engineering proceedings

MDPI

Proceeding Paper

Website Cluster Management Platform: Core Technology Design and Application †

Ji Yun *, Lingfeng Kong and Xiaofang Hua

Information Center, Changzhou College of Information Technology, Changzhou 213164, China; konglingfeng@czcit.edu.cn (L.K.); huaxiaofang@czcit.edu.cn (X.H.)

* Correspondence: jiyun@czcit.edu.cn

† Presented at the 9th Eurasian Conference on Educational Innovation 2026 (ECEI 2026), Da Nang City, Vietnam, 30 January–2 February 2026.

Abstract

To address the challenges of decentralized architecture, inconsistent standards, and inadequate security in multi-organizational website cluster construction, we developed an integrated management platform incorporating unified authentication, parameterized templates, multi-layer security protection, and intelligent governance mechanisms. Implementation results demonstrate over 95% improvement in site construction efficiency and a significant reduction in operational costs, providing robust support for digital transformation in educational institutions and government departments.

Keywords: website cluster management; modular design; content governance; security protection; digital governance

1. Introduction

With the continuous advancement of digital governance, website clusters under distributed management models across multiple organizations and departments have become crucial information carriers for educational institutions, government agencies, and enterprises. However, traditional website construction commonly suffers from loose architecture, inefficient content governance, and weak security protection [1], leading to increased system maintenance costs, fluctuating content quality, and low resource utilization rates, which hinder the sustainable development of organizational digital capabilities.

From the research perspective, domestic and international studies have yielded substantial results in single-site content management, web security protection, and template reuse. However, research on website cluster platforms involving multiple entities, cross-departmental coordination, and multi-role collaboration remains relatively insufficient. Existing systems lack systematic technical approaches in unified identity and permission control, multi-layer security protection, and full-chain content governance, making it difficult to meet organizational needs for unified management, risk control, and efficient construction at large-scale site cluster levels.

Taking a website cluster construction practice as the research object, we explored architectural design, template systems, permission and security technologies, content governance mechanisms, and intelligent operation and maintenance strategies, proposing a website cluster management platform solution applicable to multi-organizational scenarios. Through an integrated approach of unified architecture, modular collaboration, intelligent governance, and automated deployment, the solution achieves significant improvements

Check for updates

Academic Editors: Teen-Hang Meen, Chun-Yen Chang and Cheng-Fu Yang

Published: 4 June 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

in site construction efficiency, content quality optimization, enhanced security performance, and reduced maintenance costs.

2. System Architecture

To address the shortcomings of traditional website clusters in terms of decentralized architecture, independent resources, and complex operations, this research adopts a four-layer progressive architecture model consisting of an infrastructure layer, data layer, application layer, and presentation layer [2]. This structure achieves layer-by-layer separation from bottom-layer resource management to upper-layer business presentation through interfaces, protocols, and modular mechanisms, realizing system scalability, stability, and maintainability, providing a unified technical foundation for intensive site management in multi-organizational scenarios.

2.1. System Overall Architecture

The platform adopts a layered decoupling approach, dividing site operation resources, data, business logic, and user interaction into independent structural levels. Each layer maintains logical autonomy while achieving collaborative operation through a unified service framework, forming an architectural pattern that combines centralized management with independent expansion, as shown in Figure 1.

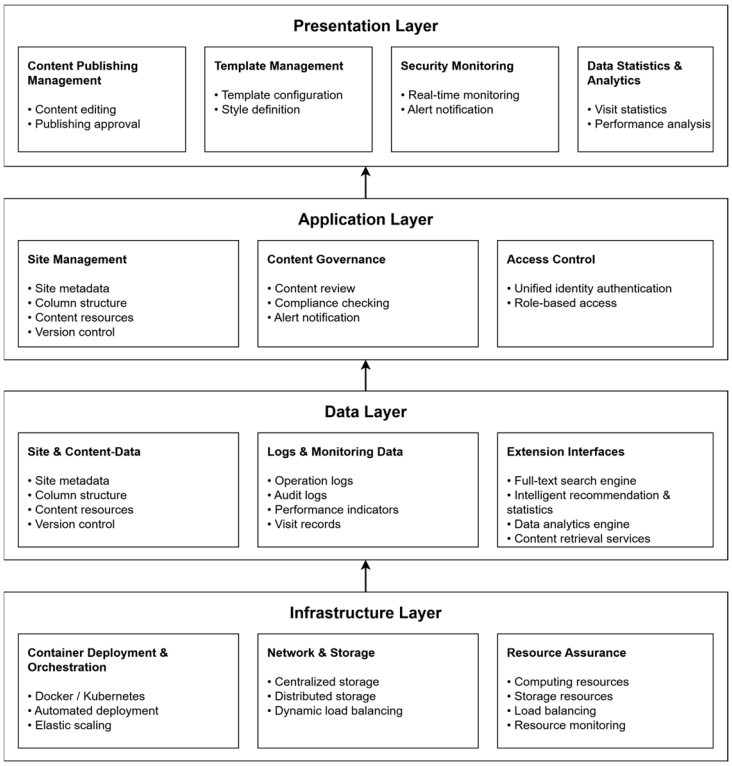


Figure 1. System architecture developed in this study.

2.1.1. Infrastructure Layer

The infrastructure layer conducts bottom-layer environment setup and resource scheduling tasks for platform operation. By introducing containerized deployment methods, the operating environment undergoes standardized processing, ensuring consistent performance when sites migrate or expand across different nodes. Simultaneously, combining virtualization technology with automatic scheduling strategies, computing and storage resources are centrally managed and dynamically allocated, enabling timely band-

width and computing power expansion during traffic fluctuations or task peaks, avoiding performance bottlenecks.

2.1.2. Data Layer

The data layer is responsible for unified management of various platform data, including structured content, resource files, and log records. The system adopts relational databases as the primary storage method and configures caching, indexing, and database sharding strategies according to site access characteristics to improve query and retrieval efficiency. Through primary–secondary system synchronization, snapshot backup, and regular archiving measures, the data layer ensures data security, enabling rapid backtracking and recovery during unexpected failures or human errors.

2.1.3. Application Layer

The application layer is responsible for the business logic of the system, including modules for site management, content governance, permission control, template configuration, and monitoring functions. The platform adopts modular decomposition and unified interface mechanisms, enabling each module to have relatively independent evolution capabilities while reducing cross-module coupling.

2.1.4. Presentation Layer

The presentation layer has different role users as the platform's direct interaction interface. The system integrates functions such as content publishing, template management, security monitoring, and statistical analysis into a unified portal, enhancing user experience across different terminals through visual layout and responsive design.

2.2. Components and Functional Division

Based on the four-layer architecture, six major subsystems are constructed at the application layer: site management, content management, permission control, workflow approval, monitoring logs, and statistical analysis.

2.2.1. Site Management Subsystem

The site management module is responsible for the entire lifecycle process of site creation, initialization, configuration, and launch. With template cloning and automated deployment mechanisms as the core, the system enables new sites to complete environment construction, structure initialization, and basic configuration within minutes.

2.2.2. Permission Management Subsystem

The permission system is built based on the Role-Based Access Control (RBAC) model, achieving refined management through multi-layer mapping among users, roles, and permissions. The system can precisely subdivide permissions to menus, buttons, and data ranges.

2.2.3. Workflow Approval Subsystem

The workflow approval module is built based on a configurable workflow engine, enabling complex process configurations such as multi-level approval, joint signature, and additional signature through visual methods.

2.2.4. Monitoring and Log Subsystem

The monitoring and log module integrates operational monitoring and operation recording functions, collecting real-time data on resource occupation, traffic volume, ab-

normal traffic, and sensitive operations, and identifying potential risks through intelligent analysis modules.

2.2.5. Statistical Analysis Subsystem

The statistical analysis module focuses on data such as access scale, activity level, column usage, and content publishing. The system provides multiple chart types and report templates, helping managers comprehensively understand the overall performance of the website cluster.

3. Technology Implementation

Multi-site parallel operation of website clusters presents high complexity in identity management, permission control, content governance, security protection, and operational monitoring. Therefore, this platform designs and implements around five core modules: unified authentication, template and site construction system, multi-layer security architecture, content governance mechanism, and intelligent operation and maintenance technology, forming a reusable and transferable technical path, as shown in Figure 2.

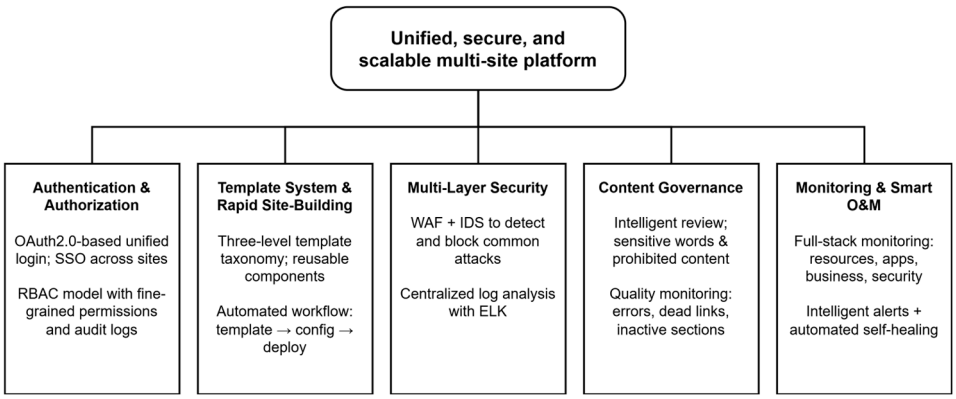


Figure 2. Core Technology modules.

3.1. Unified User Authentication and Permission Control

In website cluster environments with multiple sites and roles participating in parallel, identity management and permission boundaries often become intricately complex. Without a unified authentication system and refined permission control framework, security and management risks such as account fragmentation and permission overreach easily arise.

3.1.1. Unified Identity Authentication Mechanism

In multi-site environments, users often span different departments and roles, and traditional decentralized authentication models easily cause account duplication, permission conflicts, and security risks. Therefore, the platform adopts a unified authentication center based on OAuth2.0 [3], implementing user identity consistency and verifiability across all sites through the authorization code mode. The unified authentication system includes four types of entities: resource owner, client, authorization server, and resource server. Access tokens become unified credentials across sites, enabling users to access multiple site resources after logging in once, improving usage convenience and reducing account management costs.

Additionally, to accommodate existing organizational information systems, the platform reserves Lightweight Directory Access Protocol and Central Authentication Service, and other protocol interfaces, enabling account synchronization with academic affairs, human resources, office automation, and other systems, avoiding identity fragmentation issues from parallel multi-system management.

3.1.2. RBAC Permission Control Model

On the basis of the unified identity system, the platform constructs a permission control model centered on RBAC, achieving multi-layer mapping from users and roles to permissions [4]. Permission granularity can be refined to menus, buttons, and data ranges, making operational boundaries clear for different roles.

For example, department administrators can only access data within their domain, while system administrators can perform auditing and management tasks across all sites. Sensitive operations are all written to a centralized log repository, forming a traceable and auditable management chain, improving overall system controllability.

3.2. Template System and Rapid Site Construction Technology

In scenarios requiring frequent new site creation, without a reusable template system and automated site construction mechanism, issues such as structural differences, inconsistent configurations, and low deployment efficiency easily arise.

3.2.1. Template Classification System Design

The template library constructs a three-level classification system from three dimensions: site type, industry characteristics, and functional requirements. The first level includes general types such as portals, departments, special topics, and activities; the second level subdivides by domains such as education, government, enterprises, and media; the third level further distinguishes by display, interactive, and application function types. The hierarchical classification method enables templates to form reusable groups in visual style, layout structure, and functional components, facilitating rapid selection of appropriate templates for different organizations.

3.2.2. Template Parameterization and Structure Decoupling

To avoid excessive template rigidity, the platform abstracts all visual, structural, and functional elements as parameter items. For example, theme color, font, icons, header-footer layout, column arrangement, field types, and component switches (such as search, comments) are all recorded in the JavaScript Object Notation format and support batch import, historical recovery, and version management. Parameterized design enables a single template to derive multiple adapted forms, improving reuse rates and enhancing template flexibility.

3.2.3. Automated Site Construction Process

The site construction process is implemented based on an automated workflow, including template selection, parameter injection, resource replication, database initialization, permission configuration, and launch publishing. The system allocates independent resource directories for each site and completes service registration and access path generation through deployment scripts, reducing site construction time from traditional day-long cycles to minute-level, significantly improving construction efficiency.

3.3. Multi-Layer Security Protection System

Facing continuously evolving network security threats, relying solely on single security components makes it difficult to achieve effective protection. The platform constructs a multi-layer defense-in-depth security system consisting of the Web Application Firewall (WAF), Intrusion Detection System (IDS), log audit platform, and behavior analysis models.

3.3.1. WAF

The platform deploys ModSecurity-based WAF [5], performing real-time interception of common attacks such as Structured Query Language (SQL) injection, Cross-Site

Scripting (XSS), and Cross-Site Request Forgery. Recognition logic combines rule matching with behavior analysis, enabling the system to identify both known patterns and capture abnormal behaviors, improving detection accuracy.

3.3.2. IDS

The network layer adopts Suricata-based IDS [6], detecting traffic patterns, port behaviors, and potential attack chains. The system integrates signature recognition with machine learning models, enabling the identification of covert behaviors such as Distributed Denial of Service attacks and port scanning, further enhancing security resilience.

3.3.3. Security Log and Centralized Analysis Mechanism

The platform constructs a security log centralized analysis architecture based on Elasticsearch, Logstash, Kibana (ELK, version 9.2.3) [7], collecting system logs, operation logs, and security events, forming traceable evidence chains through visual analysis, trend judgment, and correlation analysis, providing a basis for security handling and audit supervision.

3.4. Unified Content Governance Technology

When multiple departments and roles participate in content production, without unified governance mechanisms, issues such as content quality fluctuation, approval gaps, and structural inconsistencies easily arise. This platform constructs a collaborative mechanism between automatic review and manual review, forming a complete content governance chain.

3.4.1. Intelligent Content Review Model

The intelligent review module is based on natural language processing algorithms, mainly including sensitive word identification and prohibited content recognition [8]. Sensitive word identification supports evasion methods such as homophone replacement and character deformation; prohibited content recognition relies on deep learning models to classify and judge content related to politics, violence, and inappropriateness. Automatic review and manual review form a complementary relationship, balancing efficiency and quality.

3.4.2. Content Quality Monitoring Mechanism

The platform constructs mechanisms such as quality inspection, dead link detection, and content update monitoring. The quality detection module identifies issues such as typos, grammatical anomalies, and structural inappropriateness. Dead link detection regularly scans link structures across all sites and updates monitoring to identify columns that have not been updated for extended periods, avoiding zombie columns. Multiple mechanisms work together to improve the overall health of the content ecosystem.

3.5. Site Monitoring and Intelligent Operation Technology

To ensure long-term stable platform operation, the system constructs a multi-dimensional monitoring system covering resource status, business performance, and security events, reducing operational pressure through intelligent alerting and automated operation mechanisms.

3.5.1. Monitoring System

The platform uses Prometheus to collect hardware indicators such as CPU, memory, disk, and network; the application layer uses distributed tracing technology to analyze business request chains; the business layer monitors access scale and publishing behaviors;

the security layer monitors attack events and sensitive operations. Monitoring data is presented in a unified interface, improving system observability.

3.5.2. Intelligent Alerting Mechanism

The alerting mechanism adopts a rule + prediction dual-channel strategy. Rules set threshold conditions through Domain-Specific Language (such as CPU continuously above 85%); prediction models identify abnormal load trends, providing the warnings of potential failures. Alert aggregation mechanisms can identify event root causes, reducing noise alerts.

3.5.3. Automated Operation Tools

The system supports tools such as batch operations, health checks, automatic self-healing, and log analysis. The fault self-healing mechanism can automatically restart related services or switch nodes when anomalies occur; the operation ticketing system transforms alert events into traceable tasks, forming a closed loop in operational processes.

4. Results

The platform was deployed and applied at the implementation institution, conducting systematic evaluation around dimensions such as construction efficiency, operational costs, security protection, content quality, and system availability. Monitoring results indicate that the platform improved overall construction effectiveness and operational levels in multi-site management scenarios, validating the effectiveness of architectural design and technical routes, as shown in Table 1.

Table 1. Implementation results and their comparison.

Evaluation Indicator	Before Implementation	After Implementation	Improvement
Site construction time	Day-based	3–5 min	>95%
Template reuse rate	<30%	80–85%	+50–55%
Operation capacity (sites/person)	1:10	1:50	5×
Server utilization	40–50%	>70%	+20–30%
Attack recognition rate	<70%	>90%	+20%
Security false-positive rate	>15%	<5%	−10%

4.1. Construction Efficiency Improvement

Relying on the parameterized template system and automated deployment chain, the platform transformed the new site construction process from traditional item-by-item configuration to holistic automated generation. Actual operation data shows that site creation time was reduced from days-based calculation to 3–5 min level, achieving approximately 95% or greater efficiency improvement. Template reuse rate stabilized in the 80–85% range, significantly reducing repetitive development and manual configuration workload.

4.2. Operational Cost Reduction

Intensive resource management and unified monitoring mechanisms significantly increased the number of sites a single operations personnel can manage, with management capacity improving from the traditional model's 1 person ≈ 10 sites to 1 person ≈ 50 sites. Daily inspections, resource expansion, version updates, and other work are completed by automated tools, with manual intervention ratios significantly declining. The unified

resource pool reduced redundant environment deployment between sites, improving server utilization rates and correspondingly reducing hardware costs.

4.3. Enhanced Security Protection Capabilities

Under the collaborative effect of multi-layer protection systems, including WAF, IDS, log analysis, and behavior monitoring, the platform's security protection performance has achieved stable improvement. Recognition and blocking rates for common attacks such as SQL injection and XSS significantly increased, with abnormal behavior recognition accuracy stabilizing around 90%, security false-positive rates controlled within 5%, and overall system security incident trigger frequency showing a downward trend. The multi-layer security system enhanced the platform's defense capabilities against emerging attack methods.

4.4. Content Quality Improvement

Through mechanisms such as intelligent review, dead link detection, and column activity monitoring, the content quality and structural consistency of the website cluster achieved effective improvement. The combination of automatic review and manual review improved review efficiency by 1–2 times, with automatic review pass rates stabilizing in the 70–85% range, effectively reducing manual review pressure. Dead link detection and structural inspection mechanisms maintained the site effective link rates at high levels. Long-term un-updated columns were automatically identified, effectively reducing zombie columns and content gap issues.

4.5. System Operational Response Efficiency Improvement

The platform's observability and intelligent operation capabilities have been significantly enhanced, as shown in Table 2. Fault location time was reduced from traditional manual troubleshooting's hour-level to minute-level, with some resource anomalies automatically recoverable through self-healing mechanisms without manual intervention. The platform's monitoring, alerting, and automated mechanisms formed a closed loop from detection, identification, to handling, providing stable operation guarantees for large-scale website clusters.

Table 2. Key performance indicators.

Performance Indicator	Traditional Model	Platform Model	Performance Improvement
Fault location	Time Hour-level	Minute-level	10–20×
Average recovery time	>2 h	<10 min	12×+
System availability	95–97%	>99%	+2–4%
Concurrent user support	<500	>2000	4×
Average response time	>3 s	<1 s	3×
Link validity rate	70–80%	>95%	+15–25%

5. Conclusions

Addressing common issues in website clusters regarding decentralized architecture, uncoordinated content management, and weak security protection, this research conducted a systematic design from dimensions including architectural system, template mechanism, content governance, security strategy, and operational methods, constructing a management platform oriented toward multi-organizational scenarios. Through technologies such as template reuse, automated site construction, unified governance, and multi-layer

security protection, the platform transformed multi-site construction from a decentralized model to centralized management, with both resource utilization rates and operational efficiency achieving significant improvements.

The main value of this research lies in: proposing a unified architectural model applicable to multiple entity types, including education, government, and enterprises; constructing a technical system covering content, security, and operations; and forming a transferable and scalable construction framework, providing a referenceable path for organizational digital construction.

Although the platform achieved certain results, there remains room for continued improvement in aspects such as intelligent review accuracy, high-concurrency scenario performance optimization, and privacy protection in data flow processes. Future research will further deepen around intelligent recognition, performance optimization, and data security to enhance the platform's adaptability in complex scenarios.

Author Contributions: Conceptualization, J.Y.; methodology, J.Y.; software, L.K.; validation, J.Y. and X.H.; formal analysis, L.K.; investigation, X.H.; resources, J.Y.; data curation, L.K.; writing—original draft preparation, J.Y.; writing—review and editing, L.K. and X.H.; visualization, X.H.; supervision, J.Y.; project administration, J.Y.; funding acquisition, J.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang, L.; Zhang, H.; Zhu, H. Research and Construction of University Website Cluster Security Management System Under New Situations—Taking Jinan University as an Example. *Microcomput. Appl.* **2024**, *40*, 211–214. (In Chinese)
2. Wu, Y.; Wang, T.; Wang, J. Design and Research of University Website Cluster Architecture from All-Media Perspective. *Gansu Keji Zongheng* **2023**, *52*, 1–4+91. (In Chinese)
3. Yang, X.; Liu, W. Research on Mainstream Security Identity Authentication and Authorization Technology OAuth2.0. *Netw. Secur. Technol. Appl.* **2024**, *4*, 9–12. (In Chinese)
4. Lai, T.; Wang, Y.; Luo, P.; Gao, Z. Design and Application Research of Permission Control Model Based on Role Resource Level. *J. Commun.* **2024**, *45*, 153–159. (In Chinese)
5. Wang, H.; Ma, Y.; Wang, C. Research and Improvement of Intrusion Detection Model Based on ModSecurity Firewall. *J. Nankai Univ. (Nat. Sci. Ed.)* **2016**, *49*, 53–57. (In Chinese)
6. You, G.; Xu, L.; Li, M.; Liu, W.; Zhang, P.; Lu, Z. Research on Network Abnormal Traffic Detection Based on Machine Learning and Rules. *Netw. Secur. Data Gov.* **2025**, *44*, 1–9. (In Chinese)
7. Wu, R. Design of a Campus Network Log Platform Based on ELK. *Netw. Secur. Informatiz.* **2025**, *10*, 86–87. (In Chinese)
8. Zhao, L.; Li, Z.; Fan, C.; Li, F.; Yu, D.; Fei, Y. Content Moderation Method Based on Multimodal Large Models. *Comput. Eng. Appl.* 2025, *in press*.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.