What Is Claimed Is

1. A computer-executed method, the method comprising:

obtaining attribute features of a user;

determining, by a computer, a first set of identification products and identification success rates thereof based on the attribute features of the user and a first machine-learning model for determining identification security;

generating a first set of identification product combinations, wherein a respective identification product combination comprises two different identification products selected from the first set identification products;

selecting, from the first set of identification product combinations, a second set of identification product combinations based on the identification success rates of the first set of identification products; and

selecting, from the second set of identification product combinations, a third set of identification product combinations based on the attribute features of the user and a second machine-learning model for determining identification applicability, thereby facilitating identification of the user using at least one of the third set of the identification product combinations.

2. The method according to claim 1, wherein selecting, from the first set of identification product combinations, the second set of identification product combinations comprises:

computing combined identification success rate for each of the first set of identification product combinations based on the identification success rate of each identification product; and

in response to the combined identification success rate of an identification product combination being greater than a first threshold, including the

identification product combination in the second set of identification product combinations.

3. The method according to claim 1, wherein selecting, from the second set of identification product combinations, the subset of identification product combinations comprises:

forming a second set of identification products using identification products included in the second set of identification product combinations;

for each identification product in the second set of identification products, determining an applicability-related identification success rate by inputting the identification product and the attribute features of the user into the second machine-learning model for determining identification applicability;

computing a combined applicability-related identification success rate for each of the second set of identification product combinations based on the applicability-related identification success rate of each identification product in the second set of identification products; and

in response to the combined applicability-related identification success rate of an identification product combination being greater than a second threshold, including the identification product combination in the subset of identification product combinations.

4. The method according to claim 3, wherein forming the second set of identification products further comprising applying a filter based on a predetermined security control policy.

5. The method according to claim 1, wherein determining the first identification products and the identification success rates thereof comprises:

determining a long-term identification success rate of a respective identification product based on the attribute features of the user;

determining a short-term identification success rate of the identification product corresponding to a target time period;

using a greater value of the long-term and short-term identification success rates of the identification product as the identification success rate of the first identification product.

6. The method according to claim 5, wherein determining the short-term identification success rate of the identification product comprises:

dividing potential risks associated with the identification product within the target time period into risk groups;

statistically computing an identification success rate of each risk group; and weighing identification success rates of the risk groups to obtain the short-term identification success rate of the identification product.

7. The method according to claim 1, further comprising training the first machine-learning model for determining identification security, which comprises:

obtaining identification security samples and first labels, wherein a respective identification security sample comprises a historical breakthrough event, an identification product corresponding to the historical breakthrough event, and historical attribute features of a user, and wherein a first label corresponding to the respective identification security sample indicates whether identification performed using the identification product corresponding to the historical breakthrough event is successful or not; and

training the first machine-learning model for determining identification security using the identification security samples and the first labels.

8. The method according to claim 1, wherein the first machine-learning model for determining identification security comprises a Markov Chain Monte Carlo (MCMC) model.

9. The method according to claim 1, further comprising training the second machine-learning model for determining identification applicability, which comprises:

obtaining identification applicability samples and second labels, wherein a respective identification applicability sample comprises a historical non-breakthrough event, identification product corresponding to the historical non-breakthrough event, and historical attribute features of a user, and wherein a second label corresponding to the respective identification applicability sample indicates whether identification performed using the identification product corresponding to the historical non-breakthrough event is successful or not; and

training the second machine-learning model for determining identification applicability using the identification applicability samples and the second labels.

10. The method according to claim 1, wherein the second machine-learning model for determining identification applicability comprises a random forest model.

11. A computer system, comprising:

a processer;

a storage device coupled to the processor and storing instructions, which when executed by the processor cause the processor to perform a method, the method comprising:

obtaining attribute features of a user;

determining a first set of identification products and identification

success rates thereof based on the attribute features of the user and a first machine-learning model for determining identification security;

generating a first set of identification product combinations, wherein a respective identification product combination comprises two different identification products selected from the first set identification products;

selecting, from the first set of identification product combinations, a second set of identification product combinations based on the identification success rates of the first set of identification products; and

selecting, from the second set of identification product combinations, a third set of identification product combinations based on the attribute features of the user and a second machine-learning model for determining identification applicability, thereby facilitating identification of the user using at least one of the third set of the identification product combinations.

12. The computer system according to claim 11, wherein selecting, from the first set of identification product combinations, the second set of identification product combinations comprises:

computing combined identification success rate for each of the first set of identification product combinations based on the identification success rate of each identification product; and

in response to the combined identification success rate of an identification product combination being greater than a first threshold, including the identification product combination in the second set of identification product combinations.

13. The computer system according to claim 11, wherein selecting, from the second set of identification product combinations, the subset of identification product combinations comprises:

forming a second set of identification products using identification products included in the second set of identification product combinations;

for each identification product in the second set of identification products, determining an applicability-related identification success rate by inputting the identification product and the attribute features of the user into the second machine-learning model for determining identification applicability;

computing a combined applicability-related identification success rate for each of the second set of identification product combinations based on the applicability-related identification success rate of each identification product in the second set of identification products; and

in response to the combined applicability-related identification success rate of an identification product combination being greater than a second threshold, including the identification product combination in the subset of identification product combinations.

14. The computer system according to claim 13, wherein forming the second set of identification products further comprising applying a filter based on a predetermined security control policy.

15. The computer system according to claim 11, wherein the method further comprises training the first machine-learning model for determining identification security, which comprises:

obtaining identification security samples and first labels, wherein a respective identification security sample comprises a historical breakthrough event, an identification product corresponding to the historical breakthrough

event, and historical attribute features of a user, and wherein a first label corresponding to the respective identification security sample indicates whether identification performed using the identification product corresponding to the historical breakthrough event is successful or not; and

training the first machine-learning model for determining identification security using the identification security samples and the first labels.

16. The computer system according to claim 11, wherein the first machine-learning model for determining identification security comprises a Markov Chain Monte Carlo (MCMC) model.

17. The computer system according to claim 11, wherein the method further comprises training the second machine-learning model for determining identification applicability, which comprises:

obtaining identification applicability samples and second labels, wherein a respective identification applicability sample comprises a historical non-breakthrough event, identification product corresponding to the historical non-breakthrough event, and historical attribute features of a user, and wherein a second label corresponding to the respective identification applicability sample indicates whether identification performed using the identification product corresponding to the historical non-breakthrough event is successful or not; and

training the second machine-learning model for determining identification applicability using the identification applicability samples and the second labels.

18. The computer system according to claim 11, wherein the second machine-learning model for determining identification applicability comprises a random forest model.

19. A non-transitory computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method, the method comprising:

obtaining attribute features of a user;

determining, by a computer, a first set of identification products and identification success rates thereof based on the attribute features of the user and a first machine-learning model for determining identification security;

generating a first set of identification product combinations, wherein a respective identification product combination comprises two different identification products selected from the first set identification products;

selecting, from the first set of identification product combinations, a second set of identification product combinations based on the identification success rates of the first set of identification products; and

selecting, from the second set of identification product combinations, a third set of identification product combinations based on the attribute features of the user and a second machine-learning model for determining identification applicability, thereby facilitating identification of the user using at least one of the third set of the identification product combinations.

20. The non-transitory computer-readable storage medium according to claim 19, wherein selecting, from the first set of identification product combinations, the second set of identification product combinations comprises:

computing combined identification success rate for each of the first set of identification product combinations based on the identification success rate of each identification product; and

in response to the combined identification success rate of an identification product combination being greater than a first threshold, including the

identification product combination in the second set of identification product combinations.

21. The non-transitory computer-readable storage medium according to claim 19, wherein selecting, from the second set of identification product combinations, the subset of identification product combinations comprises:

forming a second set of identification products using identification products included in the second set of identification product combinations;

for each identification product in the second set of identification products, determining an applicability-related identification success rate by inputting the identification product and the attribute features of the user into the second machine-learning model for determining identification applicability;

computing a combined applicability-related identification success rate for each of the second set of identification product combinations based on the applicability-related identification success rate of each identification product in the second set of identification products; and

in response to the combined applicability-related identification success rate of an identification product combination being greater than a second threshold, including the identification product combination in the subset of identification product combinations.

22. The non-transitory computer-readable storage medium according to claim 21, wherein forming the second set of identification products further comprising applying a filter based on a predetermined security control policy.

23. The non-transitory computer-readable storage medium according to claim 19, wherein the method further comprises training the first machine-learning model for determining identification security, which comprises:

obtaining identification security samples and first labels, wherein a respective identification security sample comprises a historical breakthrough event, an identification product corresponding to the historical breakthrough event, and historical attribute features of a user, and wherein a first label corresponding to the respective identification security sample indicates whether identification performed using the identification product corresponding to the historical breakthrough event is successful or not; and

training the first machine-learning model for determining identification security using the identification security samples and the first labels.

24. The non-transitory computer-readable storage medium according to claim 19, wherein the first machine-learning model for determining identification security comprises a Markov Chain Monte Carlo (MCMC) model.

25. The non-transitory computer-readable storage medium according to claim 19, wherein the method further comprises training the second machine-learning model for determining identification applicability, which comprises:

obtaining identification applicability samples and second labels, wherein a respective identification applicability sample comprises a historical non-breakthrough event, identification product corresponding to the historical non-breakthrough event, and historical attribute features of a user, and wherein a second label corresponding to the respective identification applicability sample indicates whether identification performed using the identification product corresponding to the historical non-breakthrough event is successful or not; and

training the second machine-learning model for determining identification applicability using the identification applicability samples and the second labels.

26. The non-transitory computer-readable storage medium according to claim 19, wherein the second machine-learning model for determining identification applicability comprises a random forest model.