (SSDF), the proposed framework that was to be discussed by the candidate, was conceptualized in terms of its helping the continuity ontology engineering, semantic validation, cybersecurity, governance, and adapting to regulations in the enterprise ontology engines. The assessment attempts to contrast the frameworks on their ability to deliver semantic consistency, enhance the quality of ontology, enhanced security and automatic compliance in ontology development lifecycle. Also, it examines the framework in terms of its ability to integrate DevSecOps practices and semantic technologies as well as allowing an implementation at scale on a cloud-native and hybrid enterprise cloud. The main point is to demonstrate that adding validation, security and governance to all objects of ontology development can result in the greater reliability and trustworthiness of the enterprise knowledge systems on semantics.

4.2 Evaluation Criteria

The framework is also quantified in terms of a wall of qualitative performance criterion which portray the imperative divide of enterprise ontology platforms. These standards are semantic consistency, ontology quality, security assurance, compliance management, scalability, automation, governance, interoperability, deployment readiness and maintainability. Semantic consistency is an appraisal of the capability of the framework to perform logical inconsistency, rediscover entities, invalid relationships and ontology conflicts by making inferences within OWL, SHACL constraints, SPARQL queries and semantic rule validation. Security checks against assurance are used to verify the functionality of ontology vulnerability assessment, access-checking, API protection, identity management and infrastructure security. Non-compliance test identifies the effectiveness of the frame to apply the organizational policies and control principles like GDPR, HIPAA, ISO/IEC 27001, NIST, and SOC 2. The deployment automation, which is used to gain further analysis, runtime monitoring and continual feedback, can be used to attain long term ontology governance.

4.3 Framework Performance Analysis

Its proposed SSDF has a high potential across the lifecycle of ontology via association semantic engineering to DevSecOps in the message of the entire ontology engineering. Ongoing semantic validation enjoys a great benefit over ontology quality, in that the ontology automatically detects inconsistencies as the ontology modifications are made. All

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

automation such as OWL reasoning, SHACL validation and validation by SPARQL minimizes manual validation because knowledge graphs within the enterprise are stored in a coherent and well structured manner. The integrated security validation pipeline enhances the ontology security by preventing ontology semantic attacks, unauthorized ontology updates, unsecured APIs, configuration attacks and unsecured credentials during deployment. At the same time, longer compliance checks will mitigate risks of regulation since it will be able to check ontology artifacts against the policy of governance of organization and international standards members during its creation and not post-deployment. AI-based semantic intelligence can also aid the framework in increased functionality by automatically detecting ontology drift, duplication, semantic anomalies and inconsistency in the relationships and provide smart recommendations on how ontologies can be corrected. The AI-based CI/CD delivery pipeline remains capable of delivering ontologies in a very short time, without undermining the security, validation or compliance aspects rendering the framework the best platform in large-scale operations of semantics in the enterprise.

4.4 Comparative Assessment

The proposed SSDF has some valuable advantages over traditional ontology engineering methods. Ontological development process is carried out traditionally in a sequence with semantic validation to completion, security testing and compliance testing whose sequence becomes post-development and results in violation of detection of defects and high maintenance costs. SSDF, on the other hand, can transform these activities into a never-ending DevSecOps churn to enable the detection of semantic errors and security vulnerabilities at an early stage. Current engineering models of ontology include conceptual and knowledge representation engineering but the model suggested has automated governance, running monitoring, AI-engaging validation and ongoing carrying out compliance checking. To add to this, the framework can support more recent cloud-native deployment models based on the Infrastructure-as-Code and containerized deployment frameworks which have a higher degree of scalability, operational resiliency and deployment efficiency than a classic semantic development model.

4.5 Summary of Evaluation

The conceptual analysis reveals the proposed Secure Semantic DevSecOps Framework effectively overcomes some of the shortcomings of available enterprise ontology platforms, by uniting ontology engineering, semantic validation, cybersecurity, governance, compliance management, artificial intelligence, and automated deployment. The framework improves semantic integrity, minimized aspects to their weaknesses in security, and improved regulatory compliance and perpetual development of ontology via automated validation and governance systems. It has an extreme degree of modularity and allows it to be used in a wide range of enterprise architectures and allows the possibility of manipulating enormous knowledge graphs and making informed choices. Overall, the discussion revealed that SSDF provides a critical and feasible foundation on how to develop secure, reliable and perpetually governed semantic knowledge platforms that could be leveraged to assist in digital transformation initiatives within the next generation entertainment sector through supporting enterprise-wide digital transformation programmes.

V. CONCLUSION AND FUTURE WORK

The article presented Secure Semantic DevSecOps Framework (SSDF) of Enterprise Ontology Platforms, a full architecture that directs ontology engineering, continuous semantic integrity, and cybersecurity, governance, regulatory compliance, AI, and auto CI/CD deployment to integrate into a solitary DevSecOps lifecycle process. In contrast with the out-of-date manner of doing the engineering of ontology, where the validation process is performed and then, only security verification process is performed at the end of ontology engineering processes, the framework suggested that the semantic quality assurance, security check and compliance control is carried out at every stage of ontology lifecycle. Acquisition of enterprise knowledge, ontology modeling, version and control, persistent semantic validation of OWL reasoning, SHACL, SPARQL and SwRL, applications of the automated security testing, the AI-driven semantic intelligence, compliance testing, runtime monitoring and continuous feedback are contained in the architecture. The framework will promote the reliability of the ontology, semantic consistency, efficient deployment and governance and cybersecurity not only in business but will minimize the use of manual validation services and business risks as well. The suggested architecture offers an expandable and dependable platform of enterprise knowledge graphs used in cloud-native, hybrid-cloud, and on-premise settings, thus, facilitating wise decision-making and digital transformation endeavors.

The second stage of the research will be associated with application of the suggested framework to the real workplaces of businesses to measure its effectiveness numerically based on big scale ontology repositories and industrial knowledge graphs. Experimentally explored such measures as semantic consistency, quality of ontology, deployment efficiency, reduction of security vulnerabilities, accuracy of compliance and scalability of the system. Graph Neural

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 2, March-April 2024||

DOI:10.15662/IJRPETM.2024.0702007

networks (GNNs), Large Language Models (LLMs) and retrieval-augmented generation (RAG) and autonomous AI agents will also be used to complement this framework to enable intelligent ontology evolution, autonomous ontology repair, semantic anomaly prediction and dynamic governance. There are still more applications of blockchain provenance management, confidential computing, and zero-trust security architectures, federated semantic knowledge graphs, and explainable AI approaches that can make improvements to transparency, trust and resiliency. The complements will also enhance semantic knowledge networks of enterprises and can afford safe, intelligent and self-guiding ontology platforms, which could supply AI powered digital ecosystems of the following generation.

REFERENCES

[1] M. Iannacone, S. Bohn, G. Nakamura, et al., "Developing an ontology for cyber security knowledge graphs," in Proc. 10th Annual Cyber and Information Security Research Conference (CISR), New York, NY, USA: ACM, 2015, pp. 1–4, doi: 10.1145/2746266.2746278.
[2] Z. Syed, A. Padia, T. Finin, A. Joshi, and C. Mathews, "UCO: A Unified Cybersecurity Ontology," in Proc. AAAI Workshop on Artificial Intelligence for Cyber Security, Phoenix, AZ, USA, 2016.
[3] Y. Jia, Y. Qi, H. Shang, R. Jiang, and A. Li, "A practical approach to constructing a knowledge graph for cybersecurity," Engineering, vol. 4, no. 1, pp. 53–60, Feb. 2018, doi: 10.1016/j.eng.2018.01.004.
[4] E. Kiesling, A. Ekelhart, K. Kurniawan, M. Huber, and E. Weippl, "The SEPSES knowledge graph: An integrated resource for cybersecurity," in The Semantic Web – ISWC 2019, Lecture Notes in Computer Science, Cham, Switzerland: Springer, 2019, pp. 198–214, doi: 10.1007/978-3-030-30796-7_13.
[5] L. F. Sikos, "OWL ontologies in cybersecurity: Conceptual modeling of cyber-knowledge," in AI in Cybersecurity. Cham, Switzerland: Springer, 2019, pp. 1–17, doi: 10.1007/978-3-319-98842-9_1.
[6] L. F. Sikos and D. Philp, "Provenance-aware knowledge representation: A survey of data models and contextualized knowledge graphs," Data Science and Engineering, vol. 5, no. 4, pp. 293–316, Dec. 2020, doi: 10.1007/s41019-020-00118-0.
[7] Z. Liu, Z. Sun, J. Chen, et al., "STIX-based network security knowledge graph ontology modeling method," in Proc. 3rd International Conference on Geoinformatics and Data Analysis (ICGDA), New York, NY, USA: ACM, 2020, pp. 152–157, doi: 10.1145/3397056.3397083.
[8] A. Piplai, S. Mittal, A. Joshi, et al., "Creating cybersecurity knowledge graphs from malware after action reports," IEEE Access, vol. 8, pp. 211691–211703, 2020, doi: 10.1109/ACCESS.2020.3039234.
[9] I. Sarhan and M. Spruit, "Open-CyKG: An open cyber threat intelligence knowledge graph," Knowledge-Based Systems, vol. 233, Art. no. 107524, 2021, doi: 10.1016/j.knosys.2021.107524.
[10] A. Mohamed, G. Abuoda, A. Ghanem, et al., "RDFFrames: Knowledge graph access for machine learning tools," The VLDB Journal, vol. 30, no. 6, pp. 1009–1035, 2021, doi: 10.1007/s00778-021-00690-5.
[11] Z. Wang, H. Zhu, P. Liu, et al., "Social engineering in cybersecurity: A domain ontology and knowledge graph application examples," Cybersecurity, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00094-6.
[12] K. Kurniawan, A. Ekelhart, E. Kiesling, et al., "KRYSTAL: Knowledge graph-based framework for tactical attack discovery in audit data," Computers & Security, vol. 115, Art. no. 102828, 2022, doi: 10.1016/j.cose.2022.102828.