A Domain Reputation System Architecture Description Using TOGAF

Mihail DUMITRACHE[1,3,4]*, Carmen Ionela ROTUNĂ[1,2], Alexandru GHEORGHIȚĂ[1,2], Adrian Victor VEVERA[1], Ionut SANDU[1], Dragoș SMADA[1]

[1] National Institute for Research and Development in Informatics, 8-10 Mareșal Averescu Avenue, Bucharest, 011455, Romania
mihail.dumitrache@ici.ro (**Corresponding author*), carmen.rotuna@ici.ro, alexandru.gheorghita@ici.ro, victor.vevera@ici.ro, ionut.sandu@ici.ro, dragos.smada@ici.ro

[2] Politehnica University of Bucharest, 313 Splaiul Independenţei, Bucharest, 060042, Romania

[3] University of Bucharest, Faculty of Letters, 5-7 Edgar Quinet Street, Bucharest, 010017, Romania

[4] Academy of Romanian Scientists, 3 Ilfov Street, Bucharest, 050044, Romania

Abstract: The number of domain names is continuously increasing and the extent of security incidents is increasing accordingly. Thus, automated solutions are becoming necessary for monitoring the domain names and alerting their stakeholders. Determining the reputation level of a domain name increases domain security for individuals, public institutions and private companies because it enables users to gain a clear understanding of the trustworthiness associated with a certain domain name. This, in turn, creates a safer online environment. This paper aims to present the architecture of an automated monitoring platform, which is meant to dynamically establish the reputation for each .ro domain and other domains as well. The primary objective of this paper is to enhance people`s trust in the use of .ro domains by reducing the exposure to malicious activities on the Internet through automated monitoring and consequence mitigation.

Keywords: Domain, DNS, Generic architecture, Domain reputation system, TLD.

1. Introduction

Online transactions and interactions have become an essential part of people`s daily lives in today's digitally connected society. With the growing number of online users, the requirement for reliable and secure systems is more vital than ever. The Domain Name Reputation System is a system that allows the assessment of the domains` reputation in order to prevent criminal behaviours and improve online security. It protects Internet domains from malicious activity in the Internet space by automatically monitoring them and providing methods to deal with any risks (Rotună et al., 2023).

The highly dynamic nature of the domain name ecosystem, as well as the proliferation of malicious domains which pose a real and immediate threat to people's and companies' privacy and security, are the primary motivators for developing an automated solution to establish a domain's reputation level and continuously monitor its changes throughout its lifetime.

By evaluating the reputation level of owned domains, existing and future owners (authorities, governmental institutions, private enterprises, individuals, and so on) will obtain a more precise picture of their credibility, resulting in a safer Internet space.

In comparison with other existing domain reputation systems such as Notos, Kopis, and Exposure, the proposed Domain Name Reputation System encourages the creation of an ecosystem that permits real-time, dynamic domain reputation scoring. This capability enables the study of domains that have been transferred or re-registered by various individuals who may not have the same intents as the prior owner, whether good or harmful.

The benefits of the proposed system architecture include continuous monitoring of domain name operations to detect any malicious activity, machine learning algorithms to analyse the data and learn from the chosen data set using a variety of information. The internal sources include domain-related data from the Registry of .ro domains and the external domain reputation services provided by other organisations. The solution will offer customizable reports that can be profiled to meet the specific needs of users.

General parameters that determine a good reputation score for a domain name considered for the analysed system are domain age, owner history, domain name relevance, host history, trade history, nameserver history, domain status, Registry analysts' reports, and policy violation. To these parameters are added the results provided by

https://doi.org/10.24846/v33i1y202406

external Domain Reputation Services (blacklists, whitelists), absence of phishing activities, existence of a valid SSL Certificate, correctly configured DNS records, reputation of the Registrar, how often a domain is accessed, SSL historical data, number of redirects, etc.

The automated domain reputation monitoring system is intended to provide a full study of a domain's reputation by gathering data from many sources and processing it by using internal and external tools to generate a score. In parallel, machine learning algorithms will evaluate the same domain and attempt to extract patterns of harmful domains, which will then be utilized to increase the accuracy of the Domain Name Reputation System's results. (TLDRep).

The main objectives of this paper are to identify an Enterprise Architecture Framework appropriate for the development of a domain reputation system and to develop that architecture using the selected framework.

The remainder of this paper is as follows. Section 2 presents the state of the art with regard to the importance of developing an architecture for the sustainable development of a domain name system. In Section 3 the widely used architecture frameworks are presented while Section 4 proposes a methodology for the selection of an appropriate framework for the Domain Name Reputation System. In Section 5 the architecture of the proposed system is illustrated using TOGAF Enterprise Architecture (EA) (The Open Group, 2023a). Finally, Section 6 outlines the conclusions of this paper.

2. State of the Art

The substantial increase in the number of daily registered domains and the proliferation of compromised domains, which can be exploited as attack vectors against Domain Name System (DNS) servers, requires the development of a system for assessing domain reputation.

Domain security refers to policies, procedures, tools, and security solutions put in place to protect a domain from unauthorized access, data breaches, and website unavailability (ICANN, 2023). Some of the most critical domain security risks are:

- Phishing, used by hackers to steal confidential information such as passwords, credit card information, and information related to bank accounts using an email or social media message with a link, asking the recipient to update details, such as their password, via the provided link. (Dumitrache et al., 2023).

- Domain Name System (DNS) spoofing attack where a hacker redirects traffic from a legitimate website to a fake one;

- Domain hijacking which involves unauthorized access to domain registrar account and changing the registration information;

- Typosquatting, involving registering a domain name that is similar to a legitimate one, with the intention of misleading users (Bolster, 2023).

The cornerstone of an effective threat mitigation approach is conducting threat assessments, developing mitigation strategies, and establishing appropriate risk levels (Cîrnu et al., 2018).

Domain Name Reputation System has the objective to determine the reputation level of domain names using information from internal sources, .ro Domain Registry and from external sources, blacklists, email lists and other trusted providers. By establishing the reputation level of .ro domains, it provides individual users, government institutions and private enterprises with an accurate understanding of the trustworthiness associated with a certain domain name. Consequently, this contributes to creating a more secure online environment. In addition to the traditional methods employed by DNS administrators, such as maintaining blacklists of infected domains, the automatic detection architecture described in this paper offers the advantages of swift identification and automatic updates regarding potentially compromised domains.

Due to the complex nature of the proposed system, there is a need to design an architecture model that enables interoperability, sustainability and scalability. Thus, an evaluation was carried out to identify a methodology for using this system (IANA, 2020).

The importance of Software Architecture has been discussed by many researchers and practitioners since 1968, when Djikstra Edsger (Dijkstra, 1968) first mentioned the importance of this field for software development. The first attempts at defining software architecture

relied on organizing the structure of large-scale software systems at the time. The approach was centred on documenting the structure of software systems by using then-well-known concepts such as separation of concerns, modularity and hierarchical decomposition. Then, in the 1990s, other concepts and ideas on software architecture were introduced by Royce & Royce (1991) and Shaw & Garlan (1996).

Architectural documentation cannot be neglected, given the well-known importance of software architecture for the success of a software project (Kouroshfar et al., 2015; Whiting & Andrews, 2020). A well-defined architecture supports new developments from existing processes and systems, as well as different analyses and the implementation of changes.

Examples of concerns related to software architecture include separation of interests, coupling, cohesion, encapsulation, modularity, change implementation (learnability, instability, testability, and manageability), interoperability, compliance, and reusability, among others. The software architecture is documented through the different scenarios related to the system and, consequently, by evaluating its impact throughout the organization (Rocha, Misra & Soares, 2023; Banciu & Dumitrache, 2016).

3. Widely Used Architecture Frameworks

The most commonly used enterprise architecture frameworks include Zachman Framework, Federal Enterprise Architecture Framework (FEAF), Unified Architecture Framework (UAF), and The Open Group Architecture Framework (TOGAF). These frameworks provide a structured approach to designing and managing enterprise architectures.

The Zachman Framework is an enterprise architecture ontology that provides a way of viewing an enterprise and its information systems from different perspectives and how the components of the enterprise interact. A Zachman architecture description is a two-dimensional classification scheme for descriptive representations of an Enterprise that is structured as a matrix containing 36 cells, each of them focusing on one dimension or perspective of the enterprise (Zachman, 1996).

The Zachman Framework does not recommend any specific modelling language. Instead, it provides a structure for organizing architectural artifacts such as design documents, specifications, and models. The framework is used as a fundamental structure for Enterprise Architecture (Harkai et al., 2018) and can be used with various modelling languages such as UML (Object Management Group, 2023b), ArchiMate (The Open Group, 2023b), and BPMN (Object Management Group, 2023a; Visual Paradigm, 2019; Zachman, 2010).

TOGAF offers a structured and comprehensive approach for developing enterprise architecture, making it ideal for complex ecosystems such as domain name reputation scoring. It emphasizes the alignment of architecture with an organization's strategic objectives, ensuring that the application or ecosystem supports overarching business goals, with TOGAF's business architecture phase facilitating this alignment. TOGAF accommodates the integration of diverse data sources, such as DNS records and web traffic, ensuring secure and well-defined data flows. It also promotes interoperability, making it easier to integrate the ecosystem with external systems and adhere to industry standards, which is crucial in the domain reputation context (Kotusev, 2018).

The Unified Architecture Framework (UAF) is an architecture framework based on the Unified Modeling Language (UML) (Object Management Group, 2023b), Systems Modeling Language (SysML) used to model and design complex systems and enterprises. It is a comprehensive framework designed to support the development and management of various types of architectures, including enterprise architecture, systems architecture, and solution architecture. UAF aims to provide a unified and integrated approach for architecting and aligning different aspects of an organization or system (Object Management Group, 2023c).

The UAF specification comprises three primary components:

- Domain Metamodel (DMM) which serves as the foundational framework for modeling an enterprise, encompassing key entities within that enterprise. It establishes the core modeling constructs to be employed, making up the basis for architecture development.

- View Specifications guide tool vendors and architects tasked with creating architecture

views, providing clear directions on which DMM elements are relevant to each specific view. This ensures consistency and clarity in the development of architectural perspectives.

UAF Profile (UAFP) is an embodiment of the DMM, offering a practical means of modelling UAF views using SysML notation. It defines how UAF views can be represented, aiding to the effective implementation of the framework in practice (Object Management Group, 2023c).

The Federal Enterprise Architecture Framework (FEAF) is an architecture framework used by U.S. federal government agencies to guide the development and management of their enterprise architectures. It provides a structured approach to aligning an agency's business processes, data, applications, and technology with its strategic goals and mission.

FEAF aims to help federal agencies align their operations with government-wide priorities and mandates. It supports efficient and effective service delivery, promotes data sharing, enhances security, and facilitates the management of technology investments. FEAF serves as a valuable tool for federal agencies to improve their operations and better serve the public by ensuring that their enterprise architectures are strategically aligned and well-managed (U.S. Government, 2023).

4. Enterprise Architecture Selection Methodology

4.1 Research Methodology

Comparing the Federal Enterprise Architecture Framework (FEAF), The Open Group Architecture Framework (TOGAF), Unified Architecture Framework (UAF), and Zachman Enterprise Framework, along with their modelling language considerations, provides insights into their similarities, differences and capabilities.

Table 1 provides an overview of these frameworks in terms of scope, particularities and considerations related to performance, data, SOA (Service Oriented Architecture), modelling languages, security, and alignment with standards. It also highlights their respective approaches to modelling languages. Generally, the choice of a framework depends on specific organizational

Table 1. EA Frameworks Comparison

Characteristics	FEAF	TOGAF	UAF	Zachman
Scope and Applicability	U.S. federal government agencies	Diverse industries and organizations globally	Complex systems and enterprises	Various industries and organizations
Particularities	Five reference models: Performance Reference, Business Reference, Service Component, Technical, Data	Three domains: Business Architecture, Data and Application Architecture, Technology Architecture	Four views: business, information, technology, and operational	Taxonomy for architectural descriptions
Alignment with Standards	Not a standard	Not a standard	Used as a standard	Not a standard
Emphasis on Business Architecture	Strong focus on business architecture	Addresses business architecture; comprehensive	Promotes integration across domains	Provides a classification system
Performance and Metrics	Performance Reference Model (PRM) for measurement	Consideration of business performance	Emphasizes traceability and lifecycle	Does not explicitly incorporate metrics
Modelling Language	Often uses UML, BPMN, and other standard notations	Provides guidance on architecture modelling	Associated with modelling tools, SysML, UML	Does not prescribe a specific language
Data Management	Data Reference Model (DRM) for data standards	Extensive guidance on data and information	Offers an integrated approach for data	Does not provide specific data guidance
Service-Oriented Architecture (SOA)	Service Component Reference Model (SRM)	Addresses SOA, broader architectural context	Supports various architectural viewpoints	Not technology-focused
Security and Privacy	Security and Privacy Profile (SPP) for requirements	Covers security, but more generalized	Supports clear and comprehensive docs	Does not specifically address security

needs and context. In relation to the scope of this research, all these 4 frameworks are compared with the purpose of selecting the most appropriate for the description of Domain Name Reputation System Architecture.

After comparing the capabilities and benefits of the four frameworks above, TOGAF was chosen for the development of TLDrep architecture because it offers a comprehensive approach to enterprise architecture development that is widely used in the industry, it is used as a standard and it is easy to use and implement (Priyadharshini, 2013).

TOGAF offers a structured and comprehensive approach for developing enterprise architecture, making it ideal for complex ecosystems for domain name reputation scoring. It emphasizes aligning architecture with an organization's strategic objectives, ensuring that the application or ecosystem supports overarching business goals, with TOGAF's business architecture phase facilitating this alignment.

Using TOGAF for a Domain Reputation System ensures that the system is well-aligned with business objectives, follows best practices, and is developed systematically and cost-effectively. It also supports adaptability and long-term success by facilitating change management and quality assurance.

TOGAF accommodates the integration of diverse data sources, such as domain Registry data, DNS records and web data services, ensuring secure and well-defined data flows. It also promotes interoperability, the integration of the ecosystem with external systems and adherence to industry standards easier, which is crucial in the domain reputation context.

5. Domain Reputation System Architecture Description using TOGAF

5.1 Stakeholders Architecture View

The TOGAF standard provides a formal modelling approach to understand stakeholders, concerns, and views. Architecture views are the key artifacts in an architecture description as they are representations of the overall architecture that are meaningful to one or more stakeholders in the system. Different stakeholders with different roles in the system will have different concerns (The Open Group, 2023a). The Stakeholder Viewpoint is a part of the Business Architecture viewpoints defined in the TOGAF framework. It is used to identify and document the stakeholders who have an interest in the system, their concerns, and their viewpoints.

A domain reputation scoring tool for a domain name Registry is a critical component for managing the domain space and ensuring the overall health, security, and integrity of the registry. Various stakeholders are involved in or influenced by such a tool in different ways as follows.

Domain Name Registry Operator responsible for managing the .ro domain will use the scoring tool to monitor and analyse domain names and alert domain registrants.

Domain Registrars are companies or entities that sell domain names to domain owners. The Reputation System enables them to ensure the reputation of the domains they manage, as this can affect their business and customer trust.

Domain Resellers are companies that buy domain names from Registrars and sell them to domain owners. They are impacted by the implementation of the system in a similar manner as Registrars.

Domain Registrants are individuals or organizations that own .ro domain names, who are directly impacted by domain reputation because it can affect their business, online presence and email deliverability.

Legal Authorities may use the reputation management tool to identify malicious or fraudulent domains within the .ro space. This is crucial for combating cybercrime and intellectual property violations.

Internet Service Providers (ISPs) use domain reputation tools to filter or block emails and traffic from domains with poor reputations. This helps reduce spam, phishing, and malware distribution (RiskAnalytics, 2023).

Email Service Providers (ESPs) leverage domain reputation scoring to determine the legitimacy of email senders and reduce the risk of their users receiving spam or phishing emails.

Researchers studying online threats, cyberattacks, and domain abuse rely on reputation management tools to analyse trends and threats within the domain space.

Security companies that provide security services, such as threat intelligence, security software, and firewalls, may use domain reputation data to enhance their security offerings (Lockheed Martin, 2019).

Operators of DNS infrastructure and services may rely on reputation data to maintain DNS integrity.

Government agencies and policies and standards organisations such as ICANN (Internet Corporation for Assigned Names and Numbers) are involved in setting policies and standards related to domain reputation and security.

Cybersecurity companies offering cybersecurity solutions often incorporate domain reputation data into their threat detection and prevention mechanisms.

The main requirement fulfilled by the Domain Reputation System is Domain Scoring. The several stakeholders described above are involved or benefit from the system. Figure 1, which was developed in ArchiMate (The Open Group, 2023b), relying on TOGAF EA standard illustrates the stakeholders of the system.

Stakeholders of the Domain Reputation System play different roles, and their interests may sometimes intersect, thus balancing the needs and concerns of these stakeholders is essential for maintaining a secure and reliable domain name Registry.

5.2 Business Architecture View

The TOGAF Business Architecture View for a Domain Reputation System, illustrated in Figure 2, highlights the business components of the system and the relationships between them. In the current use case, the system consists of several business components, including internal and external data sources, data acquisition, pre-processing, processing, storage, domain scoring, and a Data Warehouse where the domain scoring information is retrieved, stored and displayed.

Domain Registry is a key data source within the business architecture. It represents the authoritative source for domain information, transactions, and updates as it maintains a registry of all .ro domains. Internal Data Sources are pieces of information that are provided by the Registry Data Analysts which evaluate manually the parameters of a domain name and user feedback and other information that is manually registered, for example the Policy violation data related to a domain. External Data Sources represent the information items retrieved from sources which are outside the domain Registry as DNS records, security applications, blacklists, the presence of SSL certificates, etc.

The Data Acquisition Function is responsible for collecting data from various sources, both internal and external. This function includes mechanisms for data retrieval, data ingestion and data transformation.

Pre-processing involves cleansing, normalizing, and validating the incoming data to ensure

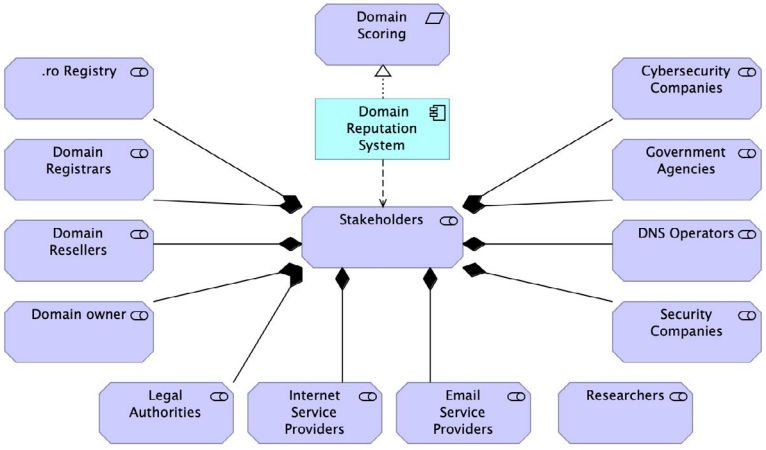

Figure 1. Domain Reputation System Stakeholders

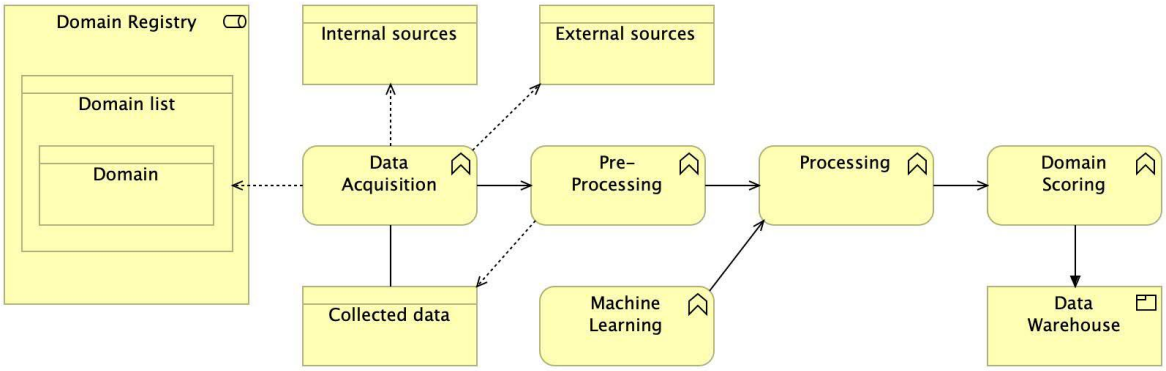

Figure 2. Business Architecture View

its quality and consistency and involves data deduplication, data enrichment, and format standardization.

The Processing component performs the core reputation assessment tasks. It utilizes algorithms, models, and heuristics to analyse data and calculate domain reputation scores. This function involves the evaluation of the chosen data to identify anomalies, threats, frequent owner change and other indicators of domain behaviour.

The Storage function relates to databases and data storage solutions to maintain historical records of domains, their attributes, and reputation scores.

Domain Scoring business function addresses a set of Machine Learning algorithms and rules for determining the reputation scores of individual domains that take into account various factors, such as domain behaviour, history, and the use of the data collected from the internal and external data sources.

The Data Warehouse serves as a repository for the results of domain scoring and other data. It stores historical data, trends, and aggregated results. Business intelligence tools and reporting systems may access the Data Warehouse to provide insights to stakeholders.

The objective of this business architecture view, illustrated in Figure 2, is to provide a high-level understanding of how the Domain Reputation System operates within the larger business context, enabling stakeholders to visualize the flow of data, processes, and relationships that contribute to domain reputation assessment and management.

5.3 Information System and Data Architecture View

The Information System and Data Architecture, illustrated in Figure 3, focuses on the design of the application architecture and demonstrates how the Business Architecture is outlined through Information Systems (Tepandi et al., 2019).

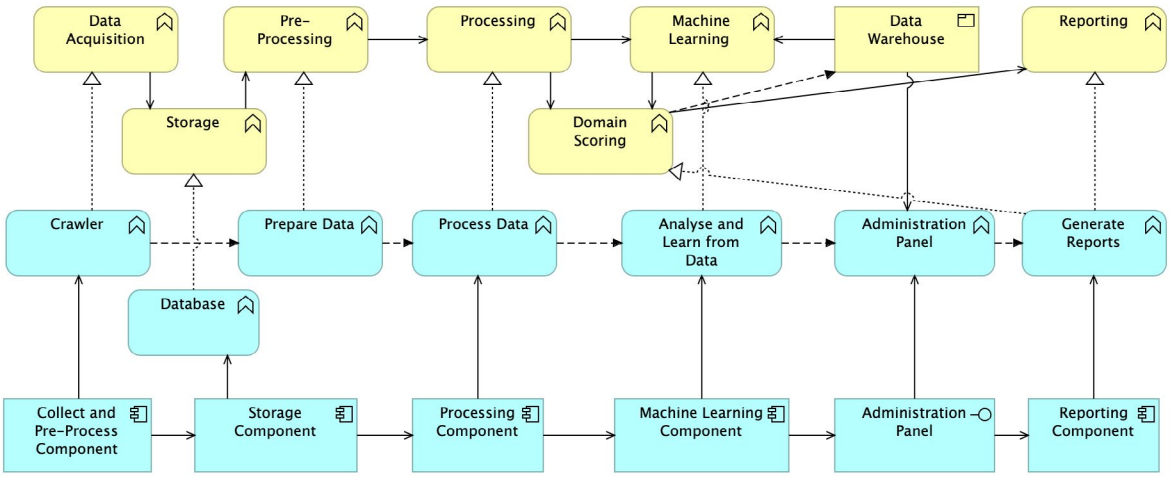

Figure 3. Information System and Data Architecture View

An Architecture Information View of a Domain Name Reputation System provides a high-level overview of the system's components, processes, and their interactions. It enables visualizations of the system functions, components and data flows between various components.

Collect and Pre-Process Component is responsible for acquiring data about domain names from Registry, internal and external sources using a crawler mechanism and collects domain-related information, such as registration details, DNS records, historical data, blacklists information and transactions and, at the next step, pre-processes the collected data for consistency and quality.

The Storage Component stores the data acquired by the Collect and Pre-Process Component and maintains a repository of domain-related information with both historical and real-time data.

The Processing Component is responsible for analysing and processing the collected data and performs various reputation assessment tasks to evaluate domain-related information and determine reputation scores. It uses algorithms and defined rules to assess domain reputations, identify threats, and perform domain data assessment.

The Machine Learning Component emphasises the system's ability to analyse and learn from data and relies on Machine Learning algorithms to improve reputation assessments over time. It continuously analyses data patterns and domain behaviour to adapt and enhance the system's ability to identify new anomalies.

The Reporting Component generates and illustrates information obtained after the processing of data and reputation assessments. It provides visualizations, reports, and notifications to stakeholders. It aggregates and visualizes domain reputation data, generates reports on domain behaviour trends, and sends alerts to relevant stakeholders when necessary.

The Administration Panel Component provides a user interface for system administrators and operators. It has various functions, including data management, system configuration, and reporting. It allows users to configure data sources, manage crawling settings, set up alert mechanisms, integrates the Reporting Component and relies on the output from the previous components.

The interactions between these components can be complex and multidirectional. The Collect and Pre-Process Component feeds data into the Storage Component, while the Processing Component uses stored data for reputation assessment. The Machine Learning Component continuously refines its models based on new and existing processed data. The Administration Panel Component manages the configuration and monitoring of the entire system, while the Reporting Component disseminates information to various stakeholders.

This Information System Architecture view provides an understanding of the domain name reputation system, highlighting the Information System functions and components, interactions and processes involved. Thus, it enables the stakeholders and architects to visualize the system's architecture and how its components interact to achieve the system's objectives.

5.4 Technology Architecture View

A TOGAF Technology Architecture View of a Domain Name Reputation System, illustrated in Figure 4, outlines the technologies used by each system component, providing insights into the technology stack.

The Collect and Pre-Process Component (developed in Golang) is responsible for collecting domain data from various sources on the Internet. Golang, also known as Go, is a statically typed, compiled language known for its efficiency, concurrency support, and strong ecosystem of libraries. It's well-suited for developing web crawlers and data acquisition tools due to its performance characteristics.

The Storage Component (developed in Mongo and PostgreSQL) serves as a repository for both raw and pre-processed data. It employs a combination of database technologies:

- PostgreSQL is used as the database management system for the TLDRep Dashboard. It is a powerful and open-source relational database known for its data integrity and reliability. PostgreSQL stores all the relevant data, including domain reputation information, user accounts, and configuration settings.

- Instead of using PostgreSQL for storing raw, unstructured data from the crawler, a

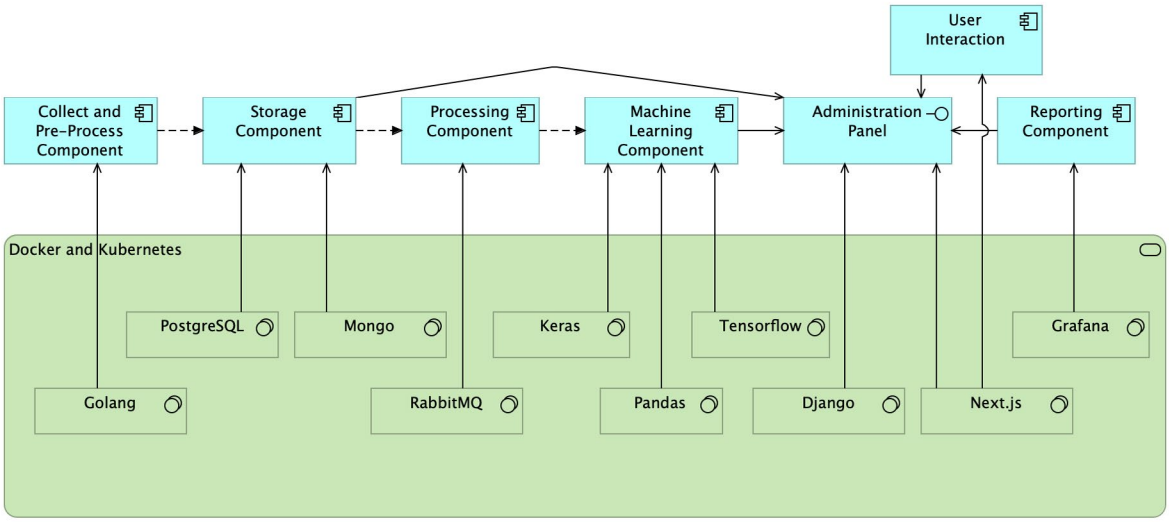

Figure 4. Technology Architecture View

MongoDB database will be used. MongoDB's flexible document-based structure is ideal for accommodating different data types and structures that may be encountered during web crawling. It's particularly suitable for handling large volumes of semi-structured or JSON-like data.

The Processing Component processes and analyses the data. It utilizes RabbitMQ, a message broker that enables efficient communication between different components of the system. It's a reliable choice for handling data processing tasks and workload distribution.

The Machine Learning Component (Keras, Pandas, Tensorflow) employs various machine learning and data analysis libraries:

- Keras, an open-source deep learning framework that provides high-level abstractions for building and training machine learning models, including neural networks;
- Pandas, a data manipulation and analysis library that offers data structures and functions for working with structured data;
- Tensorflow, an open-source machine learning framework developed by Google. It's used for building and training machine learning models, including deep learning models. It's known for its flexibility and support for neural networks.

The Administration Panel Component (Django and Node.js) provides a user-friendly interface for system administrators and users. It includes Reporting Component and User Interaction Component. Reporting Component ensures real-time monitoring functionality as it displays updates on domain reputation, allowing users to quickly respond to changes and potential threats. User Interaction enables users to interact with the data, such as manually verifying domain reputations and making informed decisions based on the information presented.

It combines several technologies. The backend of the system Administration Panel is built using the Django framework. Django is a high-level Python web framework known for its robust and secure features. It is used to carry out various server-side tasks such as handling requests, managing databases, and processing data.

The user interface is developed using Next.js with ReactJS, a popular React framework that simplifies the creation of server-rendered React applications. ReactJS is a JavaScript library for building user interfaces. Together, they provide an efficient and interactive user interface for accessing and visualizing domain reputation data.

The selection of specific technologies including TensorFlow, RabbitMQ, and Django for the implementation of a Domain Name Reputation System can be justified based on their features, capabilities, and suitability for the system's requirements. These include databases and data storage solutions to ensure data persistence and retrieval and also data backup and archiving.

These technologies were selected after a preliminary analysis so that they support the implementation of the system which should match the specific requirements and functions of each system component. The combination of these technologies ensures efficient data collection, processing, storage, machine learning, and user interaction, creating a robust and comprehensive domain name reputation system.

This Technology View provides a comprehensive overview of the technologies utilized by each component within the Domain Name Reputation System. It ensures that stakeholders have a clear understanding of the technological stack, enabling an effective communication and alignment of the technology architecture with an organization's goals and requirements.

6. Conclusion

A further step in the development of the TLDrep - Domain Name Reputation System consisted in using TOGAF, one of the most widely used enterprise architecture frameworks to create the design of the system architecture at business, information and data systems and technology levels. The objective of this system is to support and promote a safer online experience for all stakeholders, end users, domain owners, registrars and the domain registry.

The purpose of this research approach is to design the architecture of the proposed system including stakeholders, business functions, data assets, application functions, services, and technology components. This is necessary due to the complex nature of the system, as it involves multiple input data sources, components, and services that can generate a reputation score for the domain names administered by the national domain Registry.

This paper compares four prominent Enterprise Architecture (EA) frameworks, namely Zachman, TOGAF, FEAF (Federal Enterprise Architecture Framework), and UAF (Unified Architecture Framework), it selects the most appropriate framework for designing a Generic Architecture for a Domain Name Reputation System and brings about several innovation outcomes.

The Framework Evaluation Methodology is a comprehensive methodology for evaluating and comparing EA frameworks. It includes criteria such as Scope and Applicability, Alignment with industry standards, Emphasis on Business Architecture, Performance and metrics, Modelling language, Data Management, Service-Oriented Architecture and Security and Privacy. This methodology can be a valuable contribution to the field, helping architects and organizations make more informed choices when selecting an EA framework.

By comparing four EA frameworks, this paper can provide insights into the strengths and weaknesses of each framework. This cross-framework analysis can help architects understand which framework best aligns with their specific project or system design requirements. It also facilitates a more objective and data-driven selection process.

This paper proposes a framework selection model that takes into account the unique characteristics and needs of a Domain Name Reputation System. This model can serve as a template for selecting the most suitable EA framework for other specific application domains.

The study highlights the degree to which each EA framework aligns with industry standards and best practices, ensuring that the chosen framework is compliant and can be seamlessly integrated into the existing technology ecosystem.

Also, the study's results include the selection of the most appropriate EA framework for a Domain Name Reputation System. This, in turn, leads to a better-designed system that is well-aligned with an organization's goals, ensuring its optimal performance and efficiency.

Ultimately, the study's innovation results include the use of TOGAF Architecture Development Methodology to create the generic architecture of the analysed system, as a preliminary step to solution development.

In summary, using TOGAF for designing a Domain Name Reputation System can lead to a better structure, enable its alignment with industry standards and best practices and bring about efficiency to the architecture development process. It helps ensure that the system is well-defined, well-managed, and well-suited to meet the organization's needs and objectives while

mitigating risks and maximizing the value of reputation assessments.

In the future, an experimental model will be developed based on the above-mentioned architecture. The system will generate reputation scores for new domains based on learned models by studying the patterns of legitimate and malicious domains using anonymized data from the RoTLD domain Registry. The project's prototype will be used to detect and monitor malicious registered domains. The following step will be the development of the TLDRep software solution, which will empower domain name registries and users.

Acknowledgements

This research work was supported by a grant of the Romanian Ministry of Research, Innovation and Digitization, Nucleu Programme, project code: PN 2338 02 01, project name "Architecture - platform of an intelligent system for monitoring Internet domains by developing a dynamic reputation establishment system (TLDRep)" and by a grant of the Romanian Academy of Sciences through the competition "AOSR-TEAMS-II" Edition 2023-2024 - "Digital transformation in Science", project name "Digital transformation tools for eGovernment through the use of .ro domains".

REFERENCES

Banciu, D. & Dumitrache, M. (2016) *Managing a cloud-based documents system*. In: *Proceedings of The 2nd International Scientific Conference SAMRO 2016* -" News*, challenges and trends in management of knowledge-based organizations"*, *October 2016, Romania*. Editura Tehnică (Technical Publishing House), pp. 13-19.

Bolster. (2023) *The Most Critical Domain Security Risks & Five Ways to Prevent Attacks*. https://bolster.ai/blog/domain-security-risks [Accessed 12th October 2023].

Cîrnu, C. E., Rotună, C. I., Vevera, A. V. & Boncea, R. (2018) Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. *Studies in Informatics and Control*. 27(3), 359-368. doi: 10.24846/v27i3y201811.

Dijkstra, E. W. (1968) The structure of the "THE"-multiprogramming system. *Communications of the ACM*. 11(5), 341-346. doi: 10.1145/363095.363143.

Dumitrache, M., Sandu, I. E., Udroiu, A. M. & Gheorghiță, C. A. (2023) Considerații teoretice privind stabilirea reputației unui domeniu Internet [Theoretical considerations about establishing the Internet domain reputation]. *Revista Română de Informatică şi Automatică* [*Romanian Journal of Information Technology and Automatic Control*]. 33(1), 81-92. doi: 10.33436/v33i1y202307.

Harkai, A., Cinpoeru, M. & Buchmann, R. A. (2018) The "What" Facet of the Zachman Framework – A Linked Data-Driven Interpretation. In: Matulevičius, R. & Dijkman, R. (eds.) *Advanced Information Systems Engineering Workshops. CAiSE 2018. Lecture Notes in Business Information Processing*, vol 316. Cham, Switzerland, Springer, pp. 197-208. doi: 10.1007/978-3-319-92898-2_17.

IANA (2020) *Root Zone Database*. https://www.iana.org/domains/root/db [Accessed 10th February 2023]

Internet Corporation for Assigned Names and Numbers (ICANN). (2023) *Securely Managing Your Domain Name.* https://www.icann.org/resources/pages/securely-managing-domain-name-2020-08-26-en [Accessed 10th February 2023]

Kotusev, S. (2018) TOGAF: Just the Next Fad That Turned into a New Religion. In: Smith, K. L. (ed.) *TOGAF Is Not an EA Framework: The Inconvenient Pragmatic Truth*. Great Notley, UK, Pragmatic EA Ltd, pp. 27-40.

Kouroshfar, E., Mirakhorli, M., Bagheri, H., Xiao, L., Malek, S. & Cai, Y. (2015) A study on the role of software architecture in the evolution and quality of software. In: *2015 IEEE/ACM 12th Working Conference on Mining Software Repositories*, *16-17 May, 2015*, *Florence, Italy*. IEEE, 246-257.

Lockheed Martin. (2019) *Cyber Kill Chain®*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed 10th February 2023]

Object Management Group. (2023a) *BPMN Specification - Business Process Model and Notation*. https://www.bpmn.org/ [Accessed 12th December 2023]

Object Management Group. (2023b) *Unified Modeling Language, UML*. http://www.omg.org/spec/UML/ [Accessed 15th December 2023]

Object Management Group. (2023c) *Unified Architecture Framework (UAF)* https://www.omg.org/uaf [Accessed 15th November 2023]

Priyadharshini. (2013) *Top 10 Benefits of TOGAF® Certification in Enterprise Architecture*. https://www.

simplilearn.com/togaf-certification-benefits-article [Accessed 10th November 2023]

RiskAnalytics. (2023) *Malware Domain Block List*. https://riskanalytics.com/ [Accessed 17th January 2023]

Rocha, F. G., Misra, S. & Soares, M. S. (2023) Guidelines for Future Agile Methodologies and Architecture Reconciliation for Software-Intensive Systems. *Electronics*. 12(7), 1582. doi: 10.3390/electronics12071582.

Rotună, C. I., Gheorghiță, C. A., Sandu, I. E., Dumitrache, M., Udroiu, A. M. & Smada, D. (2023) A Generic Architecture for Building a Domain Name Reputation System. *Studies in Informatics and Control*. 32(2), 39-49. doi: 10.24846/v32i2y202304.

Royce, W. E. & Royce, W. (1991) Software architecture: Integrating process and technology. *Quest*. 14(1), 2-15.

Shaw, M. & Garlan, D. (1996) *Software architecture: perspectives on an emerging discipline*. Hoboken, Prentice-Hall, Inc..

Tepandi, J., Grandry, E., Fieten, S., Rotuna, C., Sellitto, G. P., Zeginis, D., Draheim, D., Piho, G., Tambouris, E. & Tarabanis, K. (2019) Towards a cross-border reference architecture for the once-only principle in Europe: an enterprise modelling approach. In: Gordijn, J., Guédria, W. & Proper, H. A. (eds.) *The Practice of Enterprise Modeling: 12th IFIP Working Conference, PoEM 2019, 27 - 29 November, 2019, Luxembourg, Luxembourg.* Springer International Publishing, pp. 103-117.

The Open Group. (2023a) *TOGAF | The Open Group*. https://www.opengroup.org/togaf [Accessed 13th November 2023]

The Open Group. (2023b) *Archi - Open Source ArchiMate Modelling*. https://www.archimatetool.com/ [Accessed 10th December 2023]

U.S. Government. (2023) *Federal Enterprise Architecture Framework*. https://www.cms.gov/data-research/cms-information-technology/enterprise-architecture/federal-enterprise-architecture-framework [Accessed 20th November 2023]

Visual Paradigm. (2019) *What is Zachman Framework?* https://www.visual-paradigm.com/guide/enterprise-architecture/what-is-zachman-framework/ [Accessed 13th November 2023]

Whiting, E. & Andrews, S. (2020) Drift and erosion in software architecture: summary and prevention strategies. In: *Proceedings of the 2020 4th International Conference on Information System and Data Mining*, *ICISDM 2020, 15-17 May, 2020, Hawaii, USA*. Association for Computing Machinery, 132-138.

Zachman, J. A. (1996) *The Framework for Enterprise Architecture: Background Description and Utility*. https://zachman-feac.com/the-framework-for-enterprise-architecture-background-description-and-utility [Accessed 14th November 2023]

Zachman, J. A. (2010) Architecture Is Architecture Is Architecture. In: Kappelman, L. A. (ed.) *The SIM Guide to Enterprise Architecture*. Boca Raton, FL, CRC Press, pp. 37-45.