

(19) United States

(12) Patent Application Publication Zheng

(10) Pub. No.: US 2015/0046696 A1

(43) **Pub. Date:**

Feb. 12, 2015

(54) METHOD AND APPARATUS FOR SECURED SOCIAL NETWORKING

(75) Inventor: Yan Zheng, Espoo (CN)

Assignee: Nokia Corporation, Espoo (FI)

(21) Appl. No.:

14/385,497

(22) PCT Filed:

Mar. 31, 2012

(86) PCT No.:

PCT/CN2012/073415

§ 371 (c)(1),

(2), (4) Date:

Sep. 15, 2014

Publication Classification

(51) **Int. Cl.** H04L 9/08

(2006.01)

H04L 9/16

(2006.01)

(52) U.S. Cl.

CPC H04L 9/083 (2013.01); H04L 9/088 (2013.01); H04L 9/16 (2013.01)

(57)ABSTRACT

Various methods are described for using a local trust level and/or a general trust level to control access of data in PSN. Any PSN user can select other users with at least a minimum level of local and/or general trust for secure communications. The users with a trust level below a minimum trust level cannot access the data sent from him/her. The general trust level is controlled by access keys that are generated and issued by a trusted server. The local trust level controlled access keys are generated by each PSN device. Each PSN device issues the corresponding personalized secret keys to those users that satisfy the decryption conditions related to local trust level evaluated by PSN user itself. Both sets of keys can be applied at the same time to secure communication data in PSN controlled by both the general trust level and the local trust level.

Determine a general trust level for one or more users

Generate a public encryption key and one or more personalized decryption secret keys for the one or more users based on the general trust levels of the one or more users

Cause the public encryption key and the one or more personalized decryption secret keys to be issued to the one or more users, wherein the one or more users are configured to encrypt a message using the encryption public key based on preferred access control conditions and are further configured to decrypt a message using the personalized secret keys issued by the trusted server in an instance in which an access control conditions is satisfied

804

802

806