CLAIMS

1. A method of identity authentication comprising the following steps:

A step determining that identity authentication on the source user will be performed in response to the request from the first device operated by the source user;

A step identifying the target user deemed to satisfy at least a preset condition, wherein the target user is different from a source user, the steps that identify the target user comprise:

A step computing a set of one or more trusted levels between the source user and respective users among the set of one or more associates users based at least in part on the historical user information of the source user and location information of respective users among a set of one or more associated users; the historical user information of the source user comprises information pertaining to one or more communications between the source user and the respective users among the set of one or more associated users; and

A step identifying the target user, including a step selecting the target user from the set of one or more associated users based at least in part on the corresponding trust level between the source user and the target user;

A step generating validation information to authenticate the identity of the source user;

A step sending the validation information to a second device operated by the target user; and

A step validating whether the validation response received from the first device operated by the source user matches the validation information sent to the second device.

2. The method of Claim 1, wherein the target user identification step is a step

selecting a set of one or more trusted users among one or more associated users of the set, the one or more trusted users has a trust level that satisfies or exceeds respective trust level threshold value, a step to select a set of one or more trusted users, wherein

the target user is selected from one or more trusted users of the set.

3. The method of Claim 2, wherein the historical user information includes Location-Based Services (LBS) information; and

the trusted levels of the set are computed based at least in part on the LBS information.

4. The method of Claim 2, wherein the historical user information includes WiFi hotspot scan information, and one or more trusted levels of the set are computed based at least in part on the WiFi hotspot scan information.

5. The method of Claim 2, wherein the historical user information includes communication information sent, received, pertaining to multiple communications sent and received by the first device, and one or more trust levels of the set are computed at least in part on the said communication information.

6. The method of Claim 1, wherein the preset condition includes a distance requirement of the second device operated by the target user on the first device operated by the source user.

7. The method of Claim 1, wherein the target user identification steps comprise:

A step determining a set of one or more nearby associated users of the source user;

A step determining a set of one or more trusted users among the one or more nearby users;

A step computing one or more trusted levels of the source user pertaining to respective users among one or more trusted users of the set; and

A step selecting a set of one or more potential target users among the set of one or more trusted users, wherein

the target user is selected among the set of one or more potential target users.

8. The method of Claim 7, wherein the set of one or more nearby users associated with the source user are determined based at least in part on the source user information sent by the first device.

9. The method of Claim 7, wherein the set of one or more nearby users associated with the source user are determined based at least in part on the current LBS information of the first device.

10. The method of Claim 7, wherein the set of one or more nearby users associated with the source user are determined based at least in part on WiFi hotspot scan information of the first device.

11. The method of Claim 1, wherein the steps of identifying the target user comprise:

A step sending information pertaining to multiple potential target users to the first device, and providing the information pertaining to multiple potential target users to the source user on the first device; and

A step receiving from the first device a selection of the target user among multiple potential target users conducted by the source users from the first device.

12. A system comprising:

one or more processors to:

determine to perform identity authentication on the source user in response to a request from the first device operated by the source user;

identify a target user deemed satisfying at least a preset condition, the target user being different from the source user, identifying the target user;

determining one or more set of associated users of the source user based at least in part on the historical source user information;

computing one or more set of trusted levels from the set associated users based at least in part on the historical source user information and the location information of each associated user, wherein the historical user information of the source user includes information associated with one or more communications between the source user and a set of one or more associated users;

identifying the target user, including selection of the target user from a set of one or more associated users, based at least in part on the trust level corresponding to the source user and the target user;

generating validation information to authenticate the identity of the source user;

sending the validation information to the second device operated by the target user;

receiving the authentication response from the first device operated by the source user;

performing identity authentication that includes validation whether the authentication response received from the first device operated by the source user matches the validation information sent from the second device; and

one or more memories coupled with said one or more processors, configured to provide instructions to the processors, including one or more memories.

13. The system of Claim 12, wherein identifying a target user comprises:

selecting a set of one or more users from the set of associated users, the one or more trusted users have a trust level satisfying or exceeding the threshold value of respective trust level threshold value, wherein

the target user is selected among the set of one or more trusted users.

14. The system of Claim 13, wherein the historical user information includes Location-Based Services (LBS), and the set of one or more trusted levels are computed based at least in part on the LBS information.

15. The system of Claim 13, wherein the historical user information includes WiFi hotspot scan information, and the one or more trusted levels of the set are computed based at least in part on the WiFi hotspot scan information.

16. The system of Claim 13, wherein the historical user information includes communication information pertaining to multiple communications sent or received, sent and received by the first device, and the one or more trust levels of the set are computed based at least in part on the communication information.

17. The system of Claim 12, wherein the preset condition includes the distance requirement of the second device operated by the target user relative to the first device operated by the source user.

18. The system of Claim 12, wherein identification of the target user includes:

determination of a set of one or more nearby users associated with the source user;

determination of a set of one or more trusted users among the one or more nearby users;

computing a set of one or more trusted levels of the source user pertaining to respective users among the set of one or more trusted users; and

selecting a set of one or more potential target users among one or more trusted users of the set, wherein

the target user is selected from the set of potential target users.

19. The system of Claim 18, wherein the set of one or more nearby users associated with the source user is determined based at least in part on source user information sent by the first device.

20. The system of Claim 18, wherein the set of one or more nearby users associated with the source user is determined based at least in part on the current LBS information of the first device.

21. The system of Claim 18, wherein the set of one or more nearby users associated with the source user is determined at least in part on the WiFi hotspot scan information of the first device.

22. The system of Claim 12, wherein identification of the target user includes

sending associated information to the first device pertaining to multiple potential target users; providing the information pertaining to the multiple potential target users to the source user on the first device; and

receiving from the first device selection of the target user conducted by the source user among the multiple potential target users.

23. A non-temporary computer readable recording medium designed to perform identity authentication, wherein a computer program contains computer instructions for:

determining, in response to a request from a first device operated by the source user, to perform identity authentication on the source user;

identifying a target user who is deemed to satisfy at least a preset condition, the target user is different from the source user, the process of identifying the target user comprises:

determining a set of one or more associated users of the source user based at least in part on the historical source user information;

computing a set of one or more trusted levels from the set of one or more associated users based at least in part on the historical source user information and the location information of respective associated users, wherein the historical user information of the source user includes information associated with one or more communications between the source user and a set of one or more associated users;

identifying the target user, including selection of the target user from a set of one or more associated users, based at least in part on the trust level, corresponding to the source user and the target user;

generating validation information to authenticate the identity of the source user;

sending the validation information to the second device operated by the target user;

receiving a validation response from the first device operated by the source user;

validating whether the validation response received from the first device operated by the source user matches the validation information sent to the second device.