

Claims

What is claimed is:

1. A sensitive information processing method performed by a computer comprising:

acquiring, by an information acquisition unit of the computer, to-be-processed information in a page;

determining, by a sensitive information identification unit of the computer, whether the to-be-processed information is sensitive information based on sensitive information stored in a sensitive information library of the computer according to a preset sensitive information identification strategy;

performing, by an information processing unit of the computer processing according to a preset sensitive information processing strategy stored by a processing strategy unit of the computer when the to-be-processed information is sensitive information, to form processed sensitive information; and

substituting, by a substitution unit of the computer, the to-be-processed information in the page with the processed sensitive information, to form a page with the processed sensitive information, wherein the acquiring to-be-processed information in a page includes:

acquiring the to-be-processed information in the page by using an interceptor after a Controller in an MVC framework structure is invoked and before a view is rendered; or

acquiring the to-be-processed information in the page by using an interceptor after a Velocity in an MVC framework structure is invoked.

2. A sensitive information processing method performed by a computer comprising:

acquiring, by an information acquisition unit of the computer, to-be-processed information in a page;

determining, by a sensitive information identification unit of the computer, whether the to-be-processed information is sensitive information based on sensitive information stored in a sensitive information library of the computer according to a preset sensitive information identification strategy;

performing, by an information processing unit of the computer, processing according to a preset sensitive information processing strategy stored by a processing

strategy unit of the computer when the to-be-processed information is sensitive information, to form processed sensitive information; and

substituting, by a substitution unit of the computer, the to-be-processed information in the page with the processed sensitive information, to form a page with the processed sensitive information, wherein the to-be-processed information includes:

variable information in a ModelMap in an MVC framework structure of a page server.

3. The sensitive information processing method of claim 2, wherein the determining whether the to-be-processed information is the sensitive information according to the preset sensitive information identification strategy includes:

acquiring a variable name of the variable information in the ModelMap in the MVC framework structure of the page server;

comparing the acquired variable name of the variable information in the ModelMap with sensitive information stored in a sensitive information library, to determine whether the variable name is in the sensitive information library; and

determining whether the to-be-processed information is the sensitive information according to the determination result of whether the variable name is in the sensitive information library.

4. The sensitive information processing method of claim 3, further comprising:

determining, by a to-be-processed sensitive information unit of a computer, according to a preset sensitive information monitoring strategy, whether a value of the variable information in the ModelMap in the MVC framework structure of the page server is to-be-processed sensitive information; and

sending, by a sending unit of the computer, a variable name corresponding to the value of the variable information to the sensitive information library when it is determined according to the sensitive information monitoring strategy that the value of the variable information is to-be-processed sensitive information.

5. The sensitive information processing method of claim 2, wherein the performing processing according to a preset sensitive information processing strategy includes:

setting a sensitive information processing strategy for values corresponding to

different variable names according to the different variable names in the variable information; or

setting, in a same variable name of the variable information according to a privilege of specified field information, a sensitive information processing strategy for a value corresponding to the same variable name.

6. The sensitive information processing method of claim 5, wherein the sensitive information processing strategy includes at least one of the followings:

- non-processing;
- display of a predetermined part;
- completion of masking;
- privilege-based masking;
- display after transformation; and
- misinformation.

7. A device for implementing sensitive information processing comprising:

- an information acquisition unit that acquires to-be-processed information in a page;
- a sensitive information library that stores sensitive information;

- a sensitive information identification unit that determines whether the to-be-processed information is sensitive information on the basis of the sensitive information stored in the sensitive information library;

- a processing strategy unit that stores a sensitive information processing strategy;

and

- an information processing unit that processes, when the sensitive information identification unit determines that the to-be-processed information is sensitive information, the to-be-processed information on the basis of the sensitive information processing strategy stored by the processing strategy unit, to form processed sensitive information, wherein the to-be-processed information acquired by the information acquisition unit includes:

- variable information in a ModelMap in an MVC framework structure of a page server.

8. The device for implementing sensitive information processing of claim 7, wherein the sensitive information processing strategy stored by the processing strategy

unit includes:

a sensitive information processing strategy that is set for values corresponding to different variable names according to the different variable names in the variable information; or

a sensitive information processing strategy, which is set in a same variable name of the variable information according to a privilege of specified field information, for a value corresponding to the same variable name.

9. The device for implementing sensitive information processing of claim 8, wherein the processing strategy unit includes at least one of the following units:

a predetermined-part display unit that displays a particular field of a value corresponding to the variable name according to a predetermined display rule;

a complete-masking unit that masks all fields of the value corresponding to the variable name according to a predetermined masking rule;

a privilege-based masking unit that processes the value corresponding to the variable name according to a privilege of a specified field;

a transformation and display unit that transform the value corresponding to the variable name according to a predetermined transformation rule, and use the transformed value as the value of the variable name; and

a misinformation unit that skips processing the value corresponding to the variable name when any one of the structural modules in the sensitive information processing device is abnormal or the sensitive information identified by the sensitive information identification unit does not conform to a sensitive information determination standard set by a third-party module, and generate a misinformation log.

10. The device for implementing sensitive information processing of claim 7, wherein the sensitive information identification unit includes:

a key value acquisition unit that acquire a variable name of the variable information in the ModelMap in the MVC framework structure of the page server;

a comparison unit that compare whether the acquired variable name of the variable information in the ModelMap is the same as the sensitive information stored in the sensitive information library; and

a first determination unit that determines whether the to-be-processed information is sensitive information according to the comparison result of the comparison unit.

11. The device for implementing sensitive information processing of claim 7, further comprising:

- a monitoring strategy unit that stores a preset sensitive information monitoring strategy;

- a to-be-processed sensitive information unit that determines, according to the preset sensitive information monitoring strategy, whether a value of the variable information in the ModelMap in the MVC framework structure of the page server is to-be-processed sensitive information; and

- a sending unit that sends a variable name corresponding to the value of the variable information to the sensitive information library when the to-be-processed sensitive information unit determines that the value of the variable information is to-be-processed sensitive information.

12. The device for implementing sensitive information processing of claim 7, further comprising:

- a returning unit that directly sends the processed sensitive information to a server or to a processed sensitive information receiving unit of the server by using an interceptor.

13. The device for implementing sensitive information processing of claim 7, further comprising:

- a substitution unit that substitutes the to-be-processed information in the page with the processed sensitive information.

14. A server for implementing sensitive information processing comprising:

- an MVC target system that receives an HTTP request sent by a client terminal, generates a page template ModelMap according to the HTTP request, transmits to-be-processed information into the generated page template ModelMap, completes rendering of a page corresponding to the HTTP request, sends the rendered page to the client terminal, receives processed sensitive information sent by a sensitive information processing module, and substitutes the corresponding to-be-processed information in the page template ModelMap with the processed sensitive information;

- an interceptor that acquires to-be-processed information in the page template ModelMap, sends the to-be-processed information to the sensitive information processing module, receives processed sensitive information sent by the sensitive information

processing module, and sends the processed sensitive information to the MVC target system; and

the sensitive information processing module that receives the to-be-processed information, determines whether the to-be-processed information is sensitive information; and processes the to-be-processed information, which is determined as sensitive information according to a preset sensitive information processing strategy, to form processed sensitive information;

wherein the sensitive information processing module includes:

an information receiving unit that receives to-be-processed information;

a first sensitive information library that store sensitive information;

a first sensitive information identification unit that determines, on the basis of the sensitive information stored in the first sensitive information library, whether the to-be-processed information is sensitive information;

a first processing strategy unit that stores the sensitive information processing strategy;

a first information processing unit that processes, when the first sensitive information identification unit determines that the to-be-processed information is sensitive information, the to-be-processed information on the basis of the sensitive information processing strategy stored by the first processing strategy unit, to form processed sensitive information; and

a first returning unit that sends the processed sensitive information to the interceptor.

15. The server for implementing sensitive information processing of claim 14, wherein the acquiring, by the interceptor, to-be-processed information in the page template ModelMap includes:

acquiring the to-be-processed information in the page template ModelMap by using a postHandle or afterCompletion processing program of the interceptor.

16. The server for implementing sensitive information processing of claim 14, wherein the first processing strategy unit includes at least one of the following units:

a first predetermined-part display unit that displays a particular field of a value corresponding to the variable name according to a predetermined display rule;

a first complete-masking unit that masks all fields of the value corresponding to the variable name according to a predetermined masking rule;

a first privilege-based masking unit that processes the value corresponding to the variable name according to a privilege of a specified field;

a first transformation and display unit that transforms the value corresponding to the variable name according to a predetermined transformation rule, and use the transformed value as the value of the variable name; and

a first misinformation unit that skip processing the value corresponding to the variable name when any one of the structural modules in the sensitive information processing device is abnormal or the sensitive information identified by the sensitive information identification unit does not conform to a sensitive information determination standard set by a third-party module, and generate a misinformation log.

17. The server for implementing sensitive information processing of claim 14, wherein the first sensitive information identification unit includes:

a first key value acquisition unit that acquires a variable name of variable information in the ModelMap in the MVC target system;

a first comparison unit that compares whether the acquired variable name of the variable information in the ModelMap is the same as the sensitive information stored in the first sensitive information library; and

a second determination unit that determines whether the to-be-processed information is sensitive information according to the comparison result of the first comparison unit.

18. The server for implementing sensitive information processing of claim 14, further comprising:

a first monitoring strategy unit that stores a preset sensitive information monitoring strategy;

a first to-be-processed sensitive information unit that determines, according to the preset sensitive information monitoring strategy, whether a value of the variable information in the ModelMap in the MVC target system is to-be-processed sensitive information; and

a first sending unit that sends a variable name corresponding to the value of the variable information to the first sensitive information library when the first

to-be-processed sensitive information unit determines that the value of the variable information is to-be-processed sensitive information.

19. A security determination system comprising:

a second sensitive information library that stores sensitive information, receives a variable name sent by a second to-be-processed sensitive information unit, determines whether the stored sensitive information includes the received variable name, and stores the variable name as newly-added sensitive information when the determination result is that the sensitive information library does not comprise the received variable name;

a second sensitive information identification unit that acquires to-be-processed information in a page, and determines whether the to-be-processed information is sensitive information on the basis of the sensitive information stored in the second sensitive information library;

a second information processing unit that stores a sensitive information processing strategy, and further processes, when the second sensitive information identification unit determines that the to-be-processed information is sensitive information, the to-be-processed information on the basis of the stored sensitive information processing strategy, to form processed sensitive information;

a monitoring unit that stores a preset sensitive information monitoring strategy, determines, according to the stored sensitive information monitoring strategy, whether a value of variable information in a ModelMap in an MVC framework structure of the page server is to-be-processed sensitive information, sends a variable name corresponding to the value of the variable information to the second sensitive information library when determining that the value of the variable information is to-be-processed sensitive information;

a newly-added sensitive information log unit that generates a newly-added sensitive information log, the newly-added sensitive information log including a number of newly-added sensitive information in the second sensitive information library;

a to-be-processed sensitive information log unit that generates a to-be-processed sensitive information log, the to-be-processed sensitive information log including the number of to-be-processed sensitive information determined by the monitoring unit; and

a first security determination unit that acquires data in the newly-added sensitive information log or the to-be-processed sensitive information log or the second sensitive

information library of a first target system, and determines, according to a preset determination rule, a security level to which the first target system belongs.

20. The security determination system of claim 19, wherein the first security determination unit includes at least one of the following units:

a first number determination unit that determines the security level of the first target system according to a number of the newly-added sensitive information within a first time window /the number of the sensitive information stored in the second sensitive information library; and

a first ratio determination unit that determines the security level of the first target system according to a ratio of a number of the newly-added sensitive information to a number of the to-be-processed sensitive information within a second time window.

21. The security determination system of claim 20, further comprising a multi-system determination unit that compares the security level of the first target system with that of a second target system according to a preset determination rule,

wherein the first security determination unit acquires data in the newly-added sensitive information log or the to-be-processed sensitive information log or the second sensitive information library of the second target system.

22. The security determination system of claim 21, wherein the multi-system determination unit includes at least one of the following units:

a second number determination unit that compares the security levels of the first target system and the second target system according to the number of the newly-added sensitive information of the first target system and the second target system within the first time window/the numbers of the sensitive information stored in the second sensitive information library; and

a second ratio determination unit that compares the security levels of the first target system and the second target system according to ratios of the numbers of the newly-added sensitive information of the first target system and the second target system to the number of the to-be-processed sensitive information within the second time window.