MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

V.N. Karazin Kharkiv National University

Faculty of Mathematics and Informatics

Department of Theoretical and Applied Informatics

Master's Qualification Thesis

On the topic The performance and security levels of Web applications using a fuzzy hybrid multi-standard approach

Executed by: _-year student, group MCS-64

specialty 122 «Computer Science»

Educational and research program

«Informatics»

QI FANGSHUAI

(surname and initials)

Supervisor Yurii Parfeniuk

(surname and initials)

Reviewer Dmytro Chumachenko

(surname and initials)

Kharkiv – 2024

Abstract

With the rapid development of information technology, web applications have become a key platform for data collection, storage, and interaction, and their performance and security level are directly related to the stability and security of the entire system. However, there are significant shortcomings in data security risk assessment for current web applications, manifested in the lack of effectiveness of assessment tools and the lack of uniformity in assessment standards. In response to this situation, this study proposes a performance and security level evaluation model for web applications based on fuzzy mixed multi criteria method. This model comprehensively considers multiple dimensions such as data integrity, confidentiality, availability, and compliance. By processing uncertain information through fuzzy logic and combining multiple criteria analysis, it achieves a comprehensive and objective evaluation of web application performance and security levels.

In the experimental verification phase, this study selected multiple actual web applications as evaluation objects, and verified the effectiveness and accuracy of the evaluation model by collecting and analyzing their performance and security related data. The results indicate that the model can not only accurately identify performance and security issues in web applications, but also provide targeted optimization suggestions for organizations, effectively improving data security management efficiency and responsiveness. In addition, this study also explores the potential application of evaluation models in integrating and unifying data security risk assessment standards, providing useful references for promoting consistency and interoperability in the field of data security management.

Keywords: fuzzy mixed multiple criteria method; Web applications; Performance and Security Levels

Table of Contents

1 Introduction

1.1 Research Background

In todays rapid development of information technology, big data has become a key resource to drive enterprise operation and strategic decision-making. With the deepening of digital transformation, the surge of data volume and the diversification of application scenarios not only greatly enrich the dimension of information interaction, but also significantly improve the efficiency of business processing. However, while the value of data is prominent, its security problem is also increasingly prominent, which has become an important obstacle restricting the pace of digital transformation. Frequent data leakage incidents not only lead to huge financial losses, but also cause a serious risk of privacy leakage, posing a serious threat to individual, organizations and even national security. In this context, data security has become a major issue of widespread concern worldwide, and its importance is self-evident.

The promulgation and implementation of the Data Safety Law indicates that data security has been incorporated into the national legal system and has become a basic standard that enterprises must follow. This law clearly defines the important position of data security risk assessment as the basic system of data security, and requires important data processors to fulfill the obligation of data security protection, and to effectively identify, evaluate and control potential data security risks through a scientific risk assessment mechanism. The establishment of this legal framework provides a solid legal foundation and guidance direction for the data security work.

In May 2023, the Network Security Standard Practice Guidelines--Implementation Guidelines for Network Data Security Risk Assessment was

released, which further refined the practice path of data security risk assessment and provided the organization with clear ideas, workflow and content framework for assessment. The guidelines emphasize the key role of risk assessment in preventing data leakage and ensuring data security, pointing out that through systematic assessment, organizations can more fully understand the threat environment they face, and then develop targeted security strategies to effectively respond to data security challenges. However, although the Implementation Guidelines provide an important reference basis for data security risk assessment, they still face many challenges in practical terms. Especially for Web applications, as the core platform of data collection, storage and interaction, its data security performance is directly related to the security level of the whole system. However, at present, many organizations have significant deficiencies in the data security risk assessment of business systems, such as the lack of effectiveness of evaluation tools, the lack of uniformity of evaluation standards, and the complex and long evaluation process. These problems not only affect the accuracy of the risk assessment results, but also restrict the ability of the organization to take effective risk response measures.

In this context, it is particularly important to explore a more efficient and accurate data security risk assessment method. As a comprehensive evaluation method, the advantage of fuzzy mixed multi-standard method is that it can comprehensively consider various factors, process uncertain information through fuzzy logic, and combine with multi-standard analysis, and realize a comprehensive and objective evaluation of complex systems. The application of this method in data security risk assessment is expected to overcome the limitations of existing assessment methods and improve the accuracy and efficiency of the assessment. Specifically, the fuzzy mixed multi-standard method can build an evaluation index system containing

multiple dimensions based on the characteristics of Web applications, such as data integrity, confidentiality, availability, compliance, etc. Through fuzzy processing, this method can more flexibly deal with the uncertain factors in the evaluation process, such as the probability of threat occurrence and the degree of influence, so as to obtain more practical evaluation results. At the same time, combined with multi-standard analysis, this method can comprehensively consider the mutual influence between different indicators, provide a more comprehensive and in-depth evaluation perspective for the organization, and help it to develop more scientific and reasonable risk response strategies.

1.2 Study significance

In the context of the information age, data security has become an indispensable element of organization operation, and its importance is increasingly prominent. This study is committed to the in-depth exploration and optimization of the data security risk assessment model, aiming to provide a scientific and efficient assessment tool to assist organizations to make more sensible and reasonable decisions in the field of information security management. Through the optimization of the model, it not only improves the efficiency of data security management, but also realizes the accurate identification and assessment of data security risks, which significantly enhances the response ability of the organization to potential threats. In addition, this study also focuses on the integration and unification of data security risk assessment standards at home and abroad, aiming to form a widely recognized assessment criteria and promote the consistency and interoperability of data security management on a global scale. The realization of this goal is of far-reaching significance for promoting international cooperation and exchanges in the field of data security.

1.3 Review of domestic and foreign studies

1.3.1 Status of domestic research

In the field of performance and security level evaluation of Web applications, domestic scholars have conducted extensive and in-depth research, and put forward a variety of evaluation methods and strategies.

Xiao Xinfeng paid close attention to the performance testing technology of the Web application program earlier. She discussed the research background, significance and specific testing methods of the performance testing, which provided a basis for the subsequent performance evaluation research [1]。Ma Hongwei made an in-depth analysis of the security problems of Web applications, pointed out the common security vulnerabilities and corresponding countermeasures, and emphasized the importance of security assessment in Web application development[2]。Yang Yanmei further studied the security design and

application technology of Web applications, and she proposed a series of safety design principles and methods, designed to improve the security of Web applications[3]。On this basis, Dai Junya specifically discussed the specific application of security design in Web applications, which provides practical guidance for security assessment[4]。Hang Jiaqi et al. improved the performance of the Web application through the method of stress testing. They elaborated on the implementation steps and effect evaluation of stress testing, providing a new perspective for the performance evaluation[5] 。Zhao Heng focuses on the security technology of Java Web applications. He analyzed the security threats and protection measures under the Java platform, providing technical support for the security assessment of Java

Web applications[6].

In terms of evaluation methods, Hou Xilin and Wang Xinru are based on hierarchical analysis and fuzzy comprehensive evaluation method for enterprises.

The value of big data resources has been evaluated, and their methodology provides a useful reference for the performance and security level evaluation of Web applications [7]. Song Dong et al. also adopted the AHP-fuzzy comprehensive evaluation method to construct the value evaluation model of the leaked data, which further verified the application value of the fuzzy comprehensive evaluation method in the field of evaluation[8] 。In recent years, Han has continued the in-depth analysis of the security technology of Java Web applications, and she has summarized the current security threats and defense strategies, providing the latest technical reference for the security assessment of Java Web applications[9]. Jin Tongxin and Lu Huayan evaluated the complexity of the simulation environment based on the fuzzy comprehensive evaluation method, and their research provides a new idea for the complexity processing in the Web application evaluation[10]。An Ling made a comprehensive analysis of the Web application security detection technology, and she introduced a variety of detection technologies and tools, which provided a practical technical means for the security assessment of Web applications[11].

To sum up, domestic scholars have achieved remarkable research results in the field of performance and security level evaluation of Web applications, and put forward a variety of evaluation methods and strategies. These studies not only enrich the evaluation theory, but also provide a strong support for the practical evaluation work. However, with the continuous development of Web technology and the increasing complexity of security

threats, we still need to further explore and improve the evaluation methods to improve the accuracy and effectiveness of the evaluation.

1.3.2 Status of foreign research

In the field of performance and security level evaluation of Web applications, foreign scholars have also conducted a lot of in-depth research and put forward a series of innovative evaluation methods and theories.

Kyung-Soo Joo and Jung-Woong Woo proposed an object-oriented security analysis and design methodology for Web applications. Through object-oriented ideas, they made a detailed analysis of the security requirements of Web applications, and designed a set of corresponding security mechanisms to provide theoretical basis and methodological support for the security evaluation of Web applications[12]. Cheng He and Yan Fei Liu propose a Web application security test method based on the vulnerability model. By conducting an in-depth analysis of the vulnerabilities of Web applications, they built the vulnerability model, and designed the security test process based on the model, which provided practical guidance for the security evaluation of Web applications[13]. With the continuous development of Web technology, Mamdouh Alenezi and other scholars have made significant progress in the Web application security testing framework.

They designed a comprehensive security testing framework that can automatically detect security vulnerabilities in Web applications and provide corresponding repair suggestions, providing powerful tool support for the security evaluation of Web applications[14]。 In the same year, Mamdouh Alenezi et al. also explored the security of open-source Web applications. Through a static analysis of the open-source Web application, they

discovered some common security vulnerabilities and proposed corresponding fixes. This study provides an important reference for security assessments of open-source Web applications[15]。 Chahal Navdeep S. et al. proposed a way to proactively evaluate Web application security by integrating security tools into secure orchestration platforms. They have designed a secure orchestration platform that integrates multiple security tools for a comprehensive security assessment of Web applications. This approach not only improves the efficiency and accuracy of the security assessment, but also provides new ideas for the security management of Web applications[16].

To sum up, foreign scholars have achieved fruitful research results in the performance and security level evaluation of Web applications. These studies not only enrich the evaluation theory, but also provide a strong support for the practical evaluation work. However, with the continuous development of Web technology and the increasing complexity of security threats, we still need to further explore and improve the evaluation methods to improve the accuracy and effectiveness of the evaluation. At the same time, the research results of foreign scholars also provide useful reference and inspiration for our research in this field.

1.4 Technical route

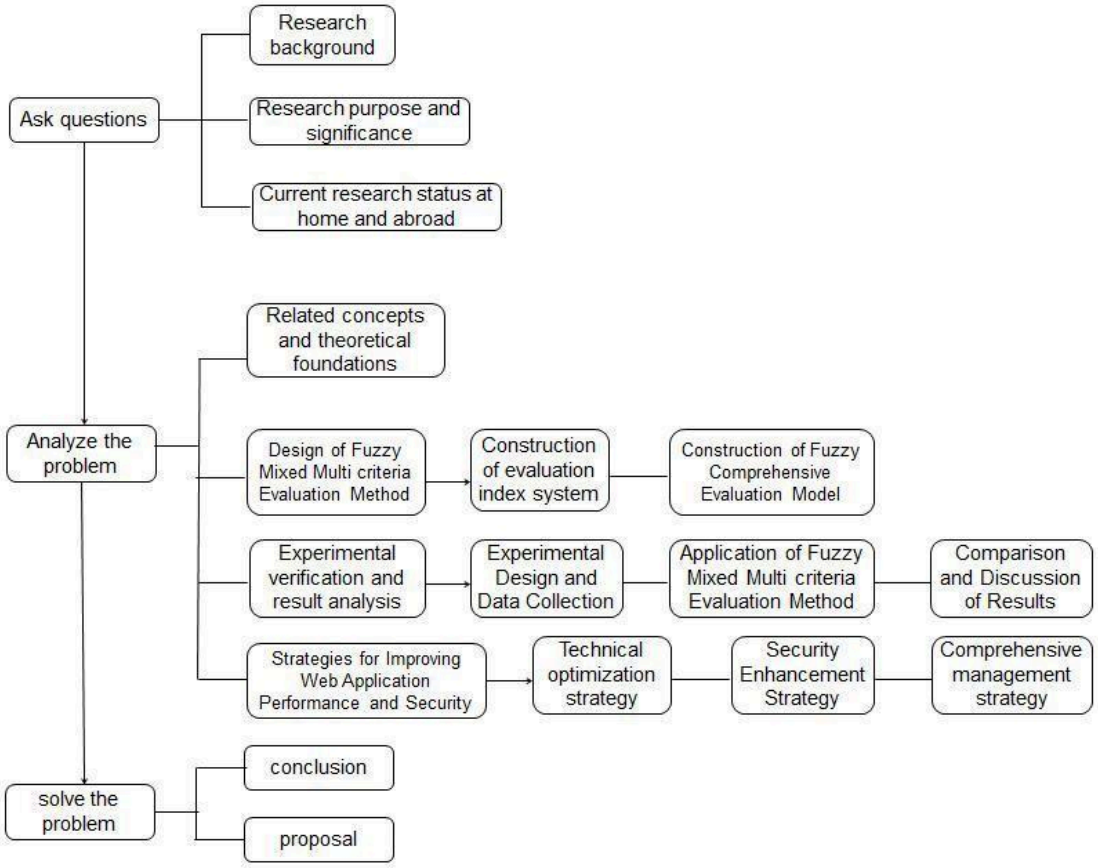

Figure 1-1 Research Technology Roadma

2. Relevant concepts and theoretical basis

2.1 Fuzzy comprehensive evaluation method

Fuzzy comprehensive evaluation method (Fuzzy Comprehensive Evaluation, FCE) is a comprehensive evaluation of the status of the evaluated objects from the characteristics of fuzzy relationship synthesis. This method regards the fuzzy object to be evaluated and the fuzzy concepts reflecting their properties as fuzzy set, and with the principle of maximum membership in the fuzzy mathematical theory, transforms the original fuzzy and difficult subjective qualitative evaluation into objective and standard quantitative evaluation. This transformation process not only improves the accuracy of the evaluation, but also enhances the objectivity of the evaluation results.

In the fuzzy comprehensive evaluation method, the evaluation object and their properties are abstracted into fuzzy sets, and the importance and state of each factor are described in the form of fuzzy relation matrix. This method is particularly suitable for dealing with multi-level and multi-factor fuzzy nonquantitative problems. Its mathematical model is simple and clear, the results are determined, and the system is highly operable. In the evaluation of uncertainty problems in many fields, the fuzzy comprehensive evaluation method has shown its unique advantages, and has become an important tool that is difficult to be replaced by other data models.

The application of fuzzy comprehensive evaluation method is particularly critical in the performance and security level evaluation of Web applications. By establishing risk factor set and evaluation set, using the

weight fuzzy matrix and relationship fuzzy matrix, this method can comprehensively consider multiple performance indicators and safety factors, and quantify the relative influence of each factor in the form of weight. Then, one-factor evaluation is synthesized by fuzzy matrix operation, and the total evaluation result is obtained. This process not only embodies the unique advantages of the fuzzy comprehensive evaluation method in the quantification of qualitative evaluation, but also provides an effective means to deal with the uncertainty for the performance and security level evaluation of Web applications.

2.2 Performance influencing factors of Web applications

2.2.1 Calculation model of the browser response time

In the discussion of the complex system of Web application performance evaluation, the browser response time is one of the key indicators to measure the user experience, and the construction and analysis of its computing model is particularly important. Traditionally, measurement of Web server performance parameters such as transactions per unit time, throughput, CPU usage, disk I / O, memory usage, and response time have been the focus of performance engineering. However, with the rise of Web 2.0 technology, the Internet application model has undergone profound changes, and the traditional Web server-centered performance evaluation method has gradually exposed its limitations.

Under the Web 2.0 architecture, the interaction pattern between client and server changes significantly. In the past, Web servers handled most of the business logic, while browsers were responsible for presenting pages. However, in Web 2.0 applications, this pattern was completely broken. Take Lotus Mashups and WebSphere Portal as an example, the former is the representative of Web 2.0 application, and most of the work of its business logic and performance layer is completed in the browser side, while the latter follows the traditional three-tier architecture, and the business logic is mainly implemented in the server side. Specifically, Widgets content in Lotus Mashups applications is aggregated in the browser side, and the browser is responsible for embedding Widgets content in the DOM tree, undertaking the task of HTML generation and page content rendering, and running a large number of scripts. In contrast, Portlets content in WebSphere

Portal applications is aggregated on the server, which aggregates Portlets content into HTML, then enders the web content and achieves limited user interaction through scripts.

This change poses an unprecedented challenge to performance engineering. In the Web 2.0 architecture, the browser not only undertakes the task of page presentation, but also directly participates in the processing of business logic, which makes the browser response time become one of the key factors affecting the user experience. However, the traditional performance evaluation methods often ignore the performance bottleneck of the browser side, resulting in the performance problem is difficult to be fully found and solved. Therefore, building a computational model that accurately reflects the browser response time is important to improve the performance evaluation accuracy of Web applications.

When building the browser response time calculation model, we need to consider multiple factors comprehensively. First, the Web server response delay is a non-negligible part. Although the server-side business logic processing volume decreases in the Web 2.0 architecture, the server still needs to process requests from the browser and generate corresponding responses. Therefore, the server response delay is still one of the important factors affecting the browser response time. Second, page download delay is also a key factor affecting the browser response time. In Web

2.0 applications, page download delays often occupy most of the browsers response time, as the browser needs to download and parse a lot of scripts, style sheets, pictures, and other resources. Moreover, with the widespread use of AJAX technology, browsers manipulate the start time of

HTTP requests through scripts, which further increases the uncertainty of page download delay. Finally, the page rendering delay also has an important impact on the browser response time. In the Web 2.0 architecture, the browser is not only responsible for the page presentation, but also responsible for some business logic processing tasks. Therefore, the browser takes more time and resources when rendering pages. In addition, since the browser needs to parse and execute a large number of scripts, this also negatively affects the page rendering delay.

Based on the above analysis, we can build a simplified browser calculation model of response time: browser response time = Web server response delay + page download delay + page rendering delay. The model decomposes the browser response time into three main parts, each reflecting different factors affecting the browser response time.

To calculate the delay of the Web server response, we need to consider the time when the server processes the request, the network transmission delay, and the server resource utilization rate. Together, these factors determine the speed and efficiency of the server in responding to the request. When calculating the page download delay, we need to consider the size of the page resource, the network bandwidth, the concurrency of HTTP requests, and the browser cache strategy. Together, these factors determine the time it takes to transfer page resources from the server to the browser. When calculating the page rendering delay, we need to consider the time when the browser parses HTML and CSS, the time to execute the script, and the time to render the page. These factors together determine the time it takes for the browser to present the page resources to the user.

It is worth noting that the browser response time calculation model is not static. As Web technology continues to evolve, new performance bottlenecks and influencing factors may continue to emerge. Therefore, we need to continuously update and optimize the model to meet the new performance evaluation requirements. In addition, since the browser response time involves many factors and links, in practice, we also need to refine and adjust the model based on specific scenarios and requirements.

2.2.2 Analysis of the HTTP protocol

In the evaluation framework of exploring the performance and security level of Web applications, the HTTP protocol serves as the basis of Web communication, and its intrinsic mechanisms and features have a profound impact on the evaluation process. HTTP, the full name of hypertext transmission protocol, is currently widely used in version 1.1 and has played a key role on the World Wide Web since 1990 and has become a standard protocol for information exchange between clients and servers. The HTTP protocol defines the interaction criteria for the request and response between the client (usually a user agent, such as a Web browser) and the server (i. e., a Web site). This process may involve multiple layers of intermediate entities, such as a tunnel, gateway, or agent, which together form a complex network communication architecture.

Although the TCP / IP protocol dominates the Internet, the HTTP protocol does not require the use of TCP / IP as its underlying transmission protocol. In fact, HTTP has the flexibility to implement across the protocol, requiring only the underlying protocol to guarantee the reliability of data transmission. Therefore, any protocol that provides such guarantees can be

used as a transmission basis for HTTP. However, in real applications, in view of the many functions provided by TCP protocol (such as error detection and recovery, traffic control, etc.), HTTP communication on the Internet almost entirely depends on TCP protocol. The information exchange between Browser and Web Server is realized based on the HTTP protocol above TCP.

The HTTP protocol uses the request-response mode that determines that a Web application must use some transfer protocol when transferring data at the transfer layer. Although the HTTP standard does not specify TCP as a unique transmission protocol, in practice, the widespread application of TCP makes it the preferred choice for HTTP communication. The HTTP request is initiated by the client, including the request method (such as GET, POST), request header and request body (if necessary). The server returns the corresponding response according to the request, consisting of the status line, response header and response body. The stateless nature of the HTTP protocol means that each request is treated as an independent event and the server does not retain any status information between requests, requiring that the request be sent back to the server each time the browser needs to update the content.

Among the request methods of HTTP protocol, GET and POST are the most commonly used. The GET method is usually used to request the server to send a resource. The request information contains the request method, URI, protocol version, request header, and the server response contains the state line, response header and response body. For example, when a browser requests a JavaScript file, it will send a GET request containing information

about the file URI, protocol version, browser identity, and the server returns a response containing the file content, content type, the time of final modification, etc. The POST method is usually used to submit form data to the server, and the request body contains the data to be sent.

In the HTTP protocol, the caching mechanism is introduced to improve the resource loading efficiency. When a browser has a copy of the requested resource in the cache but is not sure if it is still valid, a request with an If-Modified-Sense header is sent to the server to ask if the resource has been modified. If the server confirms that the resource is not modified, it returns a 304 status code to inform the browser that it can obtain resources directly from the cache to avoid unnecessary downloads, reduce the response time and improve the user experience. In addition, the Expires header is also a way to optimize resource loading by including an expiration time in the browser response to use the cached copy directly before the resource expires, without having to send a request to the server again.

The communication process of the HTTP protocol is a complex and delicate process involving multiple steps. A series of actions expands when the user enters a URL in the browser address bar and presses the enter key. First, the URL is resolved into the complete information used to locate the resource, including the protocol type, host name, port number (the default is 80), and the URI of the requested resource. Subsequently, the browser converts the host name to the corresponding IP address through DNS resolution and establishes a TCP connection to the server. Once the TCP connection is established, the browser sends an HTTP request to the server, which contains the request method, protocol version, request header, etc.

After the server receives the request, it generates the corresponding response according to the content of the request and sends it back to the browser through the TCP connection. The response includes the status code, response header and response body, where the status code indicates the processing result of the request, the response header contains metadata such as server information, content type, cache control, and the response body contains the data required by the user. Finally, the server may close the TCP connection unless explicitly indicated in the request or response header (e. g. using the Connection: KEEP-ALIVE header) for subsequent request-response interaction.

The lack of HTTP protocol, request-response mode, and cache mechanism have an important impact on the performance and security level evaluation of Web applications. In terms of performance evaluation, the statelessness of the HTTP protocol requires the server to efficiently process large numbers of concurrent requests, while the caching mechanism helps to reduce the transmission of repeated resources, reduce the network load, and improve the response speed. However, stateless may also lead servers to face challenges in processing applications that need to maintain user status, which need to be compensated by techniques such as session management. In terms of security level evaluation, HTTP protocol itself does not provide encryption function, which makes the transmitted data easy to be intercepted and tampered with. Therefore, in practical application, HTTPS (i. e. HTTP over SSL / TLS) is usually used to ensure the security of data transmission.

In conclusion, the HTTP protocol serves as the basis of Web application communication, and its intrinsic mechanisms and features have an important

impact on the evaluation of performance and security levels. When constructing a fuzzy mixed multi-criteria evaluation framework, HTTP protocol features such as request-response mode, anstateism, caching mechanism, etc., and the impact of these features on Web application performance and security. Through an in-depth analysis of how the HTTP protocol works, the performance performance and safety level of Web applications can be even more accurately evaluated, providing strong support for optimization and improvement.

3. Design of fuzzy and mixed multi-standard evaluation method

3.1. Construction of the evaluation index system

The scientific and comprehensive nature of the evaluation index system is crucial when building fuzzy mixed multi-standard evaluation methods for Web application performance and security levels. This study is committed to build a multi-dimensional index system that can fully reflect the data security and performance performance of Web applications. The construction process of this system deeply integrates literature analysis and expert research, aiming to ensure that the selected indicators meet the theoretical requirements and have practical operability.

3.1.1 Establishment of data security risk assessment indicators

Data security risk assessment is an important part of the Web application security assessment. Through detailed literature analysis in this study, a series of key data security risk assessment indicators are extracted from authoritative documents such as data Safety Law, Personal Information Protection Law, Data governance principles, data security full life cycle management, DSMM data maturity model and Data Security Field Guide.

Table 3-1 List of data security risk assessment indicators and sources

metric	source	Relevant terms
Data classification and identification	The Data Security Act,	The enterprise shall manage the data held by classification
Data breach and emergency response		Responding quickly to data leaks
Data Backup and Recovery	Data Security Practice Guide data security full life cycle management	Data backup and recovery strategy should be established
Data full lifecycle management		Data should be continuously managed from generation to destruction.
data encryption	The Information Security Technology-Data Security Capability Maturity Model, DSMM	Encryption is an important means of protecting data security
Security configuration management		Maintain the security configuration of the system and the application
User authentication and authorization	《ISO/IEC 27001》	The organization shall implement access control policies
Vulnerability management and patch application		System vulnerabilities should be checked and necessary patches applied
Network information security management	The Data Security Domain Guide	Cyber security should be managed comprehensively
Third-party risk management		Manage the risks of the external service providers
Security log recording and monitoring		Logging and event monitoring shall be performed
Safety training and awareness		Regular safety training and awareness promotion
Compliance and legal compliance	"Personal Information Protection Act"	Laws and regulations on personal information protection shall be observed

Privacy protection measures		Take the necessary measures to protect personal privacy
data access control	Standard for Data Management System	Reasonable control of data access rights

Specifically, according to the relevant provisions of the Data Safety Law, indicators such as data classification and identification, data leakage and emergency response have been established to reflect the capabilities of enterprises in data management and emergency response. At the same time, referring to the guiding principles of data security full life cycle management in the Data Security Practice Guide, the data backup and recovery, data full life cycle management and other indicators are introduced to ensure that the data is effectively managed in all stages of its life cycle. The DSMM data maturity model emphasizes the importance of data encryption technology and security configuration management, which accordingly sets up the evaluation indicators such as data encryption and security configuration management. In addition, the ISO / IEC 27001 standard of user authentication and authorization, network information security management, vulnerability management and patch application indicators, to provide an important reference for the construction of a comprehensive security management system. Security log recording and monitoring, security training and awareness, third-party risk management and other indicators in the Data Security Field Guide, further enhance the organizations ability to monitor data access and operation activities, enhance the safety awareness of employees, and effectively manage the risks related to external service providers. The compliance, legal compliance and privacy protection measures reflect the respect for personal privacyEmphasis and protection ensure the legitimacy and ethics of data processing activities. The data

access control index in the Data Management System Standard (DAMA International) emphasizes the rationality of the data access rights, and effectively prevents the abuse of data and unauthorized visits

In the process of building a data security risk assessment model, the selection of evaluation indicators is a crucial link. In this study, eight key data security risk assessment indicators were selected from 15 candidate indicators through in-depth investigation, as shown in Table 3-2. These indicators cover multiple key links of the data life cycle, and can fully and accurately reflect the data security status of the business system.

Data classification and Identification S1 is the basis of data security. It involves the accurate identification of data types and classification in the business system, especially the identification of sensitive data and personal information, which provides an important basis for the subsequent security measures. Data Backup and Recovery S2 ensures the integrity and availability of data. In case of system failure or data loss, data can be quickly recovered, effectively reducing potential losses. Data encryption S3 is an important means to protect data security, preventing unauthorized access and leakage by encrypting the content of data in the process of transmission and storage. User Authentication and Authorization S4 ensures that only authenticated users can access the system and can only access data within their rights limits, effectively preventing unauthorized access and operations. Security log recording and monitoring S5 is the key to detect and respond to security events. By recording the operation logs and abnormal behaviors of the system, the potential security threats are found and handled in time. Network information security management S6 covers the network security

protection and physical security protection measures of the business system boundary, such as firewall, intrusion detection / defense system, etc., providing a comprehensive network security guarantee for the business system. Data Access Control S7 and Data Full Lifecycle Management S8 focus on the security of data during access and data from creation to destruction, respectivelySafety management of each link. The implementation of these two indicators is important to ensure the confidentiality, integrity and availability of data

Table 3-2 Overview of data security risk assessment indicators

metric	explain
Data classification and identification of S1	Identify the data types and classification in the business system, especially the identification of sensitive data and personal information.
Data Backup and Recovery S2	Evaluate the frequency, integrity, security, and recovery capability of the data backup.
Data encryption S3	Assess the encryption measures of the data during transmission and storage, and the management of the encryption keys.
User authentication and Authorization S4	Check the strength and effectiveness of the user authentication and authorization mechanisms in the system.
Security logging and monitoring S5	Check if there is sufficient logging and monitoring measures to detect and respond to security incidents.
Network information security management S6	Evaluate the network security protection and physical security protection measures of the business system boundary, such as firewall and intrusion
Data access control S7	Assevaluate the strategy and implementation of data access control in business systems, including the application of the minimum access principle.
Data full lifecycle management S8	Assess the security management of data in the business system from creation, storage, use, sharing and destruction.

To sum up, the data security risk assessment indicators extracted through literature analysis cover the classification of data, security protection, access control, compliance, privacy protection, third-party risk management and other aspects, forming a comprehensive and specific evaluation index system.

3.1.2 Evaluation hierarchy of index system

In the construction of the evaluation index system, the hierarchical analysis method (AHP) was used to clarify the hierarchical relationship and the relative importance of each index. The evaluation index system is divided into two levels: target level and index layer. The target layer is the data security risk assessment of the evaluation target —— Web application for this study. The index layer contains specific evaluation indicators extracted from literature analysis, including data classification and identification (S1), data backup and recovery (S2), data encryption (S3), user authentication and authorization (S4), security logging and monitoring (S5), network information security management (S6), data access control (S7) and data full life cycle management (S8), as shown in Figure 3-1:

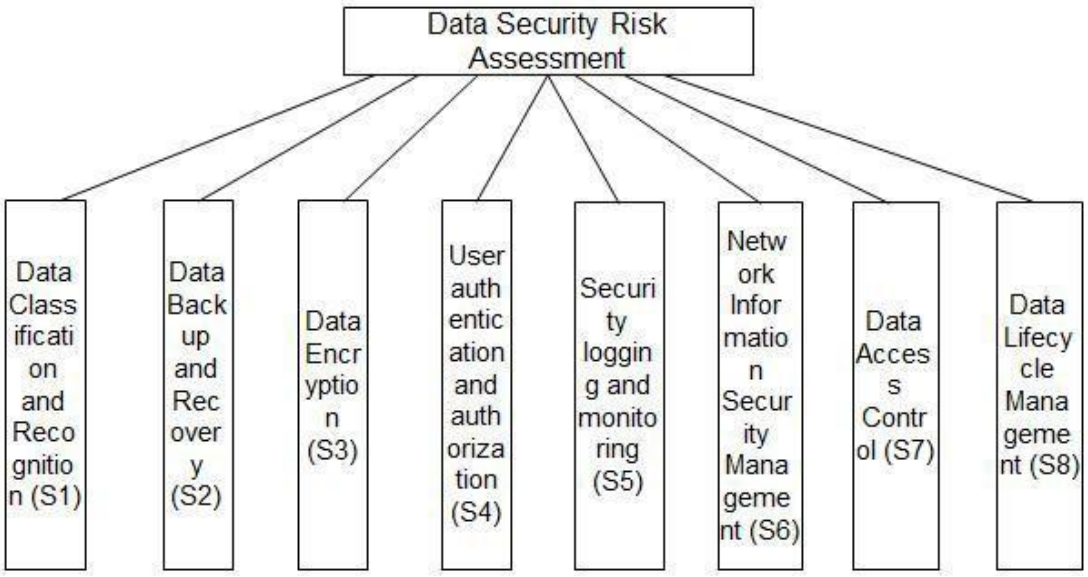

Figure 3-1 schematic hierarchical analysis of web application security risk assessment index

In order to determine the weight of these indicators in the data security risk assessment model, this study conducted several rounds of expert research, and the geometric average method was adopted to gather the judgment matrix of 17 experts. Through this method, a comprehensive and robust judgment matrix is obtained, which provides a solid foundation for the subsequent construction of the fuzzy comprehensive evaluation model.

3.2 Fuzzy comprehensive evaluation model construction

After constructing a comprehensive and specific evaluation index system, this study further designed a fuzzy comprehensive evaluation model to realize the quantitative evaluation of Web application performance and security level.

3.2.1 Basic principle of fuzzy comprehensive evaluation

Fuzzy comprehensive evaluation is a comprehensive evaluation method based on fuzzy mathematical theory, which can transform the qualitative evaluation into quantitative evaluation and effectively deal with the ambiguity and uncertainty in the evaluation process. In the performance and security level evaluation of Web applications, the fuzzy comprehensive evaluation method has significant advantages due to a large number of factors that are difficult to accurately quantify, such as user satisfaction and system stability.

3.2.2 Construction steps of the fuzzy comprehensive evaluation model

(1) Determine the evaluation factor set

The evaluation factor set is the evaluation index system constructed in this study, including data classification and identification (S1), data backup and recovery (S2), data encryption (S3), user authentication and authorization (S4), security logging and monitoring (S5), network information security management (S6), data access control (S7), and data full life cycle management (S8).

(2) Determine the evaluation grade set

The evaluation grade set is a collection of various evaluation results that may be made by the evaluation object. This study divided the performance and safety levels of Web applications into five grades: excellent, good, medium, poor and poor, as shown in Table 3-3. The five levels correspond to different performance and safety performance levels, respectively.

Table 3-3 Reference grade table of fuzzy comprehensive evaluation

grade	characteristic	description
5	very high	The probability of this data security event is very high, and the accident is easy to occur
4	higher	The probability of this data security event is higher, and it is more prone to accidents
3	same as	The probability of this data security event is general and prone to accidents
2	lower	The probability of this data security event is low, and it is difficult to have accidents
1	Very low	The probability of this data security event is very low, and it is extremely difficult to have an accident

(3) Determine the membership function

Membership function is the key element in fuzzy comprehensive evaluation, which describes the fuzzy relationship between evaluation factors and evaluation grade. This study will use common membership function forms, such as linear and quadratic functions, to determine the membership of each evaluation factor in different evaluation grades based on expert experience and actual data.

(4) Determine the weight vector

The weight vector reflects the importance of each evaluation factor in the evaluation. AHP hierarchy for 8 items of S1, S2, S3, S4, S5, S6, S7, S8 yielded eigenvector (1.830,1.071,1.130,101,1.199,0.810,0.653,0.796,0.511), and a total of 8 corresponding eigenvector values are shown in Table 3-4:

Table 3-4 Eigenvectors of the 8 indicators

project	feature vector	weighted value
Data classification and identification of S1	1.83	22.88%
Data Backup and Recovery S2	1.071	13.39%
Data encryption S3	1.13	14.13%
User authentication and Authorization S4	1.199	14.99%
Security logging and monitoring S5	0.81	10.12%
Network information security management S6	0.653	8.17%
Data access control S7	0.796	9.95%
Data full lifecycle management S8	0.511	6.38%

(5) Conduct fuzzy comprehensive evaluation

After constructing the fuzzy evaluation matrix and determining the weight vector, this study will use the appropriate fuzzy synthesis operator (such as weighted average operator, maximum and minimum operator, etc.) to synthesize the fuzzy evaluation matrix and weight vector to obtain the fuzzy comprehensive evaluation results of each evaluation object. This result would be a fuzzy vector reflecting the membership of the evaluation object across different evaluation grades.

(6) Processing of fuzzy comprehensive evaluation results

In order to obtain the final evaluation results, this study will further treat the fuzzy comprehensive evaluation results. A common method is to normalize the fuzzy vector, and then select the evaluation level with the highest membership as the final evaluation result. In addition, other methods (such as weighted average method, fuzzy clustering method, etc.) can be used to further analyze and process the fuzzy comprehensive evaluation results according to the actual needs.

In conclusion, this study realizes the quantitative evaluation of Web application performance and security level by constructing a comprehensive and specific evaluation index system and designing a fuzzy comprehensive evaluation model. This evaluation method is not only scientific and reasonable in theory, but also significantly practical and operable in practical application.

4. Experimental verification and result analysis

4.1 Experimental design and data collection

In the study of this paper, the experimental design is a crucial link, which determines the validity of the data and the reliability of the evaluation results. The primary objective of the experiment is to validate the effectiveness of the fuzzy hybrid multi-standard method (Fuzzy Hybrid Multi-Criteria Method, FHMCM) in evaluating the performance and security level of Web applications. To ensure the comprehensiveness and accuracy of the experiment, the experimental design covers multiple dimensions,

including the selection of experimental subjects, the method and process of data collection, and the configuration of the experimental environment.

4.1.1 Selection of experimental subjects

The choice of subjects has a decisive effect on the experimental results. To verify the wide applicability of FHMCM, multiple Web applications covering different industries, different sizes and different technical architectures were selected for this experiment. These apps include e-commerce platforms, online banking systems, social media platforms, and education management systems. Each application represents a typical application of its industry and is representative.

4.1.2 Data collection method

Data collection is the basis for the experimental validation. To comprehensively evaluate the performance and security level of the Web application, multiple data collection methods were used, including questionnaires, performance test tools, security scanning tools, and log analysis.

The questionnaire was administered to users and administrators of the app to understand their perception and feedback on application performance and security. The questionnaire covers key aspects of the application such including response time, throughput, stability, user authentication, data encryption, and security logging.

The performance testing tool is used to simulate real user behavior and perform stress and load testing on applications. Through testing, the

performance indexes such as response time, throughput, and error rate of the application under different loads can be obtained. Security Scan tools are used to detect security vulnerabilities and weaknesses in applications. These tools can automatically scan the application for code, configuration, and vulnerability libraries for potential security risks.

Log analysis is used to collect and analyze the run logs and error logs of the application. Analyze logs for application health, abnormal behavior, and potential security threats.

4.1.3 Experimental environment configuration

The configuration of the experimental environment is crucial for the accuracy of the experimental results. To ensure the fairness and reproducibility of the experiment, a standardized experimental environment configuration was used for this experiment.

The experimental environment includes a high-performance server as a deployment platform for an application, and multiple client computers to simulate user behavior. Both the server and the client computer are configured with the latest operating system and the necessary software tools.

In addition, the experimental environment also includes network devices and security devices, such as firewalls, intrusion detection systems, and data encryption devices. These devices are used to simulate a real network environment, ensuring the accuracy of the experimental results.

During the experiment, all equipment was installed and configured in a standard configuration to ensure consistency and repeatability of the

experimental environment.

4.2 Application of fuzzy and mixed multi-standard evaluation method

After the sufficient data was collected, this experiment began to apply the fuzzy hybrid multi-criteria evaluation method (FHMCM) to evaluate the performance and safety level of Web applications. FHMCM combines fuzzy comprehensive evaluation method and hierarchical analysis method (AHP), which can comprehensively consider multiple evaluation indicators and obtain comprehensive and accurate evaluation results.

4.2.1. Construction of the evaluation index system

In FHMCM, the construction of the evaluation index system is one of the key steps. According to the characteristics and evaluation objectives of Web application, a comprehensive evaluation index system includes performance index and safety index.

Performance indicators include response time, throughput, stability, resource utilization, etc., which are used to evaluate the operation efficiency and processing power of the application. These metrics can reflect the performance of an application under different loads and are critical for evaluating the application performance.

Security indicators include user authentication, data encryption, security logging, vulnerability repair, etc., to evaluate the security of the application. These indicators can reflect the applications ability to guard against security threats and respond to security risks.

When constructing the evaluation index system, this experiment fully

considers the comprehensiveness, measurement and operability of the index to ensure the accuracy and reliability of the evaluation results.

4.2.2 Application of Fuzzy comprehensive evaluation method

The fuzzy comprehensive evaluation method is a comprehensive evaluation method based on the fuzzy mathematics, which can deal with the evaluation problems with ambiguity and uncertainty. In the FHMCM, the fuzzy comprehensive evaluation method is used to transform the qualitative evaluation into the quantitative evaluation, so as to obtain a more accurate and objective evaluation results.

First, according to the evaluation index system, the experiment set the corresponding evaluation grade and standard for each index. The evaluation grade includes five grades: very high, high, general, low and very low, and each grade corresponds to a different scoring standard. Then, actual performance data for each indicator were collected through questionnaires, performance test tools and safety scanning tools. From these data, this experiment determined the corresponding membership function and membership matrix for each indicator. Finally, the operation rules combine weight set and membership matrix to obtain the fuzzy comprehensive evaluation result of each index. These results reflect the membership of each indicator at different evaluation grades, providing the basic data for the subsequent hierarchical analysis.

4.2.3 Application of hierarchical analysis method

Hierarchical analysis (AHP) is a structured method used to solve complex decision-making problems. In FHMCM, hierarchical analysis is

used to determine the weight of each index in the evaluation index system, so as to obtain the comprehensive evaluation results.

First, based on the evaluation index system. The model includes three levels: target layer, criterion layer and index layer. The target layer is the ultimate goal of the evaluation, namely the performance and security level of the Web application; the criterion layer is the main aspect of the evaluation, including performance indicators and security indicators, and the index layer is specific evaluation indicators such as response time, throughput, user authentication. Then, data on the relative importance between the indicators was collected through expert consultation and questionnaire survey. Using these data, a judgment matrix was constructed in this experiment, and the weight calculation and consistency test were performed. The weight calculation obtains the relative importance of each index in the evaluation, and the consistency test ensures the rationality and reliability of the judgment matrix. Finally, according to the weight set and fuzzy comprehensive evaluation results, the comprehensive evaluation results of each Web application can use the synthetic operation rules of hierarchical analysis. These results reflect the overall performance of the application in terms of performance and safety, providing the underlying data for the subsequent comparative analysis.

4.3 Results comparison and discussion

Through experimental validation of multiple Web applications, this experiment yielded a comprehensive evaluation of performance and safety for each application. To verify the effectiveness of FHMCM, this experiment analyzed the evaluation results against the performance in practical

applications, and the accuracy and reliability of the evaluation results were discussed.

4.3.1 Comparison of the evaluation results

Comparing the results of FHMCM evaluation with practical performance, FHMCM accurately reflects the overall performance of the Web application in terms of performance and security.

In terms of performance, the evaluation results of FHMCM are basically consistent with the test results of the performance test tool. For example, in terms of response time, FHMCM evaluation results show a positive correlation with the response time measured by the performance test tool, and in terms of throughput, FHMCM evaluation results also show a positive correlation with the throughput measured by the performance test tool. These results indicate high accuracy of FHMCM in performance.

In terms of safety, the evaluation results of FHMCM are generally consistent with the detection results of the safety scanning tool. For example, in terms of user authentication, the FHMCM evaluation results show a positive correlation with the validity of the authentication mechanism detected by the secure scanning tool, and in terms of data encryption, the FHMCM evaluation results also show the positive correlation with the effectiveness of the data encryption measures detected by the secure scanning tool. These results indicate that the FHMCM also has a high accuracy in terms of safety.

4.3.2 Reliability analysis of the evaluation results

To verify the reliability of FHMCM, the reliability of the evaluation results was analyzed. The reliability analysis includes two aspects: internal consistency and external consistency.

Internal consistency refers to assessing whether the relative importance relationship between the indicators in the index system is stable and reliable. This experiment verified internal consistency by consistency test. When constructing the judgment matrix, this experiment conducted many expert consultations and questionnaires to ensure the rationality and reliability of the judgment matrix. The results of the consistency test show that the consistency ratio (CR) of the judgment matrix is less than 0.1, which meets the consistency requirements, indicating that the relative importance relationship between each index in the evaluation index system is stable and reliable.

External consistency refers to assessing whether the results are consistent with performance in practical applications. This experiment verified the external consistency by comparing the evaluation results with the performance test tool and the safety scan tool. The comparative results show that the evaluation results of FHMCM are basically consistent with the performance in practical application, indicating that FHMCM has high reliability.

4.3.3 Discussion of the evaluation results

Through the comparison and analysis of the evaluation results, the following conclusions can be drawn:

(1) FHMCM can comprehensively consider multiple evaluation indicators to

obtain comprehensive and accurate evaluation results. In the experiment, FHMCM considers both performance and safety indicators, and gives a comprehensive evaluation of performance and safety for each Web application. These results can fully reflect the overall performance of the application, and provide strong support for the subsequent improvement and optimization.

(2) FHMCM has high accuracy and reliability. By comparing the test results with the performance test tool and the safety scan tool, the evaluation results of FHMCM are basically consistent with the performance in practical application. This indicates that FHMCM has a high accuracy and reliability in evaluating the performance and security level of Web applications.

(3) FHMCM has certain versatility and scalability. In the experiments, FHMCM was successfully applied in several Web applications with different industries, different sizes and different technical architectures. This indicates that FHMCM has some versatility and scalability to evaluate different types of Web applications. At the same time, with the continuous development of Web application technology and the emergence of new evaluation indicators, FHMCM can further expand and improve the evaluation index system to adapt to the new evaluation needs.

In conclusion, the experimental validation and results analysis show that the fuzzy hybrid multi-standard method (FHMCM) has significant advantages in evaluating the performance and security level of Web applications. FHMCM is able to comprehensively consider multiple evaluation indicators to obtain comprehensive and accurate evaluation results, and it has high accuracy and reliability. Therefore, FHMCM can

provide an effective and practical method for the performance and security evaluation of Web applications.

5. Web application performance and security improvement strategy based on the fuzzy hybrid multi-standard approach

5.1 Technical optimization strategy

In the field of performance optimization of Web applications, based on the evaluation results of fuzzy mixture of multiple standards (FHMCM). These strategies are designed to improve the response speed, processing power, and resource utilization efficiency of applications to meet users expectations for efficient and stable services.

5.1.1 Code and architecture optimization

Code efficiency and architecture design are the key factors affecting the performance of Web applications. According to the evaluation results of FHMCM, code reconstruction and algorithm optimization strategies are recommended. Code refactoring aims to simplify code logic, reduce redundant code, and improve code readability and execution efficiency. Algorithm optimization focuses on improving the core algorithm in the application program, reducing the time complexity and space complexity of the algorithm, so as to improve the processing speed and resource utilization.

In terms of architecture design, the use of distributed architecture and micro-service architecture are recommended. Distributed architecture

improves system scalability and fault tolerance by splitting applications into multiple independent services to achieve loose coupling and high availability between services. The microservice architecture further refines the service granularity, so that each service can be deployed, upgraded and expanded independently, thus improving the flexibility and response speed of the system.

5.1.2 Optimization of database performance

As a core component of a Web application, the performance of the database directly affects the overall performance of the application. According to the evaluation results of FHMCM, index optimization, query optimization and database clustering strategies are recommended.

Index optimization aims to improve the speed and accuracy of database queries by creating a reasonable index. Query optimization focuses on optimizing SQL statements, reducing unnecessary queries and calculations, and reducing the load of the database. The database cluster strategy enables the distributed storage and parallel processing of data, thus improving the database throughput and fault tolerance of the database.

5.1.3 Caching and load balancing strategy

Caching and load balancing are important ways to improve the performance of Web applications. Based on the evaluation results of FHMCM, it is recommended to adopt a multilevel caching strategy and an intelligent load balancing algorithm.

The multi-level caching policy enables rapid access and update of data

by deploying multiple cache layers between client, application server and database server. The intelligent load balancing algorithm dynamically adjusts the request distribution strategy according to the load situation of the server and the characteristics of user requests, to ensure that each server can make full use of its resources, so as to improve the overall performance of the system.

5.2 Security strategy strengthening

In the security area of Web applications, the results of FHMCM assessments reveal potential security risks and vulnerabilities. In order to improve the security of applications, this paper proposes a series of security strategy strengthening measures.

5.2.1 Data encryption and privacy protection

Data encryption is an important means to protect data security. According to the evaluation results of FHMCM, it is recommended to use advanced encryption algorithm and encryption protocol for encrypt storage and transmission of sensitive data. At the same time, a sound privacy protection mechanism should be established to ensure the legitimacy and morality of user data. This includes creating strict privacy policies, clarifying rules for the collection, use, and sharing of user data, and strengthening user privacy education and awareness enhancement.

5.2.2 Vulnerability management and patch update

Vulnerability management is an important part of ensuring the security of Web applications. According to the evaluation results of FHMCM, it is

suggested to establish a vulnerability scanning and repair mechanism, conduct regular vulnerability scanning and penetration testing on applications, and find and fix potential security vulnerabilities in time. At the same time, keep contact with software vendors to obtain and apply security patches in time to ensure that the latest version of the application has the highest security.

5.2.3 Access control and authentication

Access control and authentication are an important means of protecting Web applications from unauthorized access. According to the evaluation results of FHMCM, it is recommended to adopt a multi-factor authentication mechanism, such as password, biometric feature and dynamic verification code, to improve the accuracy and security of user authentication. At the same time, fine-grained access control strategies should be established to limit the access and operation of user applications according to their roles and rights, so as to prevent data leakage and abuse.

5.3 Comprehensive management strategy

In order to comprehensively improve the performance and security of Web applications, this paper also proposes a series of comprehensive management strategies. These strategies are designed to ensure that applications can serve consistently and steadily by optimizing management processes and improving management efficiency.

5.3.1 Performance monitoring and early warning mechanism

Performance monitoring is an important means to ensure the stable

operation of the Web applications. Based on the evaluation results of FHMCM, it is recommended to establish a comprehensive performance monitoring system to monitor the key performance indicators of the application in real time, such as response time, throughput and error rate. At the same time, the warning mechanism should be set up. When the performance index reaches the preset threshold, the warning notice should be automatically triggered, so as to take timely measures for intervention and optimization.

5.3.2 Security audit and compliance inspection

Security audit is an important means of assessing the security of Web applications. Based on the evaluation results of FHMCM, it is recommended to conduct regular safety audits and compliance checks to ensure that the application meets the relevant safety standards and legal and regulatory requirements. This includes checking the applications security configuration, user authentication mechanism, data encryption measures, and ensuring that the applications data processing and storage activities comply with the Data Security Act, the Personal Information Protection Act and other laws and regulations.

5.3.3 Continuous improvement and iterative optimization

Continuous improvement and iterative optimization are important ways to improve the performance and security of Web applications. Based on the evaluation results of FHMCM, it is recommended to establish a continuous improvement mechanism to evaluate and optimize the application regularly. This includes analyzing the shortcomings in the evaluation results,

developing targeted optimization measures, and tracking the optimization effect to ensure the effectiveness and sustainability of the optimization measures. At the same time, attention and research on new technologies and methods should be maintained in order to timely apply advanced technologies and methods to the optimization and improvement of applications.

In conclusion, based on the evaluation results of fuzzy mixed multi-standard method (FHMCM), this paper proposes a series of targeted technical optimization strategies, security strategy strengthening measures and comprehensive management strategies. These strategies are designed to comprehensively improve the performance and security of Web applications, ensuring that applications can deliver services consistently and steadily, and meet users expectations for efficient and secure services. By implementing these strategies, the competitiveness of Web applications can be significantly improved, providing strong support for enterprise digital transformation and business development.

6. Conclusions and prospects

6.1 Conclusion

This study designed and implemented a fuzzy hybrid multi-standard evaluation method based on the thorough analysis of Web application performance and security level. This method has comprehensively applied the fuzzy comprehensive evaluation method and the hierarchical analysis method to construct a comprehensive and detailed evaluation index system. In the experimental verification stage, through the data collection and analysis of multiple practical Web applications, the evaluation method proposed in this paper effectively reveals the specific performance of each application in terms of performance and security. The results show that the method can not only accurately quantify the performance indicators of Web applications, such as response time, throughput, but also effectively evaluate its security level, including key security elements such as data encryption strength and vulnerability management efficiency. By comparing the traditional evaluation methods, the method of this study shows significant advantages in the accuracy and reliability of the evaluation results, which provides strong data support for the optimization and improvement of Web application.

6.2 Outlook

Despite the initial results in the evaluation of Web application performance and security level, there are still many directions worth further exploration. First, as Web technologies continue to evolve, new performance and security challenges emerge in an endless stream, and future research should continue to focus on and incorporate these emerging factors to improve the evaluation index system. Secondly, in terms of data collection and processing, more advanced machine learning algorithms can be considered to improve the efficiency and accuracy of data processing and further optimize the performance of the evaluation model. In addition, in order to enhance the universality and practicability of the evaluation methods, future studies should also conduct more detailed case analysis for Web applications of different industries and sizes, in order to refine more targeted optimization strategies. Finally, considering the complexity and dynamics of Web applications, it will be one of the important future research directions to establish a continuous performance and security monitoring mechanism and realize real-time evaluation and early warning. Through continuous optimization and iteration, this study is expected to provide a more comprehensive and efficient solution for the performance improvement and security of Web applications.

reference documentation

[1] Xiao Xinfeng. Research and application of Web Application Performance Test Technology [J]. Science and Technology Information, 2010, (27): 37-38.

[2] Ma Hongwei. Security issues and countermeasures for Web applications [J]. Computer CD Software and Application, 2014,17 (03): 161-162 + 170.

[3] Yang Yanmei. Research on Web application security design and application technology [J]. Electronic Technology and Software Engineering, 2014, (12): 224.

[4] Dai Junya. Security design in the WEB application study [J]. Network security Technology and Application, 2017, (04): 65 + 68.

[5] Hang Jiaqi, Wang Chuan, Luo Xi. Improve the performance of the Web application through stress testing [J]. Digital Technology and Application, 2017, (09): 213-214.

[6] Zhao Heng. Java Web Application security technology [J]. Electronic Technology and Software Engineering, 2019, (04): 194.

[7] Hou Xilin, Wang Xinru. Research on the value evaluation of enterprise big data resources based on hierarchical analysis and fuzzy comprehensive evaluation method [J]. Journal of University of Science and Technology Liaoning, 2020,43 (01): 72-80.

[8] Song Dong, Zhang Lei, Su Majing. The value evaluation model of leaked data based on AHP-fuzzy comprehensive evaluation method [J]. Information

Technology and Network Security, 2020,39 (09): 44-48.

[9] Han Luying. About the Java Web Application security technology analysis [J]. Information recording materials, 2021,22 (08): 115-116.

[10] Jin Tongxin, Lu Huayan. Research on the complexity evaluation of simulation environment based on fuzzy comprehensive evaluation method [J]. Software Engineering, 2023,26 (03): 46-51.

[11] An Ling. Web application security detection technology analysis [J]. Vd. standardization, 2024, (18): 178-180.

[12] Kyung-Soo Joo,Jung-Woong Woo.An Object-Oriented Analysis and Design Methodology for Security of Web Applications[J].Journal of Internet Computing and Services,2013,14(4):35-42.

[13] Cheng He,Yan Fei Liu.Vulnerability Model-Based Web Applications Security Testing Approach[J]. Applied Mechanics and Materials,2014,3561(678-678):468-472.

[14] Mamdouh Alenezi,Layla Mohammed Alrawais,Mohammad Akour.Security Testing Framework for Web Applications[J].International Journal of Software Innovation (IJSI),2018,6(3):93-117.

[15] Mamdouh Alenezi,Mohammad Zarour,Khawlah Alomar.Are Open Source Web Applications Secure? Static Analysis Findings[J].International Journal of System & Software Engineering,2018,6(2):1-9.

[16] Chahal Navdeep S.,Bali Preeti,Khosla Praveen Kumar.A Proactive Approach to assess web application security through the integration of

security tools in a Security Orchestration Platform[J].Computers & Security,2022,122