CLAIMS

1. A method for application information risk management on a network device side, the method comprising:

receiving a user input selecting a target application information from a plurality of application information;

processing the target application information for a validation request;

transmitting the target application information to a system configured to validate the target application information and to determine a corresponding risk information (S32);

receiving, from the system, a prompt information based on the risk information (S33);

processing the prompt information to generate a risk warning information; and

displaying the risk warning information within a graphical user interface, wherein the target application information comprises an SMS message selected by a user, and wherein the risk warning information provides an indication of a risk the selected SMS message poses to the user.

2. The method of claim 1, wherein processing the target application information comprises removing a portion of the target application information to reduce a transmission data volume.

3. The method of any one of claims 1 to 2, wherein the target application information comprises a potentially harmful data received by the user equipment.

4. The method of claim 1, further comprising:

if the risk information indicates that the SMS message comprises false information, sending a rogue base station prompt information to a nearby user equipment of the user equipment, wherein a distance between the nearby user equipment and the user equipment is less than or equal to a predetermined device distance threshold.

5. The method of claim 1, wherein the SMS message comprises a suspected Smishing message.

6. The method of any one of claims 1 to 5, further comprising:

retrieving a related attribute information comprising at least one of the following: a sender information of the target application information, a content of the target application information, a user guide information of the target application information; and

transmitting the related attribute information to the system configured to validate the target application information.

7. A method for application information risk management on a network device side, the method comprising:

receiving a target application information that a user selects and requests for validation by using a user equipment (S31);

validating the target application information to determine a corresponding risk information (S32); and

transmitting a corresponding prompt information to the user equipment based on the risk information (S33), wherein the target application information comprises an SMS message selected by the user, and wherein the prompt information is for the user equipment to generate risk warning information which provides an indication of a risk the selected SMS message poses to the user.

8. The method of claim 7, wherein validating the target application information to obtain corresponding risk information comprises:

performing match querying in a corresponding validation database based on a related attribute information of the target application information; and

determining the corresponding risk information based on a record information that is in the validation database and that matches the related attribute information.

9. The method of claim 8, wherein the validation database comprises at least one of a library of message templates and a grade that enables successive validation of the target application information.

10. The method based on claim 8, wherein the related attribute information comprises at least one of the following:

a sender information of the target application information;

a content of the target application information; or

a user guide information of the target application information.

11. The method of claim 10, wherein the related attribute information comprises the user guide information of the target application information; and

the validating the target application information to obtain corresponding risk information further comprises:

if no record information that matches the user guide information is identified in the validation database, simulating an execution of the target application information based on the user guide information to obtain the corresponding risk information.

12. The method of claim 11, wherein simulating the execution of the target application information based on the user guide information to obtain the corresponding risk information comprises:

simulating acquiring, based on the user guide information, target information that is in the target application information and that the user is guided to acquire; and

validating a correspondence between the target information and the target application information to obtain the corresponding risk information.

13. The method of claim 12, wherein validating the correspondence between the target information and the target application information comprises at least one of the following:

checking whether a sender information of the target information is consistent with the sender information of the target application information;

checking whether a content of the target information is associated with the content of the target application information; and

checking whether a sandbox operation information of the target information matches the target application information.

14. An apparatus for application information risk management, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 13.