

What is claimed is:

1. A security scanning method for a mini program, the method comprising:
obtaining a target mini program to be released;
invoking a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program;
 wherein the multi-dimensional security scanning comprises malicious code scanning on the target mini program, security loophole scanning on the target mini program, and security loophole scanning on a server interface of the target mini program; and
 wherein the security loophole scanning on the target mini program comprises:
 detecting whether the target mini program includes a sensitive information leaking loophole;
 detecting whether the target mini program includes an HTML code loophole;
 detecting whether the target mini program includes a JS code loophole; and
 detecting whether the target mini program includes an unauthorized external resource reference loophole; and
when the target mini program passes the multi-dimensional security scanning, releasing the target mini program to a server corresponding to a target APP.
2. The method according to claim 1, wherein the malicious code scanning on the target mini program comprises one or more of:
 detecting whether the target mini program includes a payload;
 detecting whether a malicious invoking function, other than an authorized invoking function defined for the target mini program, is present in functions invoked by the target mini program; and
 detecting whether media or text content invoked by the target mini program includes non-compliant content.
3. The method according to claim 1, wherein the security loophole scanning on a server interface of the target mini program comprises:
 parsing the server interface of the target mini program; and
 performing interface loophole scanning on the parsed server interface.
4. A security scanning apparatus for a mini program, the apparatus comprising:
an obtaining module configured to obtain a target mini program to be released;
a scanning module configured to invoke a security scanning strategy combination to

perform multi-dimensional security scanning on the target mini program;

wherein the multi-dimensional security scanning comprises malicious code scanning on the target mini program, security loophole scanning on the target mini program, and security loophole scanning on a server interface of the target mini program; and

wherein the security loophole scanning on the target mini program comprises:

detecting whether the target mini program includes a sensitive information leaking loophole;

detecting whether the target mini program includes an HTML code loophole;

detecting whether the target mini program includes a JS code loophole; and

detecting whether the target mini program includes an unauthorized external resource reference loophole; and

a releasing module configured to, when the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP.

5. The apparatus according to claim 4, wherein the scanning module is configured to execute one or more of malicious code scanning programs including:

detecting whether the target mini program includes a payload;

detecting whether a malicious invoking function, other than authorized invoking functions defined for the target mini program, is present in functions invoked by the target mini program; and

detecting whether media or text content invoked by the target mini program includes non-compliant content.

6. The apparatus according to claim 4, wherein the scanning module is further configured to:

parse the server interface of the target mini program; and

perform interface loophole scanning on the parsed server interface.

7. An electronic device, comprising:

a processor; and

a memory configured to store machine executable instructions;

wherein, by executing a machine executable instruction stored in the memory and corresponding to a control logic for training a machine learning model, the processor is configured to:

obtain a target mini program to be released;

invoke a security scanning strategy combination to perform multi-dimensional security scanning on the target mini program;

wherein the multi-dimensional security scanning comprises malicious code scanning on the target mini program, security loophole scanning on the target mini program, and security loophole scanning on a server interface of the target mini program; and

wherein the security loophole scanning on the target mini program comprises one or more loophole scanning programs including:

detecting whether the target mini program includes a sensitive information leaking loophole;

detecting whether the target mini program includes an HTML code loophole;

detecting whether the target mini program includes a JS code loophole; and

detecting whether the target mini program includes an unauthorized external resource reference loophole; and

when the target mini program passes the multi-dimensional security scanning, release the target mini program to a server corresponding to a target APP.

8. The electronic device according to claim 7, wherein the malicious code scanning on the target mini program comprises one or more of:

detecting whether the target mini program includes a payload;

detecting whether a malicious invoking function, other than an authorized invoking function defined for the target mini program, is present in functions invoked by the target mini program; and

detecting whether media or text content invoked by the target mini program includes non-compliant content.

9. The electronic device according to claim 7, wherein the security loophole scanning on a server interface of the target mini program comprises:

parsing the server interface of the target mini program; and

performing interface loophole scanning on the parsed server interface.