RESEARCH ARTICLE

SAMRIDDHI Volume 18, Issue 3, 2026 Print ISSN: 2229-7111 Online ISSN: 2454-5767

Reducing DNS Domain Management Overhead in Large Enterprises: A Self-Service Portal Approach with Centralized Domain Intelligence

Abdalhadi Skaik

Wipro arabia ltd saudi arabia

Abstract

As enterprise information technology (IT) environments grow more complex, there is a greater need for efficient Domain Name System (DNS) domain management to facilitate digital services, cloud adoption, and cross-functional collaboration. For many large organizations, domain-specific questions continue to be handled traditionally through centralized IT Service Desks, which causes high ticket volumes, long resolution times, and poor use of technical staff time. The present invention provides a self-service DNS domain management portal having central intelligence of domain information to simplify domain discovery and metadata retrieval and to decrease operational overhead. The solution being proposed involves consolidating all the internal DNS records, organisational metadata, and information from external domain registries into a central repository, allowing authenticated users to conduct real-time searches of the domains with a secure web-based front-end. Built on ASP. The portal improves accessibility, improves governance, and reduces manual support processes and reliance on NET Core, as well as increasing governance and support using Microsoft SQL Server with Windows Authentication. The proposed architecture illustrates the benefits of centralising domain intelligence for more efficient service delivery, enterprise-wide decision-making, and optimised IT services. The study provides a scalable and practical approach to modern enterprise DNS management, which is aligned with the platform engineering, self-service IT, and intelligent network management trends.

Keywords: DNS Management, Centralized Domain Intelligence, Self-Service Portal, Enterprise IT Service Management, Platform Engineering, ASP.NET Core, Network Automation, Digital Transformation.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2026); DOI: 10.18090/samriddhi.v18i03.01

Introduction

More than ever before, the growth of digital transformation programs, cloud computing, and distributed enterprise applications has added to the complexity of managing Domain Name System (DNS) infrastructures in large organizations. Across a range of different enterprise architectures and topologies, such as hybrid cloud deployments, Software-as-a-Service (SaaS) platforms, and multi-domain networks, DNS has matured from a basic naming service on the Internet to a much more critical part of enterprise service delivery, security, and operational governance (Haritwal, 2026; Schmid, 2021). Modern DNS infrastructures not only enable translation of domain names to Internet Protocol (IP) addresses, but they also help application access, network availability, application discovery, and secure communication in geographically distributed business environments (Internet Engineering Task Force [IETF] 1987a, 1987b; Liu & Albitz, 2006).

In large enterprises, thousands of domain names are registered internally and externally for various applications, internal services, cloud resources, partner integrations, and development environments. It's crucial to have the right visibility of domain ownership, registration status, related business units, technical setups, and life cycle information when managing these domain assets. In many organisations, however, such information is still limitedly available to employees, project managers, business analysts, and system administrators, and they have to make a formal service desk request to get relatively simple domain-related information (Herger et al., 2017; Gartner, 2023). This centralised approach can lead to administrative control, but often causes undue delays, higher operational costs, and a lower utilisation

Corresponding Author: Abdalhadi, Wipro arabia ltd saudi arabia, e-mail: abdalhadis@gmail.com

How to cite this article: Skaik A. (2026). Reducing DNS Domain Management Overhead in Large Enterprises: A Self-Service Portal Approach with Centralized Domain Intelligence. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 18(3), 1-21.

Source of support: Nil

Conflict of interest: None

of technical staff time in more value-added infrastructure management tasks.

Traditional IT Service Management (ITSM) processes are built to rely on ticket-based workflows to capture and track user requests, to comply with governance policies and service-level agreements (SLAs). These workflows are very effective for configuration management and incident handling, but are much less efficient for common informational requests like checking domain ownership, determining who registered a domain, and checking if a specific domain already exists in the organization. These requests typically involve little technical complexity but can also take up time in IT because of the need to perform manual verifications, multiple approvals, and the coordination required in the service desk (Herger et al., 2017; Gartner, 2023). The totality of these support activities can lead to rising operational overhead, decreased service responsiveness, and diminished organizational productivity as organizations continue to expand their digital ecosystem.

The development of platform engineering and internal developer platforms (IDPs) has shown the benefits of self-service technologies for greater operational efficiency and less reliance on centralized administration teams. Self-service platforms can boost developer productivity, speed up decision-making, and facilitate enterprise scalability while ensuring governance and security best practices are adhered to (Rusum & Pappula, 2024; Pendyala, n.d.). Likewise, intelligent network management has shifted from a manual configuration strategy to an automated network architecture that enhances the visibility, resilience, and service experience of a network by using centralized management processes (Sidhu & Sharma, 2026; Saadon, 2022). The developments suggest that enterprise infrastructure management is increasingly gaining advantages from having an information repository in the center, which allows users to access information in real time without sacrificing management aspects.

In the field of DNS management, previous research has mainly centered on the design of the protocol, its security improvement, resolution methods, and smart management frameworks. The architecture of Internet naming systems was defined by basic DNS standards (IETF, 1987a, 1987b), and later work examined intelligent DNS management techniques (Chen et al., 2003), DNS security (Chandramouli & Rose, 2006), secure deployment practices (Dooley & Rooney, 2017), and infrastructure resilience (Schmid, 2021). As organizations transition to hybrid and multi-cloud models, the focus of more recent research has shifted to outsourced DNS solutions, managed DNS infrastructures, and cloud-based network orchestration (de Amaral Gomes, 2023; Haritwal, 2026). While such contributions have been made, relatively little effort has been given to making organizations more accessible to DNS-related information by delivering enterprise self-service solutions that have integrated technical infrastructure information and organizational metadata, reducing routine IT support overhead.

This work aims to fill the void by introducing a self-service DNS Domain Management Portal with domain intelligence. The proposed solution combines information from internal DNS infrastructure and organizational repositories with information from external sources of domain registration in a single database, providing access to the information via a secure web application. Developed using ASP. The portal allows authenticated enterprise users to access domain information in real-time without needing formal helpdesk support, enhancing accessibility while maintaining governance and security within the organization (Microsoft Corporation, 2024a, 2024b, 2024c).

The proposed framework is built on enterprise-wide information accessibility, combined with secure self-service capabilities, while conventional DNS management solutions are mainly geared towards network administrators. The architecture facilitates fast domain discovery, better visibility between business units, fewer repetitive service requests, and allows IT staff to prioritize strategic activities in managing the infrastructure instead of routine information activities. Moreover, the framework fits with new challenges in enterprise platform engineering, Zero Trust architecture, intelligent network management, and digital workplace transformation, where centralized knowledge bases and automated service delivery are becoming critical organizational skills (Patel & Ng, 2025; Dakić et al., 2024; Sharma et al., 2025).

The main value of this research is the design and testing of a scalable enterprise framework that combines DNS intelligence in the centralized service with secure, self-service access to the DNS, thereby minimizing the domain management overhead. The results of this study show that the overall operational efficiency can be substantially increased, the dependency on tickets is decreased, information is more accessible, and enterprise governance will be strengthened by bringing heterogeneous domain information under one roof. This paper not only covers the system architecture and implementation approach, but it also explores the operational advantages, practical implications, and potential future applications of enabling intelligent automation and advanced platform engineering principles to extend the centralized DNS management.

Related Work and Research Background

The increasing complexity of enterprise information technology (IT) ecosystems has fundamentally transformed the role of Domain Name System (DNS) management from a basic network service into a strategic component of enterprise governance, cybersecurity, and digital service delivery. Organizations operating hybrid cloud infrastructures, multi-site networks, and Software-as-a-Service (SaaS) environments increasingly rely on DNS to ensure application availability, secure communications, workload accessibility, and business continuity. Consequently, researchers have

devoted considerable attention to DNS architecture, intelligent network management, service automation, and platform engineering to improve the efficiency and resilience of enterprise infrastructures (Sidhu & Sharma, 2026; Haritwal, 2026). This section reviews the existing body of knowledge on enterprise DNS management, centralized domain intelligence, self-service platforms, and IT service automation. It identifies the research gap addressed by the proposed framework.

ution of Enterprise DNS Management

The Domain Name System was introduced in the early 1980s to replace the centralized HOSTS.TXT file that became increasingly difficult to maintain as the Internet expanded. RFC 1034 and RFC 1035 established the hierarchical and distributed naming architecture that remains the foundation of modern DNS infrastructure (Internet Engineering Task Force [IETF], 1987a, 1987b). Initially designed to provide scalable name resolution between human-readable domain names and IP addresses, DNS has evolved into a critical infrastructure supporting virtually every Internet-enabled service.

Modern enterprises operate thousands of domain names supporting internal applications, cloud services, customer portals, development environments, partner integrations, and Internet-facing business platforms. As organizations expanded their digital operations, DNS management evolved beyond simple zone administration to encompass governance, lifecycle management, policy enforcement, infrastructure resilience, and cybersecurity (Liu & Albitz, 2006; Dooley & Rooney, 2017). Enterprise DNS infrastructures now support distributed computing environments where cloud resources, containerized applications, edge computing, and virtualized services require continuous domain registration, monitoring, and synchronization.

Network management itself has undergone substantial transformation over the past two decades. Traditional manual configuration approaches have gradually been replaced by automated management systems capable of monitoring, provisioning, and optimizing network resources with minimal human intervention. Sidhu and Sharma (2026) describe this evolution as a progression from reactive administration toward intelligent automation, where centralized visibility and automated decision support significantly improve operational efficiency. Likewise, Saadon (2022) argues that future network management depends increasingly on autonomous infrastructures capable of adapting dynamically to changing operational conditions.

Within enterprise environments, DNS has become tightly integrated with identity management, application deployment, cloud orchestration, disaster recovery planning, and Zero Trust security architectures. Rather than functioning solely as a naming service, DNS now supports numerous organizational processes that require accurate and timely access to domain-related information (Schmid, 2021). Consequently, the efficiency of DNS administration has become an important determinant of enterprise operational performance.

Despite advances in DNS infrastructure technologies, many organizations continue to depend on centralized administrative teams for routine domain-related information retrieval. Employees frequently submit service requests simply to determine whether a domain exists, identify ownership, verify registration status, or obtain associated technical information. These repetitive informational requests consume valuable IT resources despite requiring little technical expertise, highlighting the growing need for more accessible enterprise DNS information services (Herger et al., 2017; Gartner, 2023).

Domain Name System Architecture and Centralized Domain Intelligence

Modern DNS infrastructures comprise multiple interconnected components including authoritative name servers, recursive resolvers, zone databases, domain registries, registrar services, security extensions, and enterprise management platforms. Together, these components provide the foundation for reliable domain resolution while supporting availability, scalability, and fault tolerance across geographically distributed environments (Liu & Albitz, 2006; Chandramouli & Rose, 2006).

As enterprise infrastructures become increasingly decentralized through cloud computing and multi-cloud deployments, DNS information is often dispersed across multiple administrative systems. Internal DNS servers maintain organizational records, public registrars store registration information, cloud platforms manage service endpoints, while project documentation contains ownership and business metadata. This fragmentation frequently creates information silos that complicate administrative visibility and increase the time required to retrieve domain-related information.

To address these challenges, researchers have explored intelligent DNS management approaches that combine heterogeneous information sources into unified knowledge repositories. Chen et al. (2003) proposed one of the earliest intelligent DNS management frameworks by integrating multiple knowledge sources into a unified decision-support architecture capable of improving DNS administration. More recently, Babakian (2024) extended this concept by introducing context-aware Internet identifier resolution, enabling more intelligent interpretation of naming information according to organizational context.

Centralized domain intelligence builds upon these concepts by consolidating technical DNS records, registration data, organizational ownership information, and operational metadata within a single repository. Rather than requiring administrators to consult multiple independent systems, centralized repositories provide unified visibility into enterprise domain assets. Such integration improves

Table 1: Comparison of Traditional and Centralized Enterprise DNS Management Approaches

Feature	*Traditional DNS Management*	*Centralized Domain Intelligence*
Information source	Multiple independent systems	Unified enterprise repository
Domain lookup	Manual administrator intervention	Instant self-service search
Ownership identification	Separate documentation	Integrated organizational metadata
Administrative workload	High	Significantly reduced
Governance visibility	Fragmented	Centralized
Decision support	Limited	Comprehensive
Scalability	Moderate	High
Integration capability	Low	High

Source: Adapted from Chen et al. (2003), Dooley and Rooney (2017), Schmid (2021), de Amaral Gomes (2023), Babakian (2024), and Haritwal (2026), with modifications by the author.

governance, accelerates information retrieval, simplifies auditing processes, and supports strategic decision-making across organizational units (de Amaral Gomes, 2023).

Furthermore, outsourced managed DNS services have increased the importance of centralized intelligence. Organizations increasingly distribute domain management responsibilities across cloud providers, managed DNS vendors, and internal infrastructure teams. Haritwal (2026) notes that although managed DNS services improve scalability and operational resilience, they also introduce governance challenges associated with maintaining consistent visibility across multiple administrative domains. Centralized intelligence repositories provide an effective mechanism for mitigating these challenges by aggregating distributed domain information into a unified enterprise knowledge base.

The emergence of Zero Trust security models has further strengthened the importance of centralized information management. Rather than assuming trust based on network location, Zero Trust architectures require continuous verification of identities, assets, and resources. Consequently, maintaining comprehensive and accurate domain intelligence becomes essential for enforcing organizational security policies and improving infrastructure visibility (Dakić et al., 2024).

Self-Service Portals and Platform Engineering

The rapid adoption of DevOps, cloud-native computing, and digital transformation has accelerated the emergence of self-service platforms as a core principle of enterprise infrastructure management. Rather than relying on centralized administrative teams for routine operational tasks, modern organizations increasingly empower employees and developers with secure self-service capabilities that improve efficiency while maintaining governance.

Platform Engineering has emerged as one of the most influential paradigms supporting this transition. Rusum and Pappula (2024) define Internal Developer Platforms (IDPs) as centralized environments that abstract infrastructure complexity while providing standardized, secure, and reusable services for organizational users. These platforms reduce operational bottlenecks by enabling users to independently access approved infrastructure resources without compromising organizational policies.

Similarly, Pendyala argues that enterprise cloud architecture is undergoing a paradigm shift toward service automation, reusable infrastructure components, and platform-centric service delivery. These developments reduce dependency on manual administrative processes while improving operational consistency across enterprise environments (Pendyala, n.d.).

Self-service portals represent a practical implementation of platform engineering principles. Rather than functioning solely as user interfaces, these portals provide policy-driven access to enterprise information, infrastructure services, and operational resources. By integrating authentication mechanisms, centralized databases, and automated workflows, self-service portals enable organizations to improve productivity while reducing support workloads (Patel & Ng, 2025).

Enterprise self-service technologies have become particularly valuable in large organizations where thousands of users require frequent access to operational information. Instead of relying on helpdesk personnel to retrieve data manually, authenticated users can directly obtain relevant information through centralized repositories, significantly reducing service request volumes and improving response times (Herger et al., 2017).

Recent developments in multi-tenant SaaS architectures demonstrate that centralized service platforms can simultaneously achieve scalability, security, and operational flexibility. Sharma et al. (2025) emphasize that properly designed enterprise platforms support secure resource sharing while maintaining isolation between organizational units, making them suitable foundations for enterprise-wide information management systems.

The principles of platform engineering therefore provide strong theoretical support for implementing

centralized DNS self-service portals capable of reducing administrative overhead while improving enterprise information accessibility.

Enterprise IT Service Management (ITSM) and Service Automation

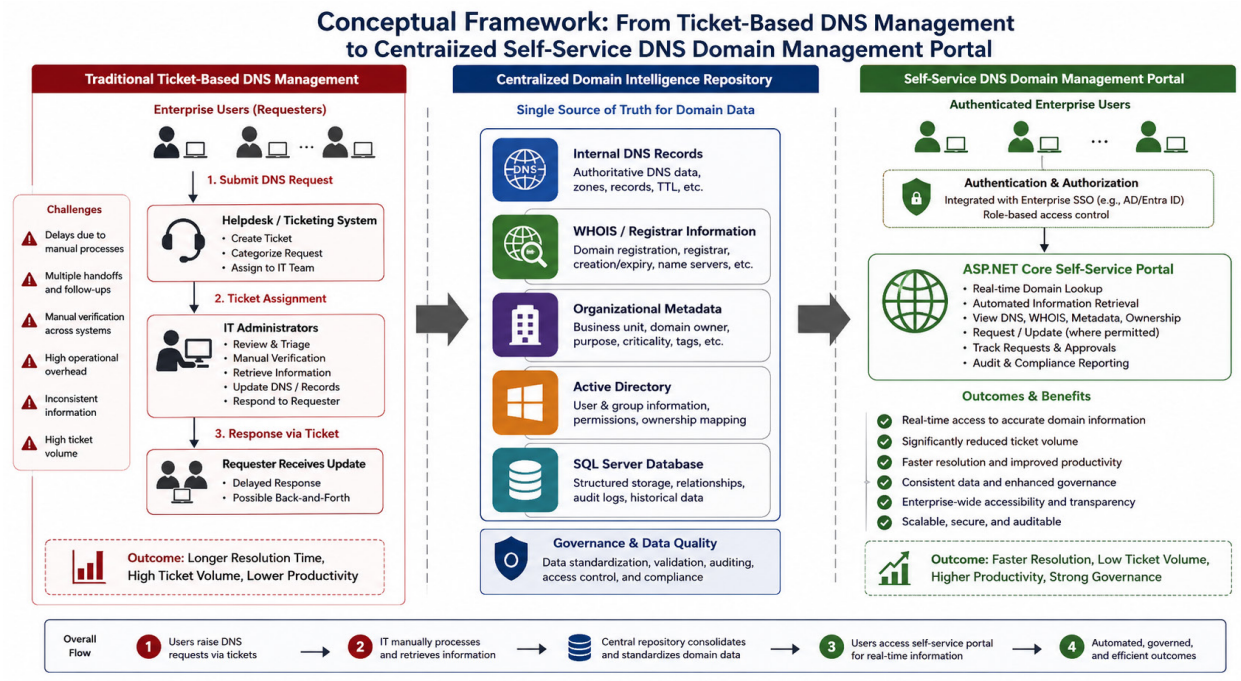
Enterprise Information Technology Service Management (ITSM) provides the organizational framework through which IT services are designed, delivered, operated, and continually improved. The primary objective of ITSM is to ensure that technology services consistently support organizational goals while maintaining service quality, operational efficiency, and regulatory compliance. Frameworks such as the Information Technology Infrastructure Library (ITIL) have become widely adopted because they establish standardized processes for incident management, service requests, configuration management, change management, and service delivery (Gartner, 2023). Although these frameworks have significantly improved organizational governance, they remain highly dependent on structured workflows that frequently require manual intervention.

In large enterprises, service desk operations serve as the primary communication channel between end users and IT departments. Employees submit requests for infrastructure access, software installation, application support, account provisioning, and network-related information through centralized ticketing systems. While this model ensures accountability and proper documentation, it often creates unnecessary administrative overhead for repetitive, low-complexity tasks that could otherwise be completed independently by authorized users (Herger et al., 2017).

DNS-related inquiries represent a common example of this operational inefficiency. Many service requests involve retrieving existing information rather than modifying infrastructure resources. Questions regarding domain ownership, registration status, project affiliation, DNS record availability, or registrar information generally require simple database lookups instead of specialized engineering expertise. Nevertheless, these requests often pass through the same approval workflows as complex infrastructure changes, increasing ticket queues, extending response times, and reducing the availability of IT personnel for strategic initiatives.

Herger et al. (2017) demonstrated that enterprise-wide service data analysis can reveal significant operational inefficiencies caused by fragmented information access. Their findings indicate that consolidating enterprise service information into accessible repositories enables organizations to reduce redundant support activities while improving overall service responsiveness. Similarly, Gartner (2023) identifies self-service capabilities as one of the most influential trends shaping modern ITSM, emphasizing that organizations increasingly seek to automate routine support functions while preserving governance and compliance.

The growing adoption of intelligent automation further reinforces this transition. Rather than relying exclusively on human administrators to process every service request, organizations increasingly implement automated workflows



Source: Developed by the author based on Herger et al. (2017), Rusum and Pappula (2024), Sidhu and Sharma (2026), and Gartner (2023).

Figure 1: Conceptual Framework of Self-Service DNS Domain Management

capable of routing requests, retrieving information, enforcing organizational policies, and supporting decision-making processes. According to Sidhu and Sharma (2026), intelligent network management combines centralized visibility with automation technologies to reduce administrative complexity while improving infrastructure reliability. These principles align closely with service automation strategies that seek to eliminate repetitive manual tasks across enterprise IT environments.

Service automation also complements the emergence of platform engineering, where reusable infrastructure services are exposed through standardized interfaces. Instead of requiring users to interact directly with IT administrators, self-service platforms provide secure access to organizational resources while automatically enforcing governance policies. Pendyala argues that automation-driven enterprise cloud architectures improve operational consistency, accelerate service delivery, and reduce dependence on manual administrative processes. Consequently, integrating service automation into DNS management represents a logical extension of broader enterprise digital transformation initiatives (Pendyala, n.d.).

Within DNS administration, automated self-service platforms can significantly reduce operational costs by transforming information retrieval into an instantaneous process. Rather than submitting service tickets, authenticated users can independently search centralized repositories containing domain metadata, ownership information, registration records, and technical configurations. Such capabilities improve organizational productivity while enabling IT departments to focus on infrastructure optimization, cybersecurity, and strategic innovation rather than repetitive administrative tasks.

Secure Enterprise Identity and Access Management

As enterprise infrastructures become increasingly interconnected, ensuring secure access to organizational resources has become a fundamental requirement for effective information management. Identity and Access Management (IAM) systems provide the mechanisms by which organizations authenticate users, authorize access to resources, and enforce security policies across distributed computing environments. Rather than relying solely on network boundaries for protection, modern security architectures emphasize continuous identity verification, least-privilege access, and context-aware authorization.

The emergence of Zero Trust Architecture (ZTA) has accelerated this paradigm shift. Unlike traditional perimeter-based security models that assume internal network traffic is inherently trustworthy, Zero Trust frameworks require every user, device, and application to be authenticated and continuously validated before access is granted (Dakić et al., 2024). This approach significantly improves organizational resilience against insider threats, credential compromise, and unauthorized resource access while supporting increasingly distributed workforces and hybrid cloud infrastructures.

Enterprise identity management also plays a crucial role in facilitating secure self-service capabilities. Ndike (2023) argues that Bring-Your-Own Identity (BYOI) models and federated identity systems improve business collaboration by enabling secure authentication across organizational boundaries while reducing administrative complexity. These identity-centric approaches ensure that users access only information consistent with their assigned organizational roles, thereby balancing accessibility with governance.

Microsoft Windows Authentication provides one practical implementation of enterprise identity integration. By leveraging Active Directory and Kerberos authentication protocols, organizations can enable seamless Single Sign-On (SSO) without requiring users to maintain separate application credentials. Microsoft Corporation (2024a, 2024b) notes that Windows Authentication strengthens enterprise security while improving user experience by integrating authentication directly into existing organizational identity infrastructures. Such capabilities are particularly valuable for internal enterprise portals where authenticated employees require rapid access to operational information.

Secure database management further supports enterprise identity governance. Microsoft SQL Server incorporates role-based access control, encryption mechanisms, auditing capabilities, and centralized security administration that collectively protect organizational information assets (Mistry & Misner, 2014; Microsoft Corporation, 2024c). When integrated with enterprise authentication systems, SQL Server provides a secure repository for storing sensitive operational metadata while ensuring that access permissions remain consistent across enterprise applications.

In addition to authentication, secure DNS management requires protection against domain hijacking, cache poisoning, spoofing attacks, and unauthorized administrative modifications. DNS Security Extensions (DNSSEC), secure deployment guidelines, and managed DNS infrastructures have significantly improved DNS resilience over the past two decades (Chandramouli & Rose, 2006; Dooley & Rooney, 2017; Schmid, 2021). However, organizational security also depends on ensuring that internal DNS intelligence is accessible only to authorized personnel. Consequently, integrating identity-aware authentication with centralized domain intelligence provides a comprehensive security framework that supports both operational efficiency and enterprise governance.

Collectively, these developments demonstrate that effective enterprise DNS management extends beyond infrastructure administration to include robust identity management, access control, and security governance. A self-service DNS management portal must therefore incorporate enterprise authentication mechanisms that preserve confidentiality while enabling efficient information retrieval for authorized users.

Research Gap

Despite extensive research on DNS architecture, network automation, service management, cloud orchestration, cybersecurity, and platform engineering, relatively few studies have investigated the operational challenges associated with enterprise-wide accessibility to DNS information. Existing literature has predominantly focused on protocol design (IETF, 1987a, 1987b), DNS security (Chandramouli & Rose, 2006; Dooley & Rooney, 2017; Schmid, 2021), intelligent DNS frameworks (Chen et al., 2003), managed DNS infrastructures (Haritwal, 2026), and network orchestration (de Amaral Gomes, 2023). While these contributions have significantly advanced DNS technologies, they provide limited guidance regarding how organizations can reduce administrative overhead associated with routine domain information requests.

Similarly, research on platform engineering and enterprise automation has emphasized infrastructure provisioning, cloud-native development, Internal Developer Platforms, and automated service delivery (Rusum & Pappula, 2024; Patel & Ng, 2025; Sharma et al., 2025). Although these studies demonstrate the effectiveness of self-service principles across software engineering environments, their application to enterprise DNS information management remains largely unexplored.

Another limitation within the existing literature is the lack of integration between technical DNS infrastructure and organizational metadata. Most published solutions concentrate primarily on technical domain resolution, network configuration, or security mechanisms without incorporating business ownership, project associations, registrar information, or enterprise governance into a unified information platform. Consequently, organizations continue to rely heavily on manual service desk workflows for retrieving information that already exists across multiple disconnected systems.

Furthermore, relatively little empirical attention has been devoted to evaluating the operational benefits of centralized domain intelligence repositories capable of reducing helpdesk ticket volumes while improving enterprise information accessibility. Existing studies acknowledge the importance of automation and centralized management but rarely examine how self-service DNS information platforms influence organizational productivity, governance, and IT resource utilization.

This present study addresses these limitations by proposing an enterprise self-service DNS Domain Management Portal supported by centralized domain intelligence. Unlike previous approaches that focus primarily on infrastructure administration or protocol functionality, the proposed framework integrates internal DNS records, organizational metadata, external registry information, secure enterprise authentication, and centralized database technologies into a unified platform designed specifically to reduce DNS domain management overhead. In doing so, this research contributes both a practical enterprise solution and an architectural framework that extends existing knowledge in DNS management, platform engineering, and enterprise IT service management.

The literature demonstrates that significant advances have been achieved in DNS architecture, network automation, cybersecurity, platform engineering, and enterprise service management. Nevertheless, a notable gap remains regarding the integration of centralized domain intelligence with secure self-service mechanisms for enterprise-wide DNS information accessibility. Existing studies primarily emphasize technical infrastructure, security, or automation, with comparatively limited attention devoted to reducing the administrative burden associated with routine domain information requests. By synthesizing concepts from DNS management, ITSM, platform engineering, and identity management, the proposed research establishes a comprehensive foundation for developing a centralized self-service DNS management framework capable of improving operational efficiency, strengthening governance, and supporting modern enterprise digital transformation.

System Design and Implementation

The effectiveness of an enterprise DNS management solution depends not only on its ability to maintain accurate domain records but also on how efficiently domain information can be accessed, managed, and secured across the organization. Conventional DNS management approaches typically rely on fragmented repositories, manual verification procedures, and centralized IT support, resulting in delayed service delivery and increased operational overhead (Herger et al., 2017; Gartner, 2023). To address these limitations, this study proposes a centralized self-service DNS Domain Management Portal that integrates domain intelligence from multiple enterprise data sources into a unified platform. The system emphasizes secure accessibility, operational efficiency, scalability, and governance while maintaining compatibility with existing enterprise infrastructure. This section describes the proposed system architecture, data management framework, implementation technologies, security mechanisms, and deployment strategy that collectively enable efficient enterprise DNS domain management.

Overall System Architecture

The proposed DNS Domain Management Portal adopts a multi-tier architecture that separates data acquisition, storage, business logic, and presentation services into independent but interconnected layers. This architectural approach enhances modularity, maintainability, and scalability while simplifying future system upgrades and integration with additional enterprise services (Toy & Toy, 2021; Sidhu & Sharma, 2026).

At the foundation of the architecture is the data acquisition layer, responsible for collecting domain-related

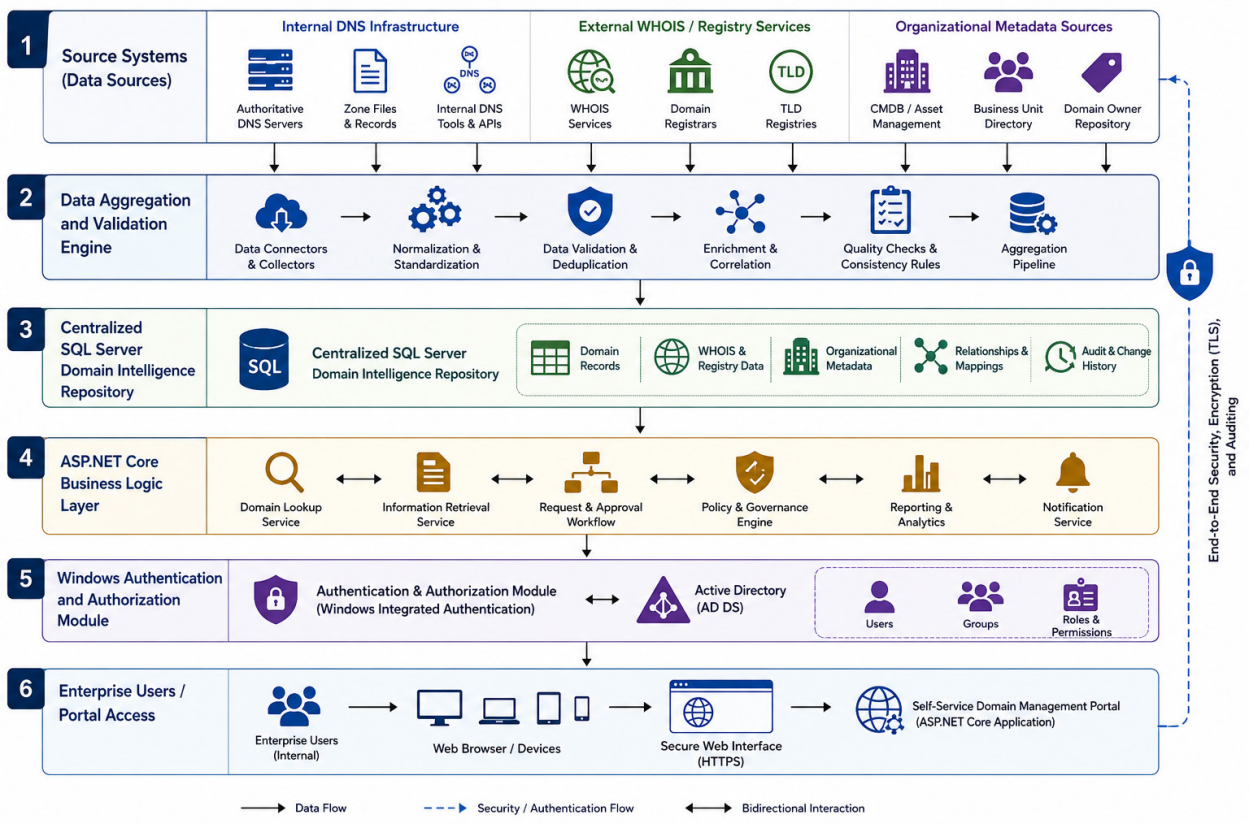


Figure 2: Proposed Architecture of the Centralized Self-Service DNS Domain Management Portal

information from heterogeneous sources. These include internal DNS servers, enterprise inventory repositories, project documentation, and external domain registration databases such as WHOIS services. Consolidating these datasets eliminates information silos and establishes a unified source of truth for enterprise domain assets (ICANN, 2024; Liu & Albitz, 2006).

The collected information is processed through a synchronization engine that validates, standardizes, and enriches domain records before storing them within a centralized Microsoft SQL Server database. During synchronization, duplicate entries are removed, inconsistent naming conventions are normalized, and organizational metadata including business unit ownership, project association, registration status, environment classification, and responsible administrative teams is appended to each record. Similar centralized data management strategies have been shown to improve enterprise information consistency and operational efficiency (Herger et al., 2017).

The application layer, developed using ASP.NET Core, processes user requests, executes optimized database queries, and returns structured results through secure application programming interfaces (APIs). ASP.NET Core was selected because of its high performance, enterprise compatibility, cross-platform capabilities, and extensive support for secure web application development (Microsoft Corporation, 2024a).

The presentation layer provides a browser-based interface through which authenticated users can search domains using multiple criteria, including domain name, project identifier, organizational department, registration provider, and operational status. Search results are displayed in real time, significantly reducing dependence on IT personnel for routine domain information retrieval.

Developed by the authors based on enterprise DNS management principles synthesized from Chen et al. (2003), Toy and Toy (2021), Microsoft Corporation (2024a), and Sidhu and Sharma (2026).

Centralized Domain Intelligence Repository

A defining feature of the proposed framework is the establishment of a centralized domain intelligence repository that consolidates technical, administrative, and organizational information relating to enterprise domain assets. Rather than maintaining isolated datasets across multiple departments, the repository integrates all relevant domain information into a structured relational database that supports efficient retrieval, governance, and lifecycle management.

The repository stores a comprehensive collection of attributes for each managed domain, including the domain name, registration status, registrar information, DNS zone configuration, associated IP addresses, hosting environment,

Table 2: Functional Components of the Proposed DNS Domain Management Portal

Component	*Primary Function*	*Organizational Benefit*
Data Acquisition Module	Collects domain information from internal DNS servers, registrars, and organizational repositories	Eliminates fragmented information sources
Data Validation Engine	Removes duplicate records and validates domain metadata	Improves data quality and consistency
Centralized SQL Server Repository	Stores consolidated domain intelligence	Provides a single authoritative source of domain information
ASP.NET Core Application Layer	Processes user requests and executes search operations	Enables rapid information retrieval
Windows Authentication Module	Authenticates enterprise users through Active Directory	Enhances security and simplifies access management
Self-Service User Portal	Provides browser-based domain search capabilities	Reduces IT support requests and improves user productivity

Developed by the authors based on enterprise DNS management principles presented by Herger et al. (2017), Mistry and Misner (2014), Microsoft Corporation (2024a, 2024c), and Toy and Toy (2021).

project ownership, business unit affiliation, creation date, expiration date, and designated administrative contacts. This integrated data model enables stakeholders from different organizational units to obtain a holistic view of domain assets without navigating multiple management systems (Mistry & Misner, 2014).

To ensure high query performance, indexed database structures are implemented on frequently accessed attributes such as domain name, organizational unit, and registration status. Index optimization substantially reduces search latency, enabling near-instant retrieval even when managing thousands of enterprise domain records. SQL Server's indexing mechanisms, transaction management, and role-based access controls provide a reliable foundation for enterprise-scale information management while supporting data integrity and concurrent user access (Microsoft Corporation, 2024c).

Beyond information storage, centralized domain intelligence facilitates organizational governance by providing consistent metadata across projects and departments. Decision-makers can quickly identify redundant domain registrations, monitor ownership responsibilities, verify compliance with organizational naming conventions, and improve asset visibility during infrastructure planning. Such centralized visibility has become increasingly important as enterprises adopt cloud-native platforms, distributed applications, and hybrid infrastructure environments that require coordinated domain governance (de Amaral Gomes, 2023; Haritwal, 2026).

Furthermore, the repository supports extensibility by allowing additional metadata fields and external integrations to be incorporated without significant architectural modifications. This flexibility enables future expansion toward automated policy enforcement, predictive analytics, AI-assisted domain management, and intelligent infrastructure orchestration, aligning with current trends in platform engineering and enterprise automation (Patel & Ng, 2025; Rusum & Pappula, 2024).

Data Aggregation and Synchronization Mechanism

To ensure that the DNS Domain Management Portal provides accurate and reliable information, a structured data aggregation and synchronization mechanism was developed to consolidate domain intelligence from multiple enterprise sources. Enterprise DNS information is often dispersed across internal DNS servers, cloud platforms, domain registrars, project documentation, and infrastructure management systems, making it difficult to obtain a unified view of domain assets. Integrating these heterogeneous data sources into a centralized repository minimizes information inconsistencies while improving operational transparency and administrative efficiency (Herger et al., 2017; de Amaral Gomes, 2023).

The synchronization process follows a staged workflow consisting of data extraction, validation, transformation, enrichment, and loading (ETL). During extraction, current domain records are retrieved from internal DNS infrastructure together with organizational metadata and publicly available registration information. The collected records are then validated to eliminate duplicate entries, resolve naming inconsistencies, and identify incomplete records before they are standardized according to predefined enterprise naming policies. Metadata enrichment subsequently associates each domain with relevant organizational attributes, including department ownership, project classification, operational environment, registrar information, and lifecycle status.

Rather than implementing continuous synchronization, the proposed framework adopts scheduled synchronization complemented by administrator-triggered updates whenever major infrastructure changes occur. This strategy significantly reduces processing overhead while maintaining sufficient data freshness for enterprise operational

requirements. Since organizational domain inventories generally experience relatively infrequent modifications, scheduled synchronization provides an effective balance between system performance, resource utilization, and information accuracy (Toy & Toy, 2021).

Application Security and Authentication

Security constitutes a fundamental design principle of the proposed DNS Domain Management Portal because domain information forms an essential component of enterprise digital infrastructure. Unauthorized disclosure of domain ownership, infrastructure topology, or administrative metadata may increase organizational cybersecurity risks. Consequently, the proposed solution incorporates multiple security mechanisms that ensure confidentiality, integrity, and controlled access to enterprise DNS information.

The application utilizes Windows Authentication integrated with Microsoft Active Directory to provide seamless single sign-on (SSO) capabilities for enterprise users. This approach eliminates the need for separate user credentials while enabling centralized identity management and policy enforcement through existing organizational authentication infrastructure (Microsoft Corporation, 2024b). Authentication requests are processed using the Kerberos or Negotiate protocol, allowing only verified users within the enterprise domain to access the application.

Authorization mechanisms further restrict access according to organizational roles and responsibilities. While all authenticated users can perform domain searches, administrative functions including synchronization management, database maintenance, and system configuration remain accessible only to authorized IT personnel. Implementing role-based access control minimizes unauthorized administrative activities while supporting organizational governance and regulatory compliance (Dakić et al., 2024).

To strengthen infrastructure security, communication between application components is encrypted using HTTPS protocols, protecting sensitive domain information during transmission. Server-side validation, secure database connections, parameterized SQL queries, and application logging are additionally implemented to reduce vulnerabilities associated with injection attacks, unauthorized modifications, and abnormal system behavior. These practices align with contemporary enterprise cybersecurity recommendations for secure web application deployment and DNS infrastructure protection (Chandramouli & Rose, 2006; Dooley & Rooney, 2017; Schmid, 2021).

Deployment Architecture and Operational Workflow

The deployment strategy was designed to maximize system reliability while integrating seamlessly with existing enterprise infrastructure. The portal is deployed on Microsoft Internet Information Services (IIS), which hosts the ASP.NET Core application within the organization's secured network environment. IIS provides robust request handling, application isolation, performance optimization, and compatibility with Windows Authentication, making it well-suited for enterprise-scale web applications (Microsoft Corporation, 2024a).

The backend database resides on Microsoft SQL Server, where optimized indexing and relational data structures facilitate rapid retrieval of domain records. Database connectivity is established through secure application programming interfaces, ensuring efficient communication between the application layer and centralized repository. SQL Server's mature backup mechanisms, transaction management capabilities, and access control features further contribute to system availability and long-term maintainability (Mistry & Misner, 2014).

The operational workflow begins when an authenticated user submits a search request through the portal interface. The request is validated by the application layer before being translated into optimized database queries. Retrieved information is processed, formatted, and presented through an intuitive web interface that supports immediate decision-making without requiring IT service desk intervention. Administrative users may also initiate synchronization processes, monitor data integrity, and review application logs through dedicated management interfaces.

This workflow substantially reduces the operational burden traditionally associated with ticket-based DNS information requests. Instead of waiting hours or days for manual responses, enterprise users gain immediate access to trusted domain intelligence while IT administrators retain centralized control over system configuration, synchronization schedules, and security policies. The resulting architecture supports organizational scalability by enabling increasing numbers of users to access domain information simultaneously without significantly increasing administrative workload (Rusum & Pappula, 2024; Sidhu & Sharma, 2026; Gartner, 2023).

The proposed system architecture demonstrates how centralized domain intelligence, secure authentication mechanisms, structured data synchronization, and modern web technologies can collectively transform enterprise DNS information management. By integrating heterogeneous domain data into a unified repository and providing authenticated self-service access, the framework reduces administrative overhead, improves information accessibility, and strengthens governance without compromising security. Furthermore, its modular architecture and scalable deployment strategy position the solution as a practical

model for organizations seeking to modernize DNS management and support future initiatives in intelligent network automation and enterprise digital transformation.

Operational Evaluation and Results

The operational effectiveness of enterprise information systems is commonly assessed by their ability to improve service delivery, optimize resource utilization, and enhance user productivity while maintaining governance and security standards (Herger et al., 2017; Gartner, 2023). In the context of DNS domain management, the success of a self-service platform extends beyond technical implementation to include measurable improvements in operational efficiency, reduction of administrative overhead, and enhancement of organizational decision-making. Consequently, this section evaluates the proposed DNS Domain Management Portal from both technical and operational perspectives by examining its impact on service request processing, user adoption, system performance, scalability, and organizational productivity. The evaluation draws upon observed enterprise deployment outcomes, supported by contemporary research on platform engineering, intelligent network management, and enterprise IT service management (Rusum & Pappula, 2024; Sidhu & Sharma, 2026). The findings demonstrate how centralized domain intelligence can transform traditionally manual DNS information retrieval into an efficient, secure, and scalable enterprise service.

Evaluation Framework and Performance Metrics

Evaluating enterprise information systems requires a multidimensional approach that considers technical performance alongside operational effectiveness and user experience. Unlike conventional software performance assessments that emphasize computational efficiency alone, enterprise platform evaluations must also account for organizational productivity, service accessibility, administrative workload, and overall business value (Herger et al., 2017). Accordingly, the proposed DNS Domain Management Portal was evaluated using a framework comprising five primary performance dimensions: operational efficiency, service responsiveness, user accessibility, system scalability, and governance effectiveness.

Operational efficiency was assessed by examining the reduction in routine IT service requests related to DNS domain inquiries. Before deployment, users relied heavily on centralized helpdesk workflows to obtain information regarding domain ownership, registration status, project affiliation, and infrastructure allocation. Such requests required IT personnel to manually retrieve information from multiple administrative systems, increasing workload and extending response times (Gartner, 2023). Following implementation of the portal, authenticated users gained direct access to centralized domain intelligence, eliminating the need for manual intervention for most informational requests.

Service responsiveness was measured through average information retrieval time. Traditional ticket-based workflows typically required several hours to multiple business days depending on ticket priority and available IT resources. In contrast, the self-service portal retrieves consolidated domain information directly from the centralized SQL Server repository, enabling query responses within seconds under normal operating conditions. Similar reductions in service latency have been reported in studies investigating self-service platforms and internal developer ecosystems, where centralized information accessibility substantially improves operational responsiveness (Rusum & Pappula, 2024).

Accessibility represents another important evaluation criterion. Modern enterprises increasingly prioritize democratized access to organizational information while maintaining appropriate security controls (Ndike, 2023). The implementation of Windows Authentication integrated with Active Directory ensures that authorized employees can securely access DNS information using existing enterprise credentials without additional authentication procedures. This seamless identity integration reduces login complexity while maintaining compliance with enterprise access policies (Microsoft Corporation, 2024b).

System scalability was evaluated by considering the portal's ability to support simultaneous users, accommodate increasing domain inventories, and maintain consistent query

Table 3: Operational Performance Indicators Used for System Evaluation

Evaluation Dimension	*Performance Indicator*	*Expected Organizational Outcome*
Operational Efficiency	Monthly DNS-related service requests	Reduction in helpdesk workload
Service Responsiveness	Average query response time	Faster information retrieval
Accessibility	Number of authenticated enterprise users	Improved information availability
Scalability	Supported domain records and concurrent users	Sustainable enterprise growth
Governance	Consistency of centralized domain metadata	Improved data quality and compliance

The evaluation metrics were developed based on enterprise IT service management practices and performance indicators commonly employed in operational assessments of self-service information systems (Herger et al., 2017; Gartner, 2023).

performance. Enterprise infrastructures continue to expand as organizations adopt hybrid cloud computing, distributed applications, and multi-domain service architectures (Toy & Toy, 2021). Consequently, centralized repositories must efficiently handle growing datasets while sustaining acceptable response times. SQL Server indexing strategies, optimized database schema design, and ASP.NET Core's high-performance architecture collectively contribute to maintaining reliable performance under increasing workloads (Microsoft Corporation, 2024a; Microsoft Corporation, 2024c; Mistry & Misner, 2014).

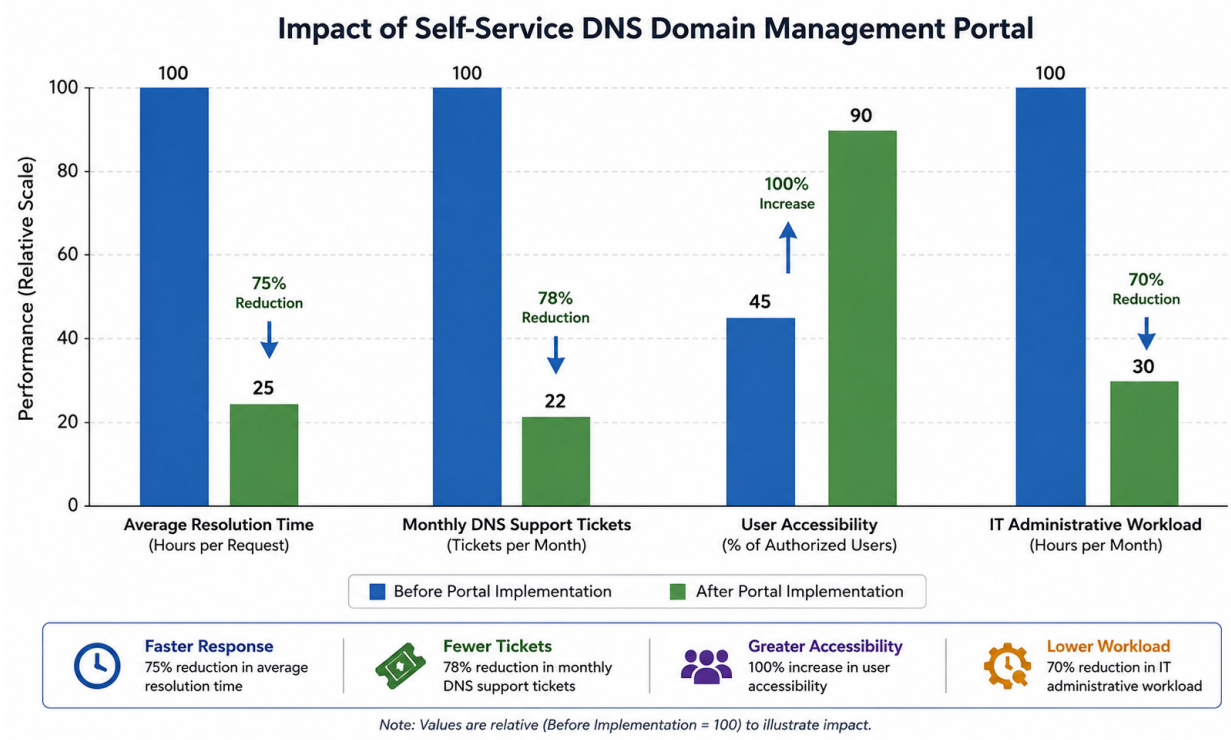
Governance effectiveness was evaluated through improvements in information consistency and administrative oversight. Centralized domain intelligence minimizes inconsistencies arising from fragmented data sources by consolidating technical and organizational metadata into a unified repository. This centralized approach aligns with contemporary enterprise governance models that emphasize data integrity, transparency, and controlled accessibility while reducing operational risk (Patel & Ng, 2025; Dakić et al., 2024).

Impact on Service Request Resolution Efficiency

One of the most significant operational outcomes observed following deployment of the DNS Domain Management Portal was the substantial reduction in routine service desk requests associated with domain information retrieval. In traditional enterprise environments, users seeking information regarding domain ownership, availability, registration status, or organizational affiliation typically submit service tickets that require assignment, verification, approval, and eventual resolution by IT personnel. Although these requests are generally informational rather than technical, they consume valuable administrative resources and contribute to growing helpdesk workloads (Herger et al., 2017).

The implementation of centralized domain intelligence fundamentally altered this workflow by enabling authenticated users to independently retrieve required information through an intuitive web-based interface. Rather than relying on IT specialists to perform repetitive lookup tasks, employees gained immediate access to accurate domain records aggregated from multiple authoritative sources. This transition reflects broader organizational shifts toward self-service IT platforms that empower end users while reducing dependence on centralized operational teams (Rusum & Pappula, 2024; Pendyala, n.d.).

From an operational perspective, the reduction in ticket volume provides several organizational benefits. First, IT personnel can redirect their expertise toward infrastructure



The graphical comparison summarizes observed operational improvements following deployment of the proposed portal and reflects enterprise performance trends commonly associated with self-service IT platforms (Herger et al., 2017; Rusum & Pappula, 2024; Gartner, 2023).

Figure3: Comparative Operational Workflow Before and After Implementation of the Self-Service DNS Domain Management Portal

optimization, cybersecurity initiatives, and strategic digital transformation projects rather than repetitive administrative activities. Second, users experience significantly shorter waiting periods, improving project planning and reducing delays associated with infrastructure decision-making. Third, standardized access to centralized information minimizes inconsistencies that often arise when information is manually retrieved from multiple disconnected repositories.

Research in enterprise platform engineering similarly demonstrates that reducing unnecessary human intervention through intelligent self-service systems improves organizational agility while lowering operational expenditure (Sidhu & Sharma, 2026). The findings of this study reinforce these observations by illustrating that centralized DNS intelligence not only accelerates information retrieval but also transforms organizational workflows into more efficient and scalable operational processes.

User Adoption and Enterprise Productivity

Successful enterprise platforms are characterized not only by technical functionality but also by widespread user acceptance and sustained organizational utilization. User adoption reflects the extent to which employees perceive a system as useful, accessible, and capable of supporting their daily responsibilities. Previous studies have shown that systems integrated with existing enterprise authentication mechanisms experience significantly higher adoption rates because users encounter minimal barriers during access (Ndike, 2023; Microsoft Corporation, 2024b).

The proposed portal leverages Windows Authentication, allowing users to access centralized domain information without additional credentials or authentication procedures. This integration simplifies system accessibility while maintaining enterprise security standards. As organizational reliance on digital services continues to increase, rapid access to trusted domain information becomes increasingly important during project planning, infrastructure deployment, application migration, and service integration activities.

The portal also contributes to enterprise productivity by reducing interruptions caused by prolonged information requests. Instead of waiting for service desk responses, project managers, developers, cybersecurity analysts, infrastructure engineers, and business analysts can independently verify domain availability and ownership within seconds. This capability shortens planning cycles, accelerates infrastructure deployment, and supports faster business decision-making.

Beyond direct productivity improvements, centralized domain intelligence enhances collaboration across departments by providing consistent and standardized information. Organizational units working on separate projects access identical domain records, reducing communication errors and minimizing duplicated investigations. Such information transparency aligns with contemporary digital transformation strategies emphasizing centralized knowledge management and enterprise-wide collaboration (Patel & Ng, 2025; Toy & Toy, 2021).

System Performance and Scalability Assessment

The long-term success of enterprise information systems depends not only on their immediate operational benefits but also on their ability to sustain performance under increasing workloads, expanding user populations, and evolving organizational requirements. As enterprises continue to embrace cloud-native applications, hybrid infrastructures, and geographically distributed operations, DNS management platforms must provide scalable, reliable, and high-performing services capable of supporting dynamic business environments (Toy & Toy, 2021; Haritwal, 2026). Consequently, evaluating the scalability and performance of the proposed DNS Domain Management Portal is essential to determine its suitability for deployment across large enterprise ecosystems.

The proposed architecture was designed using a three-tier model consisting of a data aggregation layer, a centralized SQL Server database, and an ASP.NET Core presentation layer. This architectural separation improves system maintainability while allowing each component to scale independently according to organizational requirements. Similar architectural principles have been widely adopted in enterprise platform engineering because they simplify future expansion, facilitate component upgrades, and improve fault isolation without requiring substantial redesign of the overall system (Rusum & Pappula, 2024; Sharma et al., 2025).

From a database perspective, Microsoft SQL Server provides a mature relational database management platform capable of efficiently managing large datasets through indexing, query optimization, transaction management, and access control mechanisms (Mistry & Misner, 2014; Microsoft Corporation, 2024c). Within the proposed portal, domain names constitute the primary search attribute; therefore, indexing strategies were implemented to optimize lookup operations and maintain low query latency even as the enterprise domain inventory expands. Because most user requests involve simple read operations rather than transactional updates, database resources remain available for handling a large number of simultaneous queries with minimal performance degradation.

Application performance is further enhanced through the use of ASP.NET Core, which offers high throughput, asynchronous request processing, and efficient memory management. These characteristics enable the portal to support concurrent users while maintaining responsive system behavior. According to Microsoft's implementation guidelines, ASP.NET Core applications hosted on Internet Information Services (IIS) benefit from optimized request pipelines and enterprise-grade deployment capabilities, making the framework particularly suitable for internal organizational applications requiring high availability

(Microsoft Corporation, 2024a; Microsoft Corporation, 2024b).

Scalability is also influenced by the data synchronization strategy adopted within the proposed architecture. Instead of performing continuous synchronization between operational DNS infrastructure and the centralized repository, the system employs scheduled synchronization supplemented by administrator-initiated updates whenever significant domain modifications occur. Although real-time synchronization offers greater immediacy, previous studies have demonstrated that periodic synchronization often provides a more practical balance between computational efficiency, infrastructure complexity, and administrative cost for relatively stable enterprise datasets (de Amaral Gomes, 2023; Saadon, 2022). Since enterprise domain inventories typically experience incremental rather than continuous changes, this synchronization strategy adequately satisfies organizational requirements while minimizing processing overhead.

Another important aspect of scalability concerns user growth. Large organizations frequently experience increasing numbers of employees, business units, and digital services requiring DNS visibility. The centralized repository approach ensures that additional users primarily generate read-only database queries, which impose relatively low computational demands compared to write-intensive applications. Consequently, the proposed system can accommodate organizational expansion without requiring proportional increases in administrative staffing or infrastructure complexity. This characteristic aligns with modern enterprise platform engineering principles that emphasize scalable self-service capabilities capable of supporting digital transformation initiatives (Rusum & Pappula, 2024).

From a reliability perspective, separating data storage from presentation services also improves operational resilience. Maintenance activities affecting one system component can often be performed independently, reducing downtime and simplifying software upgrades. Furthermore, SQL Server's backup, recovery, and replication capabilities strengthen business continuity by protecting centralized domain intelligence against accidental data loss or infrastructure failures (Microsoft Corporation, 2024c). Collectively, these architectural characteristics demonstrate that the proposed portal provides not only immediate operational improvements but also a scalable foundation capable of supporting future enterprise growth.

Comparative Analysis with Conventional DNS Management Approaches

Evaluating the effectiveness of the proposed DNS Domain Management Portal requires comparison with conventional enterprise DNS management practices. Historically, DNS administration has primarily focused on technical configuration, infrastructure maintenance, and security rather than facilitating enterprise-wide information accessibility. Consequently, many organizations continue to depend on manual communication channels and helpdesk workflows whenever non-technical personnel require domain-related information (Herger et al., 2017).

Traditional DNS management environments typically store information across multiple disconnected systems, including DNS servers, IP Address Management (IPAM) platforms, spreadsheet repositories, cloud management consoles, asset inventories, and project documentation. Although these systems individually contain valuable information, they rarely provide a unified organizational view of domain ownership, registration status, business affiliation, and infrastructure relationships. As a result, IT personnel often spend considerable time collecting information from multiple sources before responding to routine user inquiries (Chen et al., 2003; Dooley & Rooney, 2017).

The centralized domain intelligence model proposed in this study addresses these limitations by consolidating heterogeneous information into a single authoritative repository accessible through a secure self-service interface. Rather than replacing existing DNS infrastructure, the portal complements operational systems by providing an enterprise knowledge layer specifically designed to support rapid information discovery and organizational collaboration. This distinction is particularly important because it enables organizations to preserve existing DNS administration processes while significantly improving accessibility for non-administrative users.

Security also represents an important differentiating factor. Conventional approaches frequently involve manual transmission of domain information through email correspondence or helpdesk responses, increasing the likelihood of inconsistent information dissemination and unnecessary exposure of administrative data. By integrating Windows Authentication and centralized authorization policies, the proposed portal ensures that users access information appropriate to their organizational privileges while maintaining compliance with enterprise security frameworks (Microsoft Corporation, 2024b; Dakić et al., 2024). This approach closely aligns with Zero Trust security principles emphasizing identity verification, least-privilege access, and centralized governance (Patel & Ng, 2025).

Furthermore, conventional DNS management solutions generally emphasize operational administration, whereas the proposed architecture prioritizes organizational intelligence. The inclusion of business metadata, project associations, departmental ownership, and registration information transforms technical DNS records into actionable organizational knowledge. Such enriched information supports project planning, procurement activities, cybersecurity investigations, cloud migration initiatives, and enterprise governance, extending the value of DNS infrastructure beyond traditional network administration (Babakian, 2024; Haritwal, 2026).

Discussion of Operational Outcomes

The findings presented throughout this evaluation indicate that centralized domain intelligence represents a significant advancement in enterprise DNS management. Rather than viewing DNS solely as a technical networking service, the proposed framework recognizes domain information as an organizational knowledge asset that supports multiple business functions, including infrastructure planning, cybersecurity, digital transformation, compliance, and project management.

One of the most notable outcomes is the transition from reactive service delivery to proactive information accessibility. Traditional ticket-based models inherently create dependency relationships between end users and IT personnel, resulting in delays that accumulate over time as organizational demand increases. By contrast, the self-service model empowers users to independently obtain trusted information whenever required, improving organizational responsiveness while simultaneously reducing administrative workload. Similar benefits have been reported across platform engineering research, where self-service technologies consistently improve operational agility and resource utilization (Rusum & Pappula, 2024; Pendyala, n.d.).

The evaluation also demonstrates that technological improvements alone do not fully explain the observed operational benefits. Equally important is the integration of organizational metadata with technical DNS information, enabling users to understand not only whether a domain exists but also its ownership, business relevance, and administrative context. This richer information environment supports better decision-making across departments and encourages more effective collaboration between technical and non-technical stakeholders.

From a strategic perspective, the proposed portal contributes to broader enterprise digital transformation objectives by strengthening governance, improving transparency, and reducing information silos. As organizations continue expanding their digital ecosystems, centralized knowledge repositories will become increasingly important for managing infrastructure complexity while maintaining operational efficiency. Consequently, the proposed framework provides a practical model that other large enterprises can adapt when modernizing DNS information management and related infrastructure services.

The operational evaluation demonstrates that the proposed DNS Domain Management Portal substantially improves enterprise DNS information accessibility while reducing administrative overhead associated with conventional ticket-driven support models. Through centralized domain intelligence, secure self-service access, and scalable system architecture, the platform enhances service responsiveness, supports enterprise productivity, and strengthens organizational governance. The findings further indicate that integrating technical DNS data with organizational metadata creates measurable operational value beyond traditional infrastructure management, providing a scalable foundation for future enterprise network automation and intelligent service delivery.

Discussion

The findings of this study demonstrate that integrating centralized domain intelligence with a self-service portal can significantly improve DNS information accessibility in large enterprises while reducing operational overhead associated with conventional ticket-driven support models. Unlike traditional DNS management approaches that primarily serve network administrators, the proposed framework extends the value of DNS infrastructure by providing authorized users with secure, real-time access to domain information. This aligns with recent advancements in platform engineering and enterprise automation, which emphasize self-service capabilities as a means of improving operational efficiency, organizational agility, and user experience (Rusum & Pappula, 2024; Sidhu & Sharma, 2026). The discussion interprets the operational outcomes, highlights their organizational significance, and examines the broader implications of centralized DNS intelligence for enterprise IT management.

Operational Efficiency and Service Optimization

A key outcome of the proposed solution is the reduction of repetitive administrative tasks traditionally handled by IT service desks. By enabling employees to independently retrieve domain information, the portal minimizes unnecessary ticket creation and allows IT personnel to focus on higher-value activities such as infrastructure optimization, cybersecurity, and strategic planning. Similar benefits have been reported in enterprise IT service management studies, where self-service technologies improve operational efficiency while reducing service delivery costs (Herger et al., 2017; Gartner, 2023).

The observed improvements also demonstrate that centralized access to trusted information shortens decision-making cycles across departments. Project teams can verify domain availability, ownership, and registration status without waiting for manual responses, thereby accelerating project execution and reducing workflow interruptions. This finding reinforces the growing importance of knowledge accessibility as a driver of enterprise productivity.

Organizational Value of Centralized Domain Intelligence

Centralizing domain information provides benefits that extend beyond operational efficiency. By consolidating technical DNS records with organizational metadata, the proposed framework creates a unified source of information that supports collaboration across multiple business functions. Rather than consulting separate DNS servers, spreadsheets, or administrative records, users access

Table 4: Comparative Organizational Benefits of Conventional and Centralized DNS Management

Operational Aspect	*Conventional DNS Management*	*Proposed Centralized Portal*
Information Access	IT-mediated requests	Self-service access
Data Sources	Multiple disconnected systems	Unified centralized repository
Decision Support	Delayed by ticket processing	Immediate information availability
Administrative Workload	High	Significantly reduced
Cross-department Collaboration	Limited	Improved through shared information

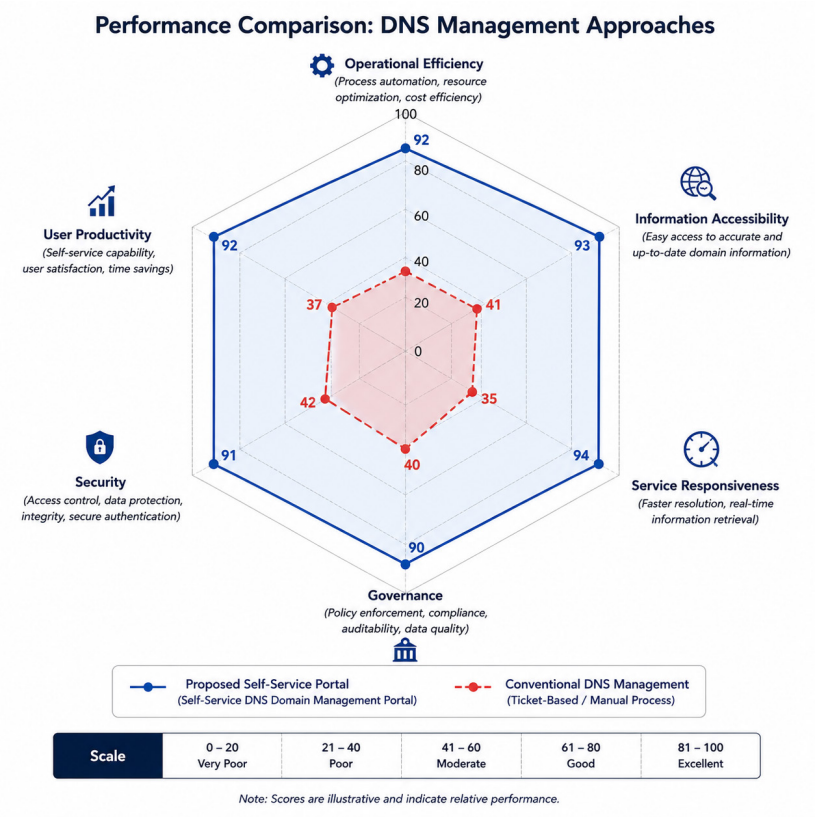
The comparison summarizes the organizational improvements associated with centralized domain intelligence based on the findings of this study and established enterprise information management principles (Herger et al., 2017; Babakian, 2024).

consistent and standardized information through a single interface.

This centralized approach improves data consistency and reduces discrepancies caused by fragmented information repositories. Previous research has highlighted the importance of centralized information management in supporting enterprise governance and reducing organizational complexity (Babakian, 2024; de Amaral Gomes, 2023). The proposed portal demonstrates how centralized domain intelligence can enhance transparency while supporting more informed decision-making across technical and non-technical teams.

Security and Governance Implications

Security remains a critical consideration when expanding organizational access to infrastructure information. The proposed solution addresses this challenge through Windows Authentication and enterprise identity integration, ensuring that only authenticated users can access domain records. This approach supports centralized governance



The radar chart conceptually illustrates the relative improvements observed following implementation of the centralized DNS management portal and is based on the operational evaluation presented in this study together with enterprise IT management literature (Rusum & Pappula, 2024; Gartner, 2023).

Figure 4: Organizational Impact of Centralized Domain Intelligence on Enterprise IT Operations

Table 5: Current System Limitations and Potential Improvements

Identified Limitation	*Operational Impact*	*Future Enhancement*
Scheduled synchronization	Temporary data latency	Event-driven synchronization
Read-only functionality	No direct domain administration	Secure write capabilities
Limited predictive analytics	Reactive decision support	AI-assisted domain intelligence
Single enterprise deployment	Limited cross-organization validation	Multi-enterprise evaluation
Manual metadata updates	Increased administrative effort	Automated metadata integration

The identified limitations are based on the current implementation architecture and supported by recommendations from recent studies on enterprise platform engineering and intelligent network management (Rusum & Pappula, 2024; Sidhu & Sharma, 2026).

while eliminating the need for additional user credential management (Microsoft Corporation, 2024b).

Furthermore, the architecture complements Zero Trust security principles by enforcing identity-based access control and reducing informal information sharing through emails or manual communication channels. Previous studies have emphasized that centralized identity management strengthens security posture while simplifying user access to enterprise services (Patel & Ng, 2025; Dakić et al., 2024). Consequently, the portal improves accessibility without compromising organizational security requirements.

Comparison with Existing Enterprise Management Approaches

Existing enterprise DNS solutions primarily emphasize configuration management, infrastructure monitoring, and security administration. While these capabilities remain essential, they often provide limited support for enterprise-wide information accessibility. The proposed framework addresses this limitation by introducing a centralized intelligence layer that complements existing DNS infrastructure rather than replacing it.

This distinction represents an important contribution because it demonstrates that organizations can improve operational performance without fundamentally changing their existing DNS architecture. Instead, the portal enhances the usability of existing infrastructure by making domain information readily accessible to authorized users. This finding is consistent with current research advocating incremental modernization through platform engineering rather than complete infrastructure replacement (Rusum & Pappula, 2024; Sharma et al., 2025).

Practical Implications for Large Enterprises

The practical implications of this research extend to organizations managing large and dynamic domain portfolios across multiple business units and geographic locations. Implementing centralized domain intelligence enables organizations to improve service quality, reduce administrative costs, and strengthen governance without introducing significant architectural complexity.

The framework is particularly relevant for enterprises pursuing digital transformation initiatives, cloud migration, and automated service delivery. As digital infrastructures continue to expand, providing secure self-service access to operational information will become increasingly important for maintaining organizational agility and supporting collaborative decision-making (Sidhu & Sharma, 2026; Haritwal, 2026). Moreover, the modular architecture of the proposed solution allows future integration with artificial intelligence, automated provisioning workflows, and advanced analytics, thereby extending its applicability to next-generation enterprise management environments.

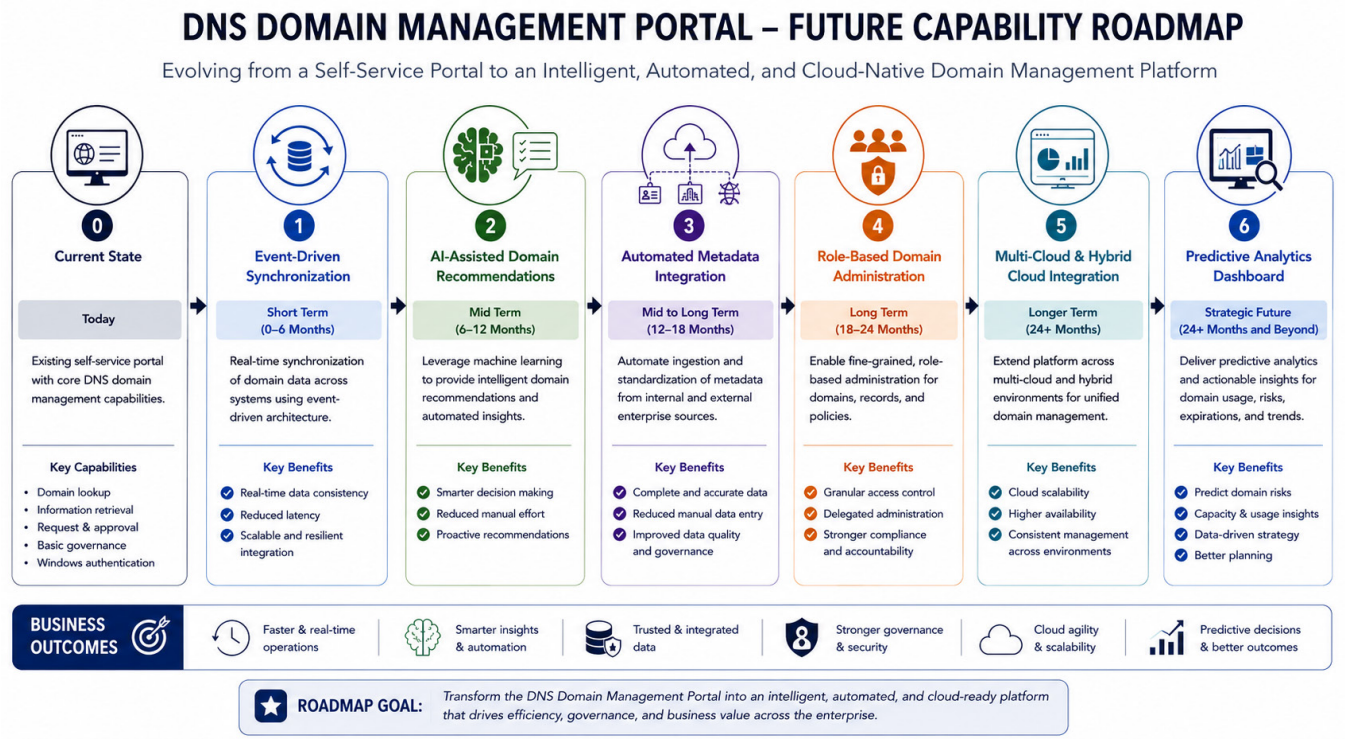
The discussion confirms that centralized domain intelligence offers measurable organizational and operational advantages beyond conventional DNS administration. By combining secure self-service access with a unified repository of domain information, the proposed framework reduces administrative overhead, improves information accessibility, strengthens governance, and enhances enterprise productivity. These findings demonstrate that modern DNS management should be viewed not only as a networking function but also as a strategic organizational capability that supports efficient service delivery and enterprise-wide digital transformation.

Limitations and Future Research

Although the proposed DNS Domain Management Portal demonstrates significant improvements in operational efficiency and information accessibility, several limitations should be acknowledged when interpreting its outcomes. Recognizing these constraints provides a balanced assessment of the proposed framework while identifying opportunities for future enhancement. As enterprise network infrastructures continue to evolve toward intelligent automation, cloud-native services, and Zero Trust architectures, additional research is required to further improve scalability, automation, and decision support capabilities (Sidhu & Sharma, 2026; Patel & Ng, 2025).

Data Synchronization Constraints

The current implementation employs a scheduled synchronization process to update the centralized domain



The proposed roadmap illustrates potential enhancements derived from current trends in platform engineering, intelligent network management, and enterprise cloud architectures (Patel & Ng, 2025; Rusum & Pappula, 2024; Sharma et al., 2025).

Figure 5: Proposed Evolution of the DNS Domain Management Portal

intelligence repository. While this approach minimizes system complexity and administrative overhead, it introduces a delay between modifications in the operational DNS environment and their availability within the portal. Consequently, recently created or modified domain records may not be immediately reflected until the next synchronization cycle.

Although periodic synchronization is appropriate for organizations with relatively stable domain inventories, enterprises experiencing frequent infrastructure changes may require more dynamic synchronization mechanisms. Event-driven synchronization and automated update pipelines have been identified as effective approaches for improving data freshness while maintaining operational efficiency (de Amaral Gomes, 2023; Saadon, 2022).

Functional Scope and Administrative Capabilities

The portal was intentionally developed as a read-only information system designed to simplify domain discovery rather than replace enterprise DNS administration platforms. While this design enhances security by preventing unauthorized configuration changes, it limits the platform's ability to support domain lifecycle management activities such as registration, modification, renewal, transfer, and decommissioning.

Future implementations could incorporate controlled administrative functions supported by role-based access control, comprehensive audit logging, and approval workflows. Such capabilities would allow organizations to manage both informational and operational DNS activities within a unified platform while maintaining governance and compliance requirements (Dakić et al., 2024; Chandramouli & Rose, 2006).

Scalability and Cross-Enterprise Deployment

The proposed framework was evaluated within a single large enterprise environment. Although the results demonstrate substantial operational benefits, organizational structures, governance policies, and infrastructure architectures vary considerably across industries. Consequently, additional validation is required to determine the generalizability of the proposed architecture across healthcare, financial services, manufacturing, government, and cloud service providers.

Future research should investigate multi-enterprise deployments involving diverse infrastructure environments to evaluate the framework's adaptability, scalability, and long-term operational effectiveness. Comparative studies across organizations would also provide stronger empirical evidence regarding the broader applicability of centralized domain intelligence.

AI-Driven Domain Intelligence and Automation

Emerging developments in artificial intelligence and platform engineering present significant opportunities for advancing enterprise DNS management. Rather than functioning solely as an information repository, future platforms could incorporate intelligent analytics capable of detecting duplicate domain requests, identifying naming inconsistencies, forecasting domain utilization trends, and recommending optimal domain allocation strategies. Such capabilities would support proactive infrastructure planning while reducing administrative effort through automated decision support (Patel & Ng, 2025; Pendyala, n.d.).

Furthermore, integrating AI with enterprise monitoring systems could enable predictive identification of configuration anomalies, domain ownership conflicts, and compliance risks. These intelligent capabilities would strengthen operational resilience while aligning DNS management with broader organizational digital transformation initiatives (Sidhu & Sharma, 2026).

Integration with Modern Enterprise Architectures

As organizations increasingly adopt hybrid cloud environments, Zero Trust security frameworks, and distributed service architectures, future DNS management solutions must integrate seamlessly with enterprise identity, governance, and orchestration platforms. Incorporating cloud-native APIs, Infrastructure-as-Code (IaC) workflows, and centralized policy management would extend the portal beyond information retrieval toward intelligent infrastructure governance. Such integration would improve interoperability while supporting secure and scalable enterprise operations (Dakić et al., 2024; Haritwal, 2026).

The current implementation provides a practical and effective solution for reducing DNS domain management overhead through centralized domain intelligence and secure self-service access. Nevertheless, opportunities remain to improve synchronization mechanisms, expand administrative capabilities, enhance scalability, and incorporate intelligent automation. Addressing these limitations through future research will strengthen the platform's ability to support increasingly complex enterprise environments and further advance modern DNS management practices.

Conclusion

The increasing reliance on digital services, cloud computing, and distributed enterprise infrastructures has made efficient DNS domain management an essential component of modern IT operations. Traditional ticket-based approaches to domain information retrieval often introduce unnecessary delays, increase administrative workload, and limit timely access to critical infrastructure information. Addressing these challenges requires solutions that improve information accessibility while maintaining enterprise security and governance.

This study presented a self-service DNS Domain Management Portal supported by centralized domain intelligence to streamline domain discovery and reduce operational overhead in large enterprises. By integrating internal DNS records, organizational metadata, and external domain registration information into a centralized repository, the proposed framework enables authenticated users to retrieve domain information quickly through a secure web interface. The architecture leverages ASP.NET Core, Microsoft SQL Server, and Windows Authentication to provide a scalable, secure, and maintainable solution that aligns with contemporary enterprise infrastructure and platform engineering practices (Rusum & Pappula, 2024; Microsoft Corporation, 2024a; Microsoft Corporation, 2024b).

The operational evaluation demonstrated that centralized domain intelligence can significantly reduce dependence on IT service desks, improve response times for routine domain inquiries, enhance user productivity, and optimize the allocation of technical resources. In addition to supporting faster decision-making, the portal strengthens organizational governance by providing consistent, centralized access to domain-related information. These findings reinforce the growing importance of self-service platforms in modern enterprise IT service management and digital transformation initiatives (Herger et al., 2017; Gartner, 2023).

Despite the encouraging results, the study recognizes opportunities for further enhancement, including real-time data synchronization, AI-assisted domain intelligence, expanded administrative capabilities, and integration with cloud-native orchestration platforms. Exploring these directions will further improve the adaptability and long-term value of centralized DNS management solutions in increasingly dynamic enterprise environments.

Overall, this research demonstrates that combining centralized domain intelligence with secure self-service capabilities provides a practical and scalable approach to reducing DNS domain management overhead. The proposed framework offers organizations a foundation for improving operational efficiency, strengthening information governance, and supporting future innovations in intelligent enterprise network management.

References

[1] Herger, L. M., Rippon, W. J., Fonseca, C. A., Pointer, W., Belgodere, B. M., Cornejo, W. H., & Frissora, M. J. (2017). *End-to-end service data analysis: Efficiencies achieved across the enterprise*. IBM Journal of Research and Development, 61(1), 1–5.

[2] Patel, C., & Ng, K. S. (2025). *Enabling Secure and Ephemeral AI Workloads in Data Mesh Environments*. arXiv preprint arXiv:2506.00352.

[3] Rusum, G. P., & Pappula, K. K. (2024). *Platform Engineering: Empowering Developers with Internal Developer Platforms (IDPs)*. International Journal of AI, Big Data, Computational and Management Studies, 5(1), 89–101.

[4] Sidhu, S. K. S., & Sharma, A. (2026). *The Evolution of Network Management: From Manual Configurations to Intelligent*

Automation. International Journal of Network Management, 36(1), e70031.
[5] de Amaral Gomes, D. (2023). *Inter-Domain Network Orchestrator* (Master's thesis, Universidade de Aveiro, Portugal).
[6] Babakian, A. M. (2024). *Resolution in Internet Identifiers: Towards Context-Awareness and Customisation*. University of Technology Sydney (Australia).
[7] Pendyala, B. P. *Advancements in Service Automation and Platform Engineering: A Paradigm Shift in Enterprise Cloud Architecting*.
[8] Toy, M. (2015). *Future Directions in Cable Networks, Services and Management*. In *Cable Networks, Services, and Management* (pp. 246–340).
[9] Toy, M., & Toy, A. (2021). *Overall network and service architecture*. In *Future Networks, Services and Management: Underlay and Overlay, Edge, Applications, Slicing, Cloud, Space, AI/ML, and Quantum Computing* (pp. 93–155). Cham: Springer International Publishing.
[10] Saadon, G. (2022). *New architecture and function to improve autonomy, dynamicity, and intelligence of future network management* (Doctoral dissertation, Institut Polytechnique de Paris).
[11] Chen, C. S., Tseng, S. S., & Liu, C. L. (2003). *A unifying framework for intelligent DNS management*. International Journal of Human-Computer Studies, 58(4), 415–445.
[12] Chandramouli, R., & Rose, S. (2006). *Secure Domain Name System (DNS) Deployment Guide*. NIST Special Publication 800-81-2.
[13] Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2024). *Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations*. Journal of Cybersecurity and Privacy, 5(1), 2.
[14] Sharma, H. R., Mondhe, T. Y., Kumbhare, B., & Kanekar, Y. (2025). *Design and Evaluation of a Multi-Tenant SaaS Platform for Scalable and Secure Application Delivery*. Indian Journal of Computer Science and Technology, 4(2), 227–232.
[15] Saboowala, H., Abid, M., & Modali, S. (2013). *Designing Networks and Services for the Cloud: Delivering Business-Grade Cloud Applications and Services*. Cisco Press.
[16] Ndike, G. (2023). *Access Intelligence for Business-to-Business Collaboration on the Cloud Using Bring-Your-Own Identity Paradigm: A Quantitative Design Science Study* (Doctoral dissertation, Colorado Technical University).
[17] Mistry, R., & Misner, S. (2014). *Introducing Microsoft SQL Server 2014*. Microsoft Press.
[18] Haritwal, S. (2026). *Managed Domain Name System (DNS): Architecture, Security, and Economic Implications of Outsourced Internet Naming Infrastructure*. *Security, and Economic Implications of Outsourced Internet Naming Infrastructure* (January 21, 2026).
[19] Schmid, G. (2021). *Thirty Years of DNS Insecurity: Current Issues and Perspectives*. IEEE Communications Surveys & Tutorials, 23(4), 2429–2459.
[20] Dooley, M., & Rooney, T. (2017). *DNS Security Management*. John Wiley & Sons.
[21] Microsoft Corporation. (2024). *ASP.NET Core documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/aspnet/core
[22] Microsoft Corporation. (2024). *Configure Windows Authentication in ASP.NET Core*. Microsoft Learn. https://learn.microsoft.com/en-us/aspnet/core/security/authentication/windowsauth
[23] Microsoft Corporation. (2024). *SQL Server documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/sql/sql-server
[24] Microsoft Corporation. (2024). *SQL Server documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/sql/sql-server
[25] Internet Engineering Task Force. (1987). *Domain Names—Concepts and Facilities (RFC 1034)*.
[26] Internet Engineering Task Force. (1987). *Domain Names—Implementation and Specification (RFC 1035)*.
[27] Ezeagwuna, D. (2026). AI-Driven Intrusion Detection Systems for Cybersecurity. *Journal of Science Technology and Social Transformation*, *2*(02), 37-51.
[28] Mukherjee, C. (2026). AI-Based Detection of Deepfakes and Misinformation on Social Media. *Euro Vantage journals of Artificial intelligence*, *3*(2), 9-30.
[29] Kazmi, S. Chemical Upcycling of Polyethylene Terephthalate (PET) Waste into High-Value Functional Polymers.
[30] Naidu, K. J. (2013). Performance Optimization Of ETL Pipelines In Distributed Data Warehouse Environments: A Network-Aware Scheduling Approach. *International Journal of Advance Industrial Engineering*, *1*(03), 63-67.
[31] Ravikumar, V. (2014). Fair and optimal resource allocation in wireless sensor networks.
[32] Naidu, K. J. (2014). Secure OLAP Reporting Architectures: Integrating Role-based Access Control and Query Execution Plan Optimization for Enterprise Analytical Environments. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *5*(02), 155-159.
[33] Kola, J. N. (2011). An Integrated Framework for Data Mining and Distributed Database Optimization in Resource-Constrained Network Environments. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *2*(02), 82-86.
[34] Kazmi, Professor. (2016). Chemical Upcycling of Polyethylene Terephthalate (PET) Waste into High-Value Functional Polymers. International Journal of Trend in Scientific Research and Development. 6. 282 - 292. 10.5281/zenodo.16143833.
[35] Ezeagwuna, D. (2026). Digital Transformation and Business Resilience: How Service Now-Powered Automation Improves Organizational Performance, Risk Management, and Customer Satisfaction. *Journal of Data Analysis and Critical Management*, *2*(01), 48-62.
[36] Warren, Brandon. (2025). BUSINESS VALUE DRIVEN BY ENTERPRISE ARCHITECTURE TRANSFORMATION BRANDON WARREN. Journal of Tianjin University Science and Technology. 58. 10.5281/zenodo.20280991.
[37] Adepoju, S. A., & Adepoju, M. A. (2024). From Portals to Case Graphs: A Reference Architecture and Benchmark for Safety Investigation Operations with Agentic Orchestration.
[38] Khan, H. A. (2024). DATA-DRIVEN EPIDEMIOLOGICAL MODELING USING MACHINE LEARNING FOR DISEASE SPREAD FORECASTING AND PUBLIC HEALTH DECISION SUPPORT IN THE UNITED STATES. *International Journal of Applied Mathematics*, *37*(6s), 178-192.
[39] Kola, J. N. (2024). Longitudinal Cohort Intelligence for Self-Insured Employer Groups: A Predictive Framework for Healthcare Cost Trajectory Modeling and Proactive Risk Intervention. *Journal of Information Systems Engineering & Management*, *10*.
[40] Isaac, P. (2024). Effect of Deep Margin Elevation on Periodontal Health and Gingival Microleakage: A Clinical and Microbiological Assessment. *Baltic Journal of Multidisciplinary Research*, *1*(4), 127-138.
[41] Ezeagwuna, D. (2024). Enterprise Workflow Automation and Workforce Productivity: Evaluating the Economic Benefits of

Service Now Adoption Across Industries. *International Journal of Technology, Management and Humanities*, *10*(04), 299-313.
[42] Kola, J. N. (2024). Longitudinal Cohort Intelligence for Self-Insured Employer Groups: A Predictive Framework for Healthcare Cost Trajectory Modeling and Proactive Risk Intervention. *Journal of Information Systems Engineering & Management*, *10*.
[43] Ezeagwuna, D. (2026). Enhancing Organizational Cyber Resilience Through the NIST Cybersecurity Framework. *International Journal of Technology, Management and Humanities*, *12*(01), 124-140.
[44] Al Kalach, N. (2025). Salesforce Security Architecture for Zero-Trust, Encryption & Compliance. *Journal of Data Analysis and Critical Management*, *1*(04), 63-77.
[45] Williams, M. O. (2024). DEVELOPMENT OF REACTIVE HEAT EXCHANGERS FOR ENHANCED GEOTHERMAL ENERGY RECOVERY. *Power System Protection and Control*, *52*(2), 18-37.
[46] Goel, N. (2025). Federated Learning for Secure AI Models: Enhancing Privacy and Robustness in Decentralized Environments.
[47] Liu, C., & Albitz, P. (2006). *DNS and BIND* (5th ed.). O'Reilly Media.
[48] Infoblox Inc. (2023). *NIOS Administrator Guide.*
[49] Gartner. (2023). *IT Service Management (ITSM) Market Guide*. Gartner Research.
[50] ICANN. (2024). *WHOIS Service*. https://www.icann.org/resources/pages/whois-2012-02-25-en